UNIVERSIDAD TÉCNICA DEL NORTE

Facultad de Ingeniería en Ciencias Aplicadas

Carrera de Software

Diseño de un Sistema de Gestión de la Seguridad de la Información para el Departamento de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte basado en la Norma ISO/IEC 27001.

Trabajo de grado previo a la obtención del título de Ingeniero de Software presentado ante la ilustre Universidad Técnica del Norte.

Autor:

Stalin Santiago Guzmán Iles

Director:

MSc. Daisy Elizabeth Imbaquingo Esparza

Ibarra – Ecuador

2023

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	100355771-5		
APELLIDOS Y NOMBRES:	GUZMÁN ILES STALIN SANTIAGO		
DIRECCIÓN:	IBARRA, SAN FRANCISCO		
EMAIL:	ssguzmani@utn.edu.ec		
TELÉFONO FIJO:	2625-091	**TELÉFONO MÓVIL:**	0969375530

DATOS DE LA OBRA	
TÍTULO:	DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA EL DEPARTAMENTO DE DESARROLLO TECNOLÓGICO E INFORMÁTICO DE LA UNIVERSIDAD TÉCNICA DEL NORTE BASADO EN LA NORMA ISO/IEC 27001.
AUTOR(ES):	STALIN SANTIAGO GUZMÁN ILES
FECHA:	31/05/2023
PROGRAMA:	PREGRADO
TÍTULO POR EL QUE OPTA:	INGENIERO DE SOFTWARE
DIRECTOR:	MSc. DAISY IMBAQUINGO
ASESOR 1:	MSc. COSME ORTEGA
ASESOR 2:	MSc. SILVIA ARCINIEGA

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de esta y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 31 días del mes de mayo de 2023

EL AUTOR:

ESTUDIANTE

Stalin Santiago Guzmán Iles

C.I: 100355771-5

CERTIFICACIÓN DIRECTOR

Ibarra 31 de mayo del 2023

CERTIFICACIÓN DIRECTOR DEL TRABAJO DE TITULACIÓN

Por medio del presente yo MSc. Daisy Elizabeth Imbaquingo Esparza, certifico que el Sr. Stalin Santiago Guzmán Iles portador de la cedula de ciudadanía número 1003557715, ha trabajado en el desarrollo del proyecto de grado "Diseño de un Sistema de Gestión de la Seguridad de la Información para el Departamento de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte basado en la Norma ISO/IEC 27001", previo a la obtención del Título de Ingeniero en Software realizado con interés profesional y responsabilidad que certifico con honor de verdad.

Es todo en cuanto puedo certificar a la verdad

Atentamente

MSc. Daisy Imbaquingo

DIRECTOR DE TRABAJO DE GRADO

Dedicatoria

Quiero dedicar este trabajo de grado a mi madre María Georgina Iles Canacuán y a mi hermana Lizbeth Paola Guzmán Iles, quienes han estado a mi lado en las etapas más difíciles de mi vida, además de saberme guiar a lo largo de este desafiante camino, brindándome su apoyo, amor y confianza, elementos esenciales para cumplir mi sueño.

También quiero destacar el apoyo de mis amigos y a los docentes que me han impartido sus conocimientos, ayudándome a crecer como persona y profesional.

Por último, quiero expresar mi gratitud a mis familiares y en especial a Lizbeth Suarez quien ha sido una persona fundamental en mi vida y en este proceso. ¡Gracias Totales!

Stalin Santiago Guzmán Iles

Agradecimientos

Agradezco infinitamente a Dios por ser mi guía, por darme fuerza y por guiarme con sabiduría durante todo este proceso. También quiero agradecer a mi madre y hermana por motivarme a nunca rendirme y cumplir mis sueños.

Además, quiero expresar mi gratitud a la Universidad Técnica del Norte, en particular a la Facultad de Ciencias Aplicadas FICA y la carrera de Ingeniería en Software, por brindarme la oportunidad de cumplir esta meta. Agradezco a mis docentes por compartir su conocimiento y tiempo en mi formación personal y profesional, y a todas las personas que me han apoyado directa e indirectamente a lo largo de mi vida universitaria.

Mi sincero agradecimiento a la MSc. Daisy Imbaquingo, por su colaboración invaluable como directora de tesis, cuyo apoyo, consejos y recomendaciones fueron claves para el éxito de este proyecto académico.

Stalin Santiago Guzmán Iles

Tabla de Contenido

Índice de Figuras

Índice de Tablas

Resumen

El presente documento llevó por título “DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA EL DEPARTAMENTO DE DESARROLLO TECNOLÓGICO E INFORMÁTICO DE LA UNIVERSIDAD TÉCNICA DEL NORTE BASADO EN LA NORMA ISO/IEC 27001”; la problemática presentada en esta institución fue la carencia de controles para gestionar la seguridad de la información; el objetivo general fue diseñar un SGSI mediante la Norma ISO/IEC 27001, para fortalecer la seguridad de la información en el DDTI de la UTN; la metodología usada fue Magerit v3 y se desarrolló en base al enfoque cuantitativo y cualitativo, las técnicas utilizadas fueron la encuesta y el instrumento un cuestionario, además se realizó una entrevista; la validación se la realizó en base al método Delphi; los resultados revelaron que la institución tiene un nivel de madurez repetible, esto se debe a la carencia de políticas o controles que aborden asuntos de seguridad de la información; la conclusión más representativa fue sugerir que se realice una mejora en las medidas de seguridad tanto físicas como electrónicas en la institución, además de planificar mantenimientos preventivos como correctivos de forma regular en los equipos.

Abstract

The present document is titled "DESIGN OF AN INFORMATION SECURITY MANAGEMENT SYSTEM FOR THE TECHNOLOGICAL AND IT DEVELOPMENT DEPARTMENT OF THE TECHNICAL UNIVERSITY OF THE NORTH BASED ON ISO/IEC 27001". The problem presented in this organization was the lack of controls to manage information security. The general objective was to design an ISMS based on ISO/IEC 27001 to strengthen information security in the DDTI of UTN. The methodology used was Magerit v3 and was developed based on a quantitative and qualitative approach. The techniques used were surveys and a questionnaire instrument, in addition to an interview. The validation was performed based on the Delphi method. The results revealed that the organization has a repeatable maturity level, which is due to the lack of policies or controls that address information security issues. The most representative conclusion was to suggest that the organization improve its physical and electronic security measures, in addition to regularly planning preventive and corrective maintenance of the equipment.

Introducción

Tema

Diseño de un Sistema de Gestión de la Seguridad de la Información para el Departamento de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte basado en la Norma ISO/IEC 27001.

Problema

Antecedentes

Debido a que las empresas dependen cada vez más de la información para agregar valor a sus productos y servicios, la protección de la información confidencial se convierte en una estrategia estratégica para garantizar la sostenibilidad (Hohan et al., 2015).

La ISO 27001 radica en proteger los riesgos que amenazan la integridad, confidencialidad y disponibilidad de la información de una institución, siendo este el caso del Departamento de Desarrollo Tecnológico e Informático (DDTI) de la Universidad Técnica del Norte (UTN), que diariamente está expuesto a riesgos potenciales por la vulnerabilidad e inseguridad que existe hoy en día dado a la exposición de la información.

De acuerdo con el Registro Oficial Nro. 228 en el Artículo Nro.4 menciona que las Instituciones de la Administración Pública Central, Institucional y que dependan de la Función Ejecutiva, actualizarán o implementarán el Esquema Gubernamental de Seguridad de la Información (EGSI) en un plazo de doce (12) meses contados a partir de la publicación del Acuerdo Ministerial en el Registro Oficial además en su Artículo Nro. 7 adjunta que el Comité de Seguridad de la Información (CSI) designará al interior de su Institución a un funcionario como Oficial de la Seguridad de la Información (Registro Oficial, 2020).

La evaluación de riesgos y el plan de respuesta a los riesgos de cada organismo se realizarán en un plazo de cinco meses, y la actualización o implementación de los controles establecidos por EGSI se realizará en un plazo de siete meses. Las actualizaciones o

implementaciones se producirán en todas las organizaciones en función del ámbito de acción, estructura orgánica, recursos y nivel de madurez de la gestión de la seguridad de la información (Registro Oficial, 2020).

La información es uno de los activos más importantes y valiosos que posee la UTN, por lo cual es necesario que esta Institución de Educación Superior (IES)cuente con una gestión idónea de los activos y recursos tecnológicos a fin de garantizar el tratamiento y manejo adecuado de la información, puesto que no existe una seguridad absoluta es factible implantar métricas de seguridad sustentados en potenciales riesgos y amenazas que se puedan detectar (López Rubio, 2014).

Según Imbaquingo et al. (2021) , la propagación de virus a través de medios tecnológicos es uno de los problemas que enfrentan las IES en el ámbito de la seguridad, además del poco o nulo interés en garantizar la seguridad de los activos de las IES y los problemas con la implementación de medidas de seguridad en las IES.

El propósito de diseñar un Sistema de gestión de la seguridad de la información (SGSI) es que sea sostenible y alineado con la misión, la estrategia y los objetivos de la institución. Un SGSI es un sistema de gestión que incluye las políticas, las estructuras organizativas, los procedimientos, los procesos y los recursos necesarios para implementar la gestión de la seguridad de la información a fin de minimizar los daños a la empresa, aumentar las oportunidades comerciales, el retorno de la inversión y garantizar la continuidad del negocio (Satán, 2017).

Situación Actual

Los sistemas de información en las IES todavía tienen "dificultades en su desempeño integral para contribuir a un control de gestión para la toma de decisiones, que responde a las Normas Técnicas Ecuatorianas (NTE) vigentes en el país". Por lo tanto, es necesario implementar evaluaciones de vulnerabilidad para mejorar la seguridad de los productos y procesos que utilizan la información como activo (Altamirano, 2019).

Actualmente, la información digital que maneja el DDTI de UTN tiene un valor indeterminado y hoy en día esta se ha convertido en un activo primordial dentro de la institución, debido a que alberga en su Cloud datos de personal administrativo, docente y estudiantil, esto lleva a considerar que en algún momento dicha información puede ser expuesta, modificada o destruida a causa de robos de identidad y malas prácticas en la gestión de la información.

Según Cano (2004) en su artículo “Inseguridad Informática: un concepto dual en seguridad informática” manifiesta realizar un análisis actual dentro de cada organización, lo cual contribuya a fortalecer sus esquemas de seguridad.

Prospectiva

El presente trabajo plantea diseñar un plan de gestión para el análisis de riesgos tecnológicos basado en la identificación de activos y riesgos asociados. El plan tiene como finalidad minimizar las probabilidades de sufrir afectaciones y pérdidas económicas, informáticas, ambientales y humanas como consecuencia del funcionamiento ineficiente de los activos tecnológicos. El plan de gestión será diseñado con base en la metodología de análisis de riesgos MAGERIT en su versión 3 para poder ser aplicado al departamento de estudio, que en este caso es el Departamento de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte.

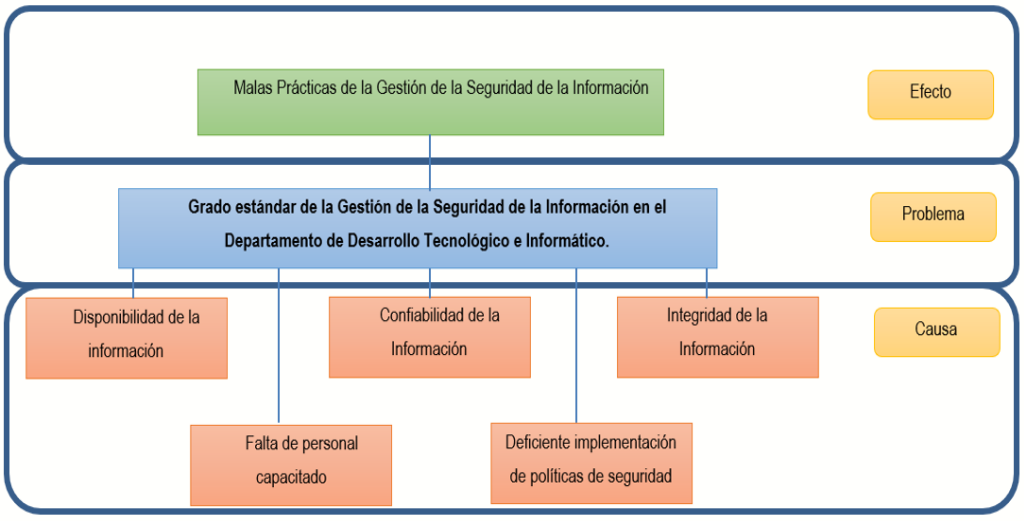
Planteamiento del problema

El manejo de la información dentro del DDTI de la UTN es una problemática que se refleja en la Gestión de la Seguridad de la Información, ya que diariamente los datos están expuestos a un sin número de amenazas lo cual pone en riesgo la documentación existente, lo que conlleva a comprometer a la institución para realizar un buen manejo de la información digital, que posee dentro de sus centros de datos para garantizar su disponibilidad, confiabilidad e integridad.

Para crear el diagrama de causa-efecto se utilizó la Matriz Vester como herramienta para reconocer y catalogar las dificultades en el proyecto planteado.

Figura 1

Árbol de problemas



Nota: La figura representa el árbol de problemas con las causas, efectos y problema identificado para el presente trabajo. Elaboración propia.

Objetivos

Objetivo General

Diseñar un SGSI mediante la Norma ISO/IEC 27001, para fortalecer la seguridad de la información en el DDTI de la UTN.

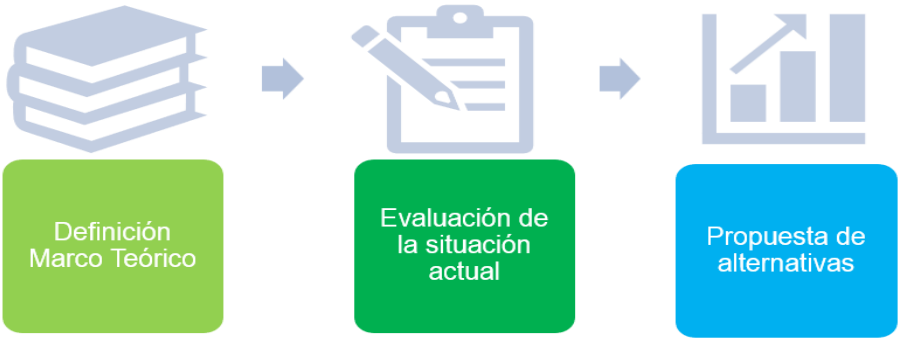
Objetivos Específicos

- Definir un marco teórico para un SGSI basado en la Norma ISO/IEC 27001
- Diseñar un modelo adecuado de SGSI, fundamentado en los indicadores de la Norma ISO/IEC 27001 para reducir la factibilidad y acontecimiento de amenazas en el DDTI de la UTN.
- Validar el modelo propuesto estadísticamente.

Alcance

Figura 2

Alcance del trabajo de investigación



Nota: Elaboración propia.

Marco teórico: Inmerso al marco teórico se realizará una búsqueda sobre trabajos relacionados al SGSI y a la norma ISO/IEC 27001, se describirá conceptos de los fundamentos de seguridad de la información, así como, la normativa ISO/IEC 27001 y las metodologías para la gestión de riesgos; los puntos previamente expuestos serán extraídos de fuentes bibliográficas con contenido científico. Siendo el marco teórico el soporte bibliográfico del tema en estudio, es importante construirlo de manera efectiva para lograr buenos resultados dentro del proyecto en desarrollo (Gallego Ramos, 2018).

Situación actual del manejo de información del DDTI de la UTN: Se realizará una recopilación de datos sobre el contexto actual del DDTI y los procesos que se generan actualmente para el manejo de la información, además de realizar un inventario de activos de la información.

Proponer alternativas que permitan aumentar la calidad en la gestión de la información: Determinar los indicadores que permitirán cuantificar la calidad en la gestión de la información que se ha obtenido en el proceso de auditoría. Cada uno de ellos deben ser adecuados para la investigación, de tal forma que se logre la medición, el análisis y la evaluación respectiva (Restrepo Ortiz & Zabala Mendoza, 2016).

Diseñar un modelo adecuado de SGSI: Los resultados del proyecto se verán reflejados en un informe de políticas y procedimientos con el fin de reducir la factibilidad y acontecimiento

de amenazas en el DDTI y con ellos se aportará a mejorar la gestión de la seguridad de la información.

El desarrollo del trabajo abarca el diseño de un sistema de Gestión de Seguridad de la información en DDTI de la UTN, además de la valoración y clasificación de los activos de información. Este trabajo no abarca implementación, mantenimiento y revisión del Sistema de Gestión de Seguridad de la Información.

Metodología

Para llevar a cabo la propuesta se realizará una metodología de investigación aplicada usando material de fuentes de datos bibliográficas, para indagar acerca de la Gestión de la Seguridad de la Información y de esta manera dar solución a los problemas encontrados, además se hará una investigación proyectiva para la creación, diseño y elaboración de planes del presente anteproyecto con el fin de alcanzan los objetivos y que todo se realice adecuadamente. Se desarrollará una metodología mixta referenciada del anexo A de la Norma ISO/IEC 27001 que permitirá recolectar información, por medio de una entrevista y encuesta cerrada que se basará en la observación, estudio y evaluación cuantitativa.

Justificación

Político

El presente proyecto se enfoca en dar solución a dos de los Objetivos de Desarrollo Sostenible (ODS), el objetivo N°16 “Sin paz, estabilidad, derechos humanos y gobernabilidad efectiva basada en el Estado de derecho, no es posible alcanzar el desarrollo sostenible” ya que se prevé reducir los riesgos en cuanto a la seguridad de la información, también el objetivo N°11 “Lograr que las ciudades sean más inclusivas, seguras, resilientes y sostenibles” (Fondo de Población de las Naciones Unidad- UNFPA, 2017).

Además, dentro del Plan Nacional Toda Una Vida se fundamenta en el objetivo N°5: ¨Impulsar la productividad y competitividad para el crecimiento económico sostenible de manera

redistributiva y solidaria¨ ((CNP) C, Moreno L, 2014), enmarcado en el desarrollo y la transferencia tecnológica

Tecnológico

Los resultados obtenidos en el proceso de auditoría de la información necesitan de un estudio objetivo, de estándares y normativas para lograr diagnosticar falencias y garantizar una adecuada gestión de los sistemas de información, para ello se hará el uso de herramientas tecnológicas que permitan el análisis de los datos.

Teórico

Se realizará un análisis de la situación actual del manejo de la información tomando en cuenta los aspectos de integridad, confidencialidad y disponibilidad en base la Norma ISO/IEC 27001.

Metodológica

Se efectuará una investigación aplicada, proyectiva y mixta que permitirá conocer sobre el manejo de la información, seguidamente elaborar planes con los cuales se alcanzará el objetivo y por último el análisis de datos obtenidos para poder plantear nuevas formas de gestionar la información.

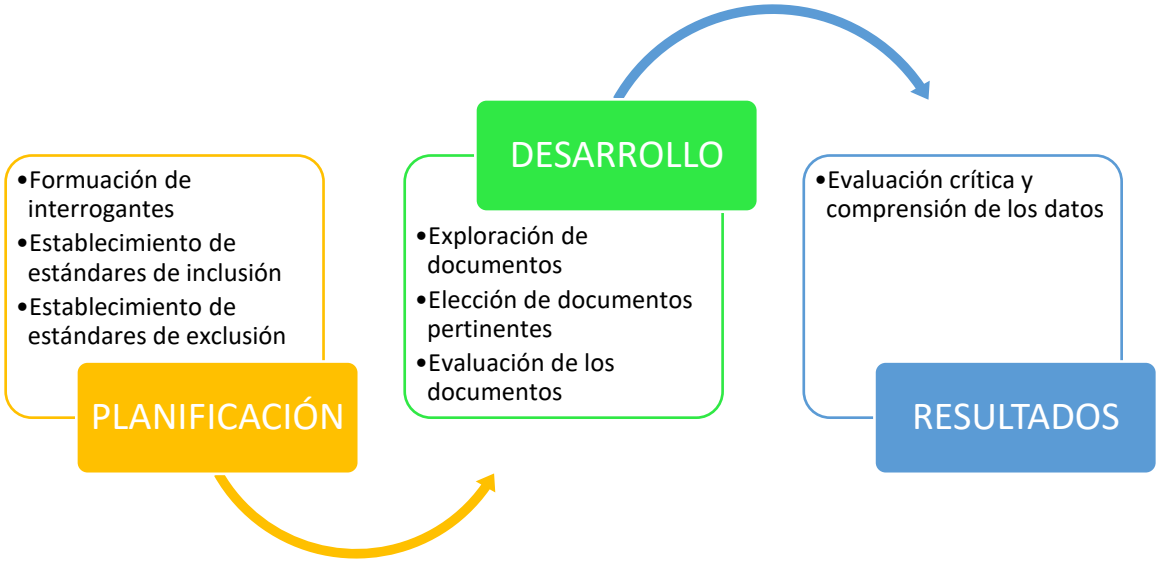
CAPÍTULO 1

Marco Teórico

Para desarrollar el marco teórico que aborda la gestión y análisis de riesgos en el ámbito del Sistema de Gestión de la Seguridad de la Información en las Instituciones de Educación Superior, se implementó el enfoque de Revisión Sistemática de Literatura (LSR). Este método se compone de diferentes etapas que se detallan en la Figura 3 para asegurar la exhaustividad y precisión en la recopilación y análisis de la información pertinente.

Figura 3

Proceso Revisión Sistemática de Literatura



Nota: La figura exhibe las etapas y las actividades correspondientes para llevar a cabo la elaboración del Marco Teórico mediante la realización de una Revisión Sistemática de Literatura. Elaboración propia.

Durante la etapa de planificación se consideraron diversas perspectivas y se formularon preguntas significativas relacionadas con el tema del Sistema de Gestión de la Seguridad de la

Información. Estas perspectivas incluyeron diferentes enfoques para abordar el problema en cuestión, estas son:

- Caracterización del concepto de Sistema de Gestión de la Seguridad de la Información en Instituciones de Educación Superior
    I. ¿Qué es el Sistema de Gestión de la Seguridad de la Información?
    II. ¿Qué conceptos relacionados existen en torno al Sistema de Gestión de la Seguridad de la Información?
    III. ¿Qué beneficios presenta el proceso de realizar un Sistema de Gestión de la Seguridad de la Información en las organizaciones?
- Caracterización de metodologías para un Sistema de Gestión de la Seguridad de la Información
    I. ¿Qué metodologías existe para el Sistema de Gestión de la Seguridad de la Información?
    II. ¿Cuáles son los pasos o fases para dichas metodologías?
    III. ¿Qué ventajas o desventajas presentan dichas metodologías?
- Caracterización de Normas para la Sistema de Gestión de la Seguridad de la Información
    I. ¿Qué normas nacionales o internacionales existen para un Sistema de Gestión de la Seguridad de la Información?
    II. ¿Qué recomendaciones o cumplimiento exigen dichas normas?
    III. ¿Qué ventajas o desventajas presentan dichas normas?

Los criterios de inclusión son una serie de requisitos que actúan como herramientas de selección para el material de investigación. Dicho material puede abarcar diversas fuentes como artículos científicos, entrevistas, informes oficiales, libros, páginas web o tesis.

Para los artículos científicos, es necesario que pertenezcan a revistas científicas ubicadas en los cuartiles Q1 a Q4 y estén disponibles en español o inglés.

En la etapa de desarrollo, se llevó a cabo una exhaustiva investigación en múltiples bases de datos bibliográficas, entre las que se incluyen Elibro, IEEE, Scopus, Springer, Elsevier, y repositorios de instituciones de educación superior. Posteriormente, se aplicaron criterios de inclusión para filtrar los resultados y se elaboró una matriz de fichaje para recopilar y organizar los datos relevantes obtenidos de esta búsqueda.

En la etapa de obtención de resultados, se llevó a cabo un minucioso examen de la información de mayor importancia, la cual se presenta a continuación de manera detallada y precisa.

1.1. Fundamentos de la Seguridad de la Información

En la actualidad, la información es esencial para el éxito y la supervivencia de cualquier empresa u organización (Wang & Tsai, 2009). Por lo tanto, cuando las instituciones, organizaciones y personas responsables eligen implementar métodos de seguridad de la información, los modelos y sistemas deben evaluarse por su eficiencia y eficacia a través de auditorías que permiten su revisión y análisis a través de estándares y buenas prácticas (Dhillon et al., 2021).

La seguridad de la información según la ISO/ IEC (2016) hace referencia a las adecuadas estrategias y procesos que logran proteger la infraestructura tecnológica y los sistemas de información de acceso, logrando con ello el máximo rendimiento de una organización con el mínimo riesgo.

La seguridad está fundamentada por tres pilares: la confidencialidad, integridad y disponibilidad que preverá la perdida de la seguridad o usabilidad, por lo tanto, es importante comprender la vital importancia de la información para una organización porque puede llegar a perder su valor y seguridad (Guano & Jaramillo, 2020).

Figura 4

Pilares de la seguridad de información

Nota: Elaboración propia.

Confidencialidad: Únicamente el personal autorizado podrá acceder a la información asignada utilizando la autenticación de usuario, gestión de permisos y cifrado de información, además se debe considerar que los principios de confidencialidad no pueden ni deben ser aplicados con la finalidad netamente de protección a la información sino también de todos los datos cuya organización sea responsable (Romero, 2018).

Según Kisan & Rao (2020) señala que el principio de confidencialidad establece que solo el remitente y los destinatarios previstos deben poder acceder al contenido del mensaje.

Integridad: Garantizar que la información no sufra manipulaciones voluntarias e involuntarias mediante monitoreos del tráfico de red, auditar sistemas para conocer las actividades e información correspondientes a cada empleado, implementar sistemas de control de cambios y finalmente poseer copias de seguridad que ayuden a prevenir los errores acumulativos (Figueroa, 2018) .

De acuerdo con Mahfouz Alhassan & Adjei-Quaye (2017) sostiene que la integridad es segura que el mensaje no se haya modificado o transitado y que este protegido durante su transmisión. También ayuda a garantizar que nuestros datos sean lo que se supone que son, en cualquier momento que se necesite, y que no han sido modificados sin autorización, integridad y legibilidad de la información.

Disponibilidad: Es importante considerar la accesibilidad de la información y servicios para el usuario debido a que debe ser útil y valiosa, para cumplir este propósito se emplea el

acuerdo de nivel de servicio (SLA), balanceadores de carga de tráfico que impiden el impacto de DDoS y copias de seguridad en casos de emergencia de recuperación de datos (Vera, 2018).

De Acuerdo con Mahfouz Alhassan & Adjei-Quaye (2017) la disponibilidad significa que los sistemas informáticos que se utilizan para almacenar y procesar datos, los controles de seguridad que se utilizan para protegerlos y los canales de comunicación que se utilizan para acceder deben estar operativos y disponibles en todo momento para evitar interrupciones del servicio causadas por cortes de energía, fallas de hardware y actualizaciones del sistema.

1.1.1. Vulnerabilidad

Las vulnerabilidades existen no pueden llegar a ser fabricadas, pero si ser explotadas por amenazas y considerarse debilidades que ocasionan daños. El hardware o software ocasionan impactos negativos dentro de la organización al momento de ser explotadas y pueden ser físicas: afectan de manera directa a la estructura física de la organización como son los desastres naturales, además existen vulnerabilidades lógicas: afectan a la operación de la infraestructura tecnológica, ejemplo de ello son los errores de programación y finalmente las vulnerabilidades humanas: afectan al factor humano de la organización por falta de entrenamiento (Vega, 2021).

1.1.2. Amenazas

Incidentes que ocurren dentro de una organización y que provocan daños directos a los activos, estos sucesos pueden ser de carácter natural en el cual es víctima pasiva el sistema de información, sin embargo, también existen amenazas causadas por las personas y que provocan desde un error de usuario hasta un ataque informático irreparable.(Michilena & Díaz, 2018)

1.1.3. Riesgo

Se considera riego al proceso encargado de determinar una posible amenaza dentro de cualquier sistema de información para ello en esta fase se establece un rango de aceptabilidad del riesgo dentro de una organización tomando en cuenta la gravedad del impacto para no generar incidentes no deseados (Trujillo & Rozo, 2018).

Según Imbaquingo al. (et 2017), el riesgo es la posibilidad de que una amenaza se materialice, lo que podría resultar en beneficios o daños.

1.1.4. Incidente

Un incidente es capaz de comprometer la continuidad de un negocio y amenazar seriamente la seguridad de la información debido a que se considera un incidente a uno o varios eventos de seguridad de la información que se desarrollan de forma no deseada. Por esta razón cuando se identifique un incidente se procede inmediatamente a ser notificado para que la gestión de incidentes determine la gravedad y logren resolverlo para posteriormente notificar que se ha arreglado el incidente (López, 2020).

1.1.5. Controles

Se consideran controles a las medidas que ayudan a mitigar el riesgo mediante una previa valoración y determinación de amenazas, basada en procesos, políticas y dispositivos. (Romero et al., 2018).

Los controles se clasifican en tres, control correctivo: corrige un error, riesgo u omisión, aunque la amenaza ha sido materializada, control detectivo: muestra el riesgo o error, la amenaza es materializada pero no puede ser corregido por sí mismo y finalmente el control preventivo: impide que se produzca un riesgo o error por lo tanto la amenaza no llega a materializarse (Guano & Jaramillo, 2020).

1.1.6. Ataques Informáticos

Los ataques informáticos se aprovechan de las vulnerabilidades existentes en el software o hardware, inclusive en el personal de la organización, con la finalidad de obtener un beneficio económico que provoca efectos negativos en la seguridad del sistema que obviamente traerá repercusiones directas a los activos de la organización (Mieres, 2009).

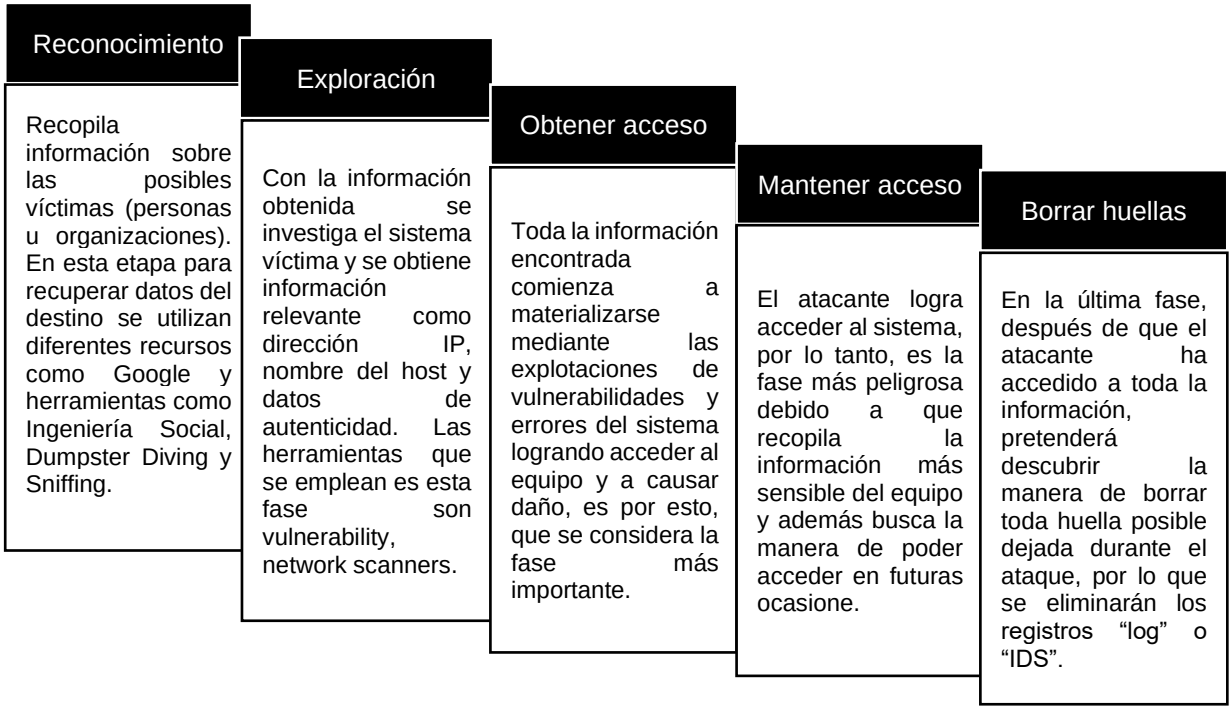
Con el desarrollo de internet y dispositivos de conectividad, actualmente existen ataques informáticos que pueden causar problemas significativos en la seguridad de la información (Imbaquingo & Pusda, 2015).

Por esta razón, es importante conocer cuáles son las debilidades más comunes, sus respectivos riesgos, cual es la forma de atacar a un sistema informático para luego de forma acertada e inteligente aplicar estrategias efectivas de seguridad y controlar actividades delictivas.

Un ataque informático tiene cinco fases comunes al momento de ser puesto en ejecución:

Figura 5

Cinco fases comunes de un ataque informático.



Nota: Elaboración propia.

1.2. Sistema de Gestión de la Seguridad de la Información

Las siglas SGSI son equivalentes a “Information Security Management System” y se enfoca a un conjunto de principios que definen, construyen, desarrollan, protegen la información y uso no autorizado mediante recursos de hardware y software. Según la ISO 27001:2015, la seguridad de la información alude la confidencialidad, integridad y disponibilidad de información sin importar el formato en el que se encuentren.

Es importante identificar el ciclo de vida y los aspectos más relevantes de la información para garantizar la confidencialidad, integridad y disponibilidad; consecutivamente con la información encontrada se adopta un proceso sistemático desde un enfoque de riesgos empresariales para conseguir los objetivos establecidos en una empresa y asegurarse de esta manera que existan beneficios económicos (Buitrago & Alvarado, 2018).

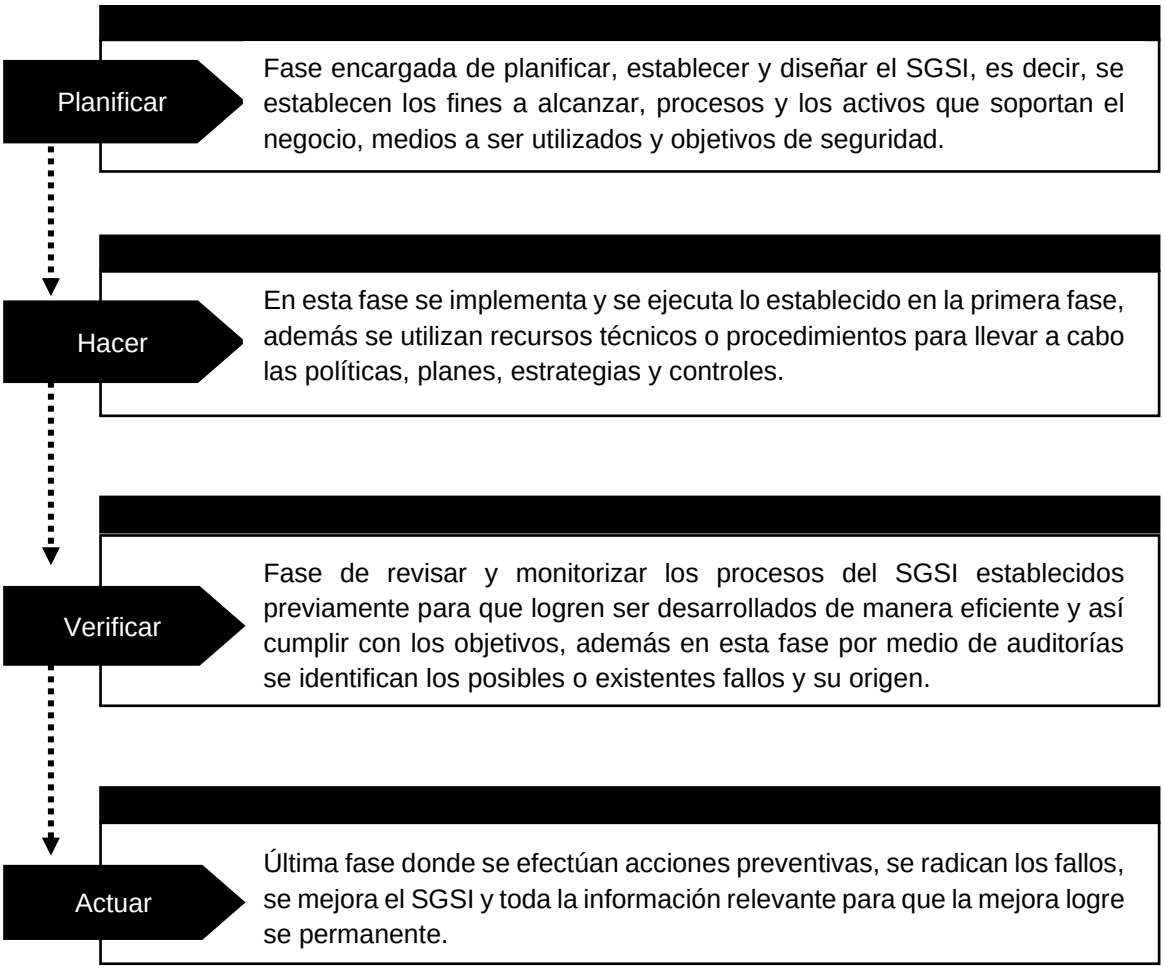
1.2.1. Ciclo PDCA

El ciclo PDCA (Plan, Do, Check, Act), es una metodología para gestionar y establecer un Sistema de Gestión de Seguridad de la Información que a la vez permite desarrollar un modelo de indicadores aplicables para cada uno de los elementos y así, proporcionar una mejora continua. (Novoa, 2015).

La metodología se desarrolla en cuatro fases correspondientes a sus siglas (PDCA), las cuales se encargan de cuantificar el avance de la organización, a continuación, en la Figura 6, se detallará las respectivas acciones:

Figura 6

Descripción de las fases de la metodología PDCA.

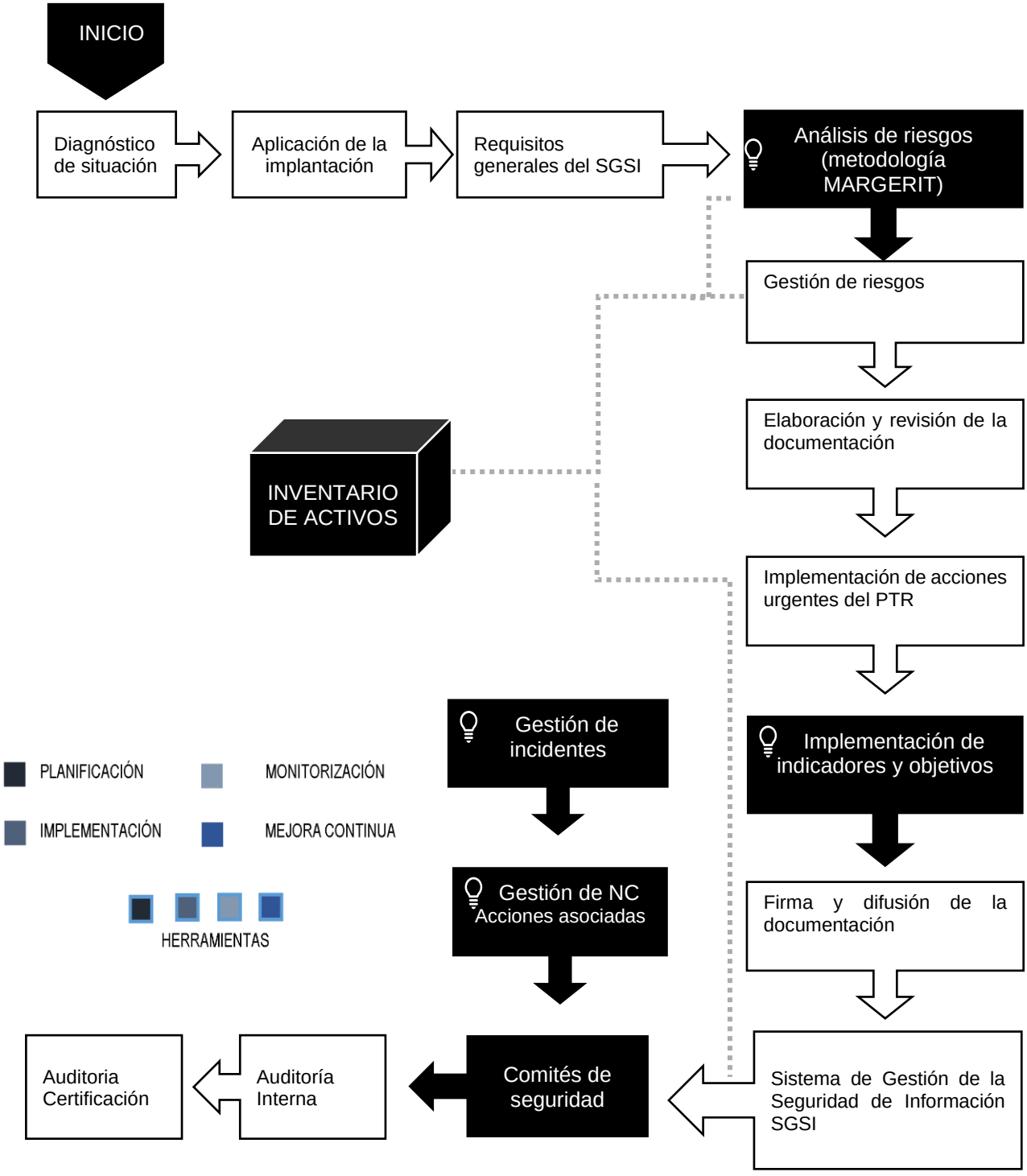


Nota: Elaboración propia, basada en Novoa, 2015.

1.2.2. Modelo Deming de SGSI

Figura 7

Ciclo PDCA detallado de un SGSI



Nota: Elaboración propia información basada en Vidal,2009

1.2.3. Gestión de Riesgos

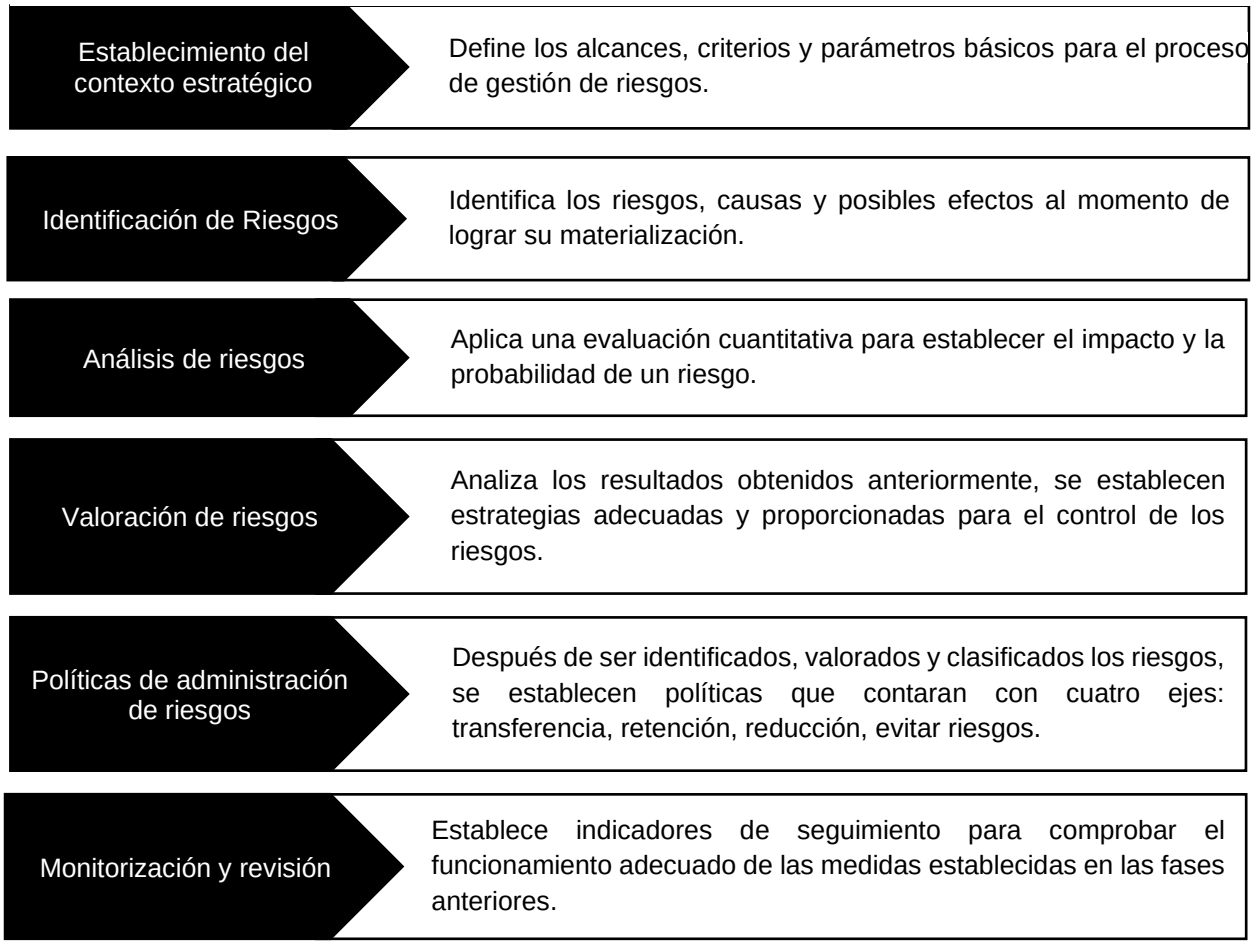
"Risk Management" es un proceso secuencial y estructurado que genera acciones preventivas, correctivas y mitigadoras para reducir riesgos negativos si llega a materializarse. Una buena gestión de riesgos contribuye al cumplimiento de los objetivos establecidos y además favorece totalmente a la organización (Navarro, 2016).

La preparación para auditorías de TI es otra ventaja de la gestión del riesgo. Según Imbaquingo et al. (2020) afirman que " la información es poder " e implementar auditorías de TI dentro de las organizaciones garantizaría esta consideración importante.

La gestión de riesgos se encuentra estructurada por una serie de fases que serán descritas a continuación:

Figura 8

Fases que conforma la gestión de riesgos



Nota. Es indispensable en el análisis de riesgo la calidad de la información que se haya obtenido y la valoración del método de análisis. Elaboración propia información basada en Navarro, 2016

1.3. Activos de la Información

Cualquier información o elemento informático como sistemas, personas, o soportes se consideran activos debido a que tienen un valor representativo para la organización, en cuanto a privacidad de la información, un activo de la seguridad de la Información es toda información pública que el usuario genere, obtenga, transfiere o controle directamente (Suarez, 2015).

Los activos de la información según la ISO 27001:2015, son recursos esenciales del SGSI que necesita una empresa para que logre sus objetivos, además, los activos tienen relación directa o indirecta con las demás entidades como las amenazas, riesgos o vulnerabilidades (MINTIC, 2016).

1.3.1. Clasificación de los activos de la Información

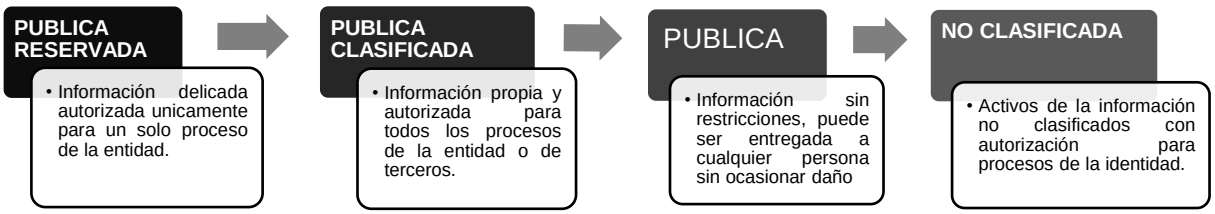
La clasificación de activos de la información ejecuta un procedimiento de la información recibida, puesto a que cada activo tiene su respectiva valoración y característica por lo tanto el manejo es de manera particular (MINTIC, 2016).

Para el sistema de clasificación se toma en cuenta lo recomendado por el MINTIC y la ISO 27001:2015, donde se establece la clasificación de los activos de la información mediante los tres pilares: confidencialidad, integridad y disponibilidad, especificados a continuación:

Conforme a la confidencialidad: En la Figura 9, se puede observar la clasificación de acuerdo con la confidencialidad.

Figura 9

Clasificación de la confidencialidad.

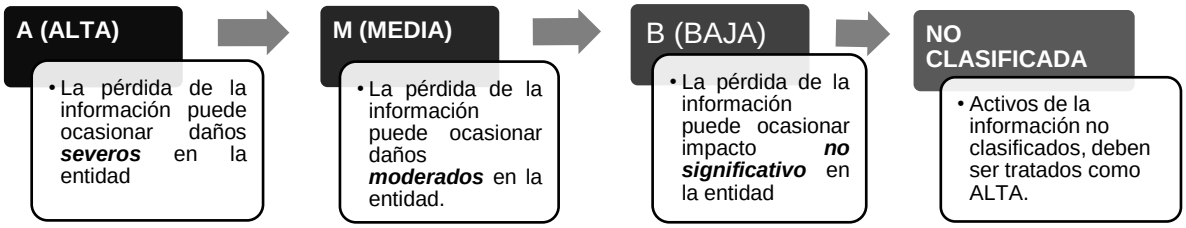


Nota. Elaboración propia información basada en MINTIC,2016

Conforme a la integridad: En la Figura 10 se puede observar la clasificación de acuerdo con la integridad.

Figura 10

Clasificación de la Integridad.

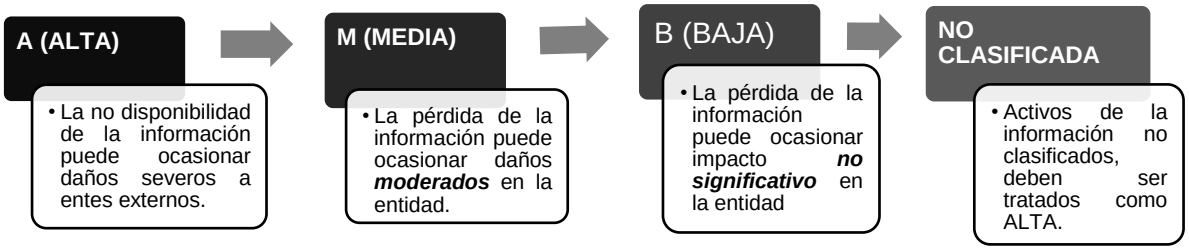


Nota. Elaboración propia información basada en MINTIC,2016

Conforme a la disponibilidad: En la Figura 11 se puede observar la clasificación de acuerdo con la disponibilidad.

Figura 11

Clasificación de la disponibilidad.



Nota. Elaboración propia información basada en MINTIC,2016

1.3.2. Inventario de los activos de la Información

La identificación de activos de la información permite que las organizaciones logren reconocer la relación que cada activo tiene con los procesos organizacionales, cuáles son los

primordiales para el cumplimiento de objetivos estratégicos y cuales resultan fundamentales para la gestión efectiva de la organización (Borrero, 2019) , para ello es indispensable conocer con claridad los tipos de activos que forman parte de la empresa.

Figura 12

Inventario de activos de la información.

Nota. Elaboración propia información basada en MINTIC,2016

1.3.3. Categorización de los activos de la Información

Para la identificación y clasificación de activos mencionados en el punto anterior, resulta indispensable realizar una categorización, así los líderes de proceso podrán determinar con facilidad que activos forman parte de su proceso y de cuales llegan a ser responsables (Borrero, 2019).

Datos: Información generada, recopilada o destruida (manuales, formatos, procedimientos)

Aplicaciones: Software utilizado para la gestión de procesos de la organización.

Hardware: Equipos físicos necesarios para el desarrollo de las actividades diarias de la organización (laptops, terminales, dispositivos móviles)

Tecnología: Equipos indispensables para la gestión y operaciones del personal (impresoras, teléfonos, cableado)

Personal: Corresponde a los colaboradores internos de cada organización es decir al personal indirecto o general que acceden a la información confidencial de la empresa.

Instalaciones: Lugar donde se ubican las oficinas, vehículos, entre otros.

Equipo auxiliar: Agrupación de activos que dan soporte a cada sistema informático y que no forman parte de ninguna de las categorías anteriormente mencionadas (Borrero, 2019).

1.3.4. Criterios de valoración de activos

Cada activo tiene una valoración cualitativa que permite calcular un valor mediante la escala cuantitativa valorando las dimensiones y la importancia en relación con seguridad tal como lo menciona la metodología de MAGERIT v3, basada en la disponibilidad, integridad y confidencialidad.

Se debe tomar en cuenta que por medio del impacto se logra establecer el valor cuantitativo brindado por la metodología que se verá reflejada en la descripción como la gravedad del daño causado por el impacto analizado, teniendo como resultado una homogenización de activos (Suarez, 2015).

1.4. Estándares de la Seguridad de la Información

1.4.1. Las normas ISO 27000

Uno de los requisitos para implementar SGSI en una organización es comprender las normas, su estructura y relaciones entre ellas, estas corresponden a la serie ISO 27000 desarrolladas por la ISO (International Estándar of Organization) y por el IEC (International Electrotechnical Commission).

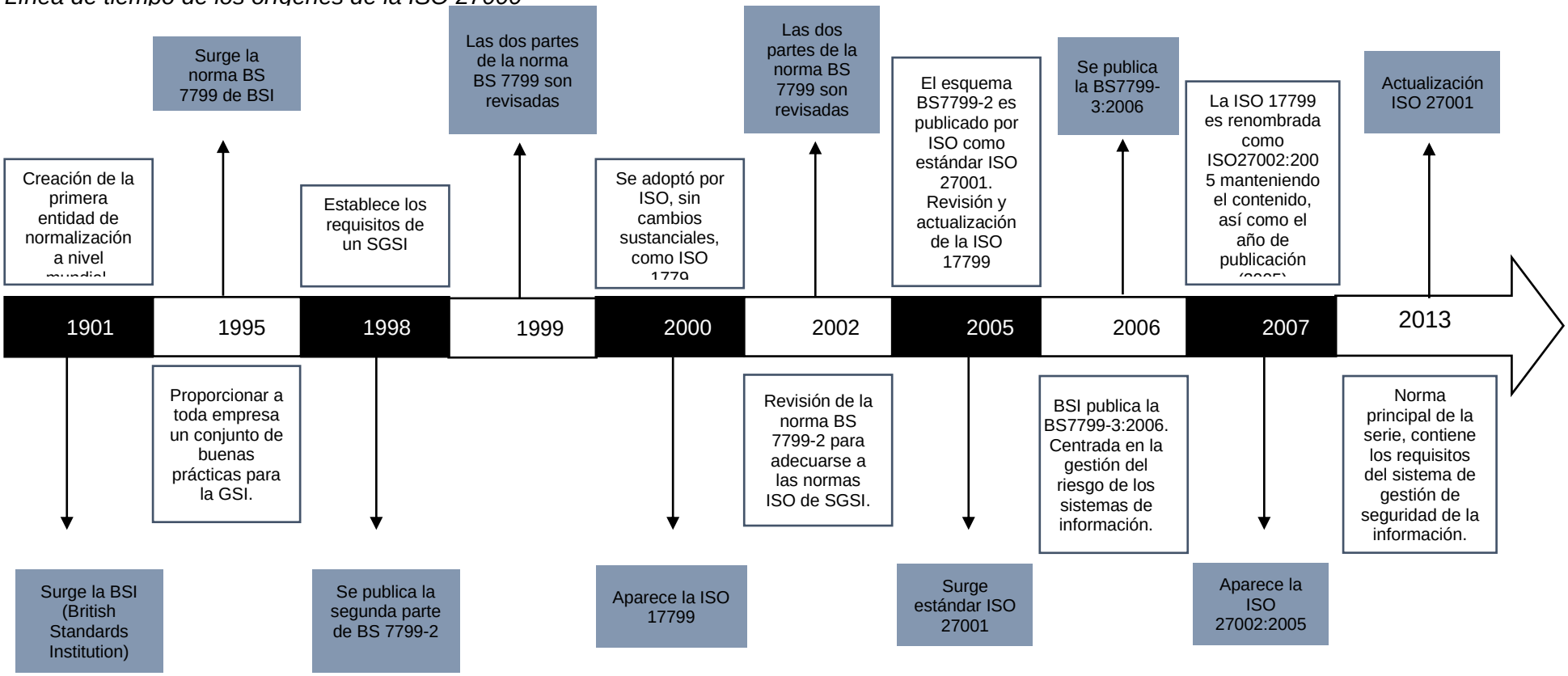
Imbaquingo et al. (2020) menciona que la información es uno de los recursos organizativos más valiosos. Por lo tanto, la existencia de esta familia de normas se vería directamente afectada por la necesidad de garantizar el aseguramiento de la información con SGSI en las áreas de TI.

ISO 27000 es un conjunto de estándares internacionales sobre seguridad de la información que proporciona buenas prácticas para establecer, implementar , y mejorar los Sistemas de Gestión de Seguridad de la Información. (De la Rosa, 2021). Los estándares 27001 y 27002 son los principales pilares de la familia 27000, y la principal distinción entre ellos es que el 27001 se basa en la continua gestión de la seguridad, respaldada por la identificación continua de riesgos. Y 27002 es un estándar de buenas prácticas que enumeran los objetivos de control y gestión que deben perseguir una organización (Cheng et al., 2008).

Estas reglas estandarizadas contienen múltiples prácticas que se pueden utilizar para la seguridad de la información y permiten el desarrollo, la implementación, el mantenimiento y mejora de los sistemas de gestión de seguridad de la información.

Figura 13

Línea de tiempo de los orígenes de la ISO 27000



Nota. Elaboración propia información basada en ISO 27000,2018

(https://www.iso27000.es/iso27000.html)

1.4.2. Objetivos de la norma ISO 27000

Internamente se tiene los siguientes objetivos de la norma ISO 27000:2018

- Optimizar los niveles de seguridad de sistemas, redes, dispositivos, información de entidades, datos de usuarios y personal de trabajo, mediante el uso de controles de análisis de riesgos.
- Preparar recomendaciones útiles para los oficiales de seguridad de la información o personas a cargo.
- Crear un plan de contingencia estratégico para ayudar a resolver cualquier amenaza o ataque que pueda detectarse en su sistema e intente ejecutarlo con el menor tiempo de respuesta posible.
- Capacitar a los empleados para que reconozcan la importancia de la seguridad de la información como un activo crítico de la empresa o institución y fomentar la familiarización con la norma ISO 27000:2018.
- Elaborar y mantener la documentación de los procesos realizados en el SGSI.
- Monitorear y verificar continuamente, o mejorar según sea necesario, la aplicación de las recomendaciones basadas en la norma ISO 27000:2018 (ISO/IEC, 2018) .

1.4.3. Beneficios de la norma ISO 27000:2018

A continuación, se muestran algunos de los beneficios que una organización puede lograr al implementar el conjunto de normas ISO 27000:2018.

- Mejorar la imagen de la organización y las relaciones con terceros, esto permite que sus partes interesadas sepan que la seguridad es una de las prioridades de su organización.
- Administrar registros de incidentes y vulnerabilidades.
- Reducir el riesgo de pérdida, robo o daño de la información.

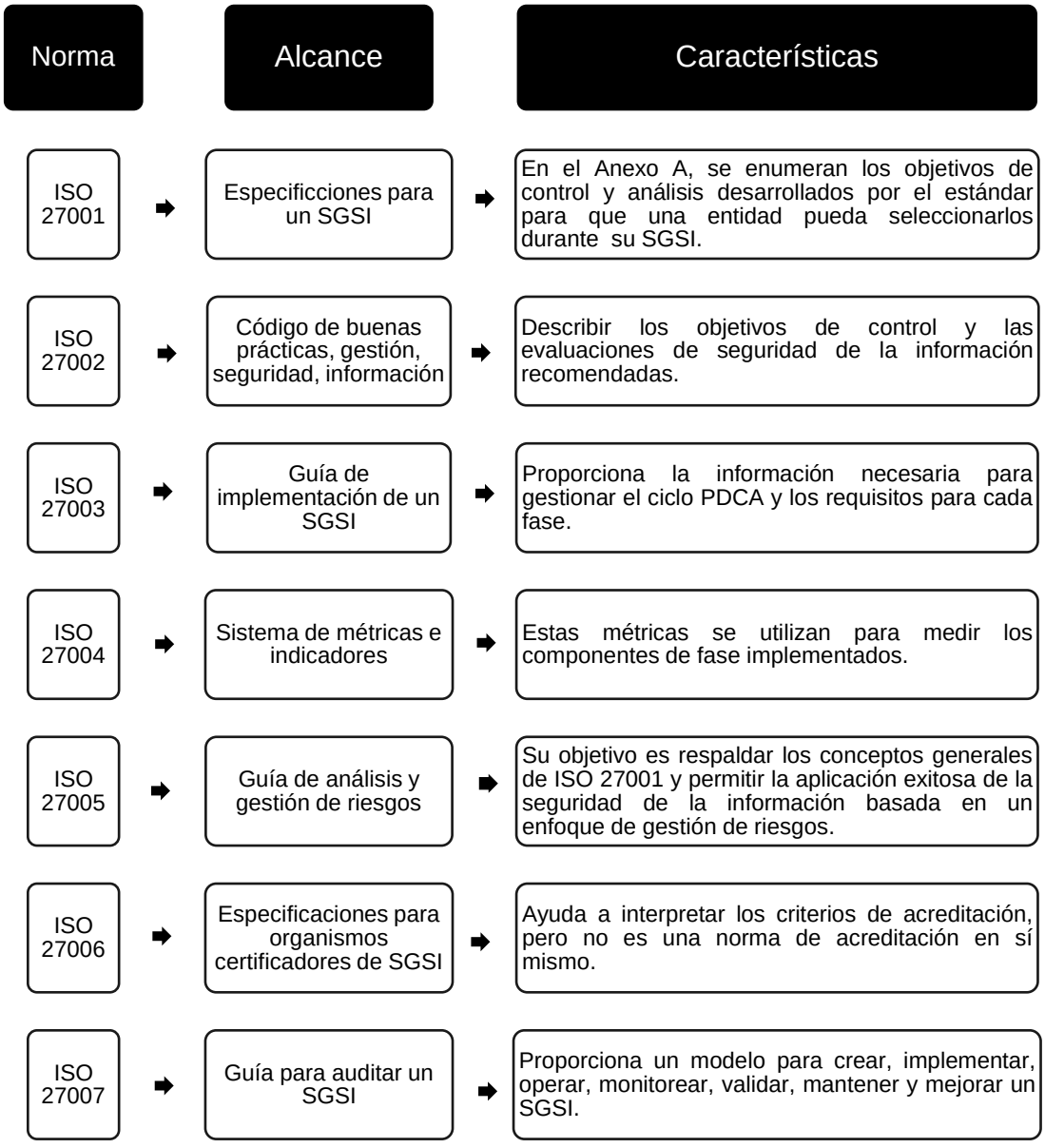
- Cumplir con las leyes aplicables en materia de datos personales, propiedad intelectual.
- Permite la revisión continua de controles y riesgos.
- Utilizar auditorías externas para ayudar a identificar las debilidades del sistema y las áreas de mejora.
- Brinda confianza y ayuda a establecer reglas claras a seguir por los miembros de la organización (ISO/IEC, 2018).

1.4.4. Introducción de los estándares ISO 27000:2018

En algunas implementaciones de SGSI, como fue el caso en relación con este proyecto de titulación, puede ser posible aplicar solo ciertos estándares de familia y no todos, porque las implementaciones de toda la familia pueden ser improductivas.

Figura 14

Estándares de la familia ISO 27000



Nota. Elaboración propia información basada en MINTIC,2016

Como podemos ver en la tabla de la Figura 14, hay varios estándares relacionados con esta familia que se complementan, es por esto por lo que el estándar 27001:2013 definirá las implementaciones del SGSI es el único certificable bajo el Anexo A.

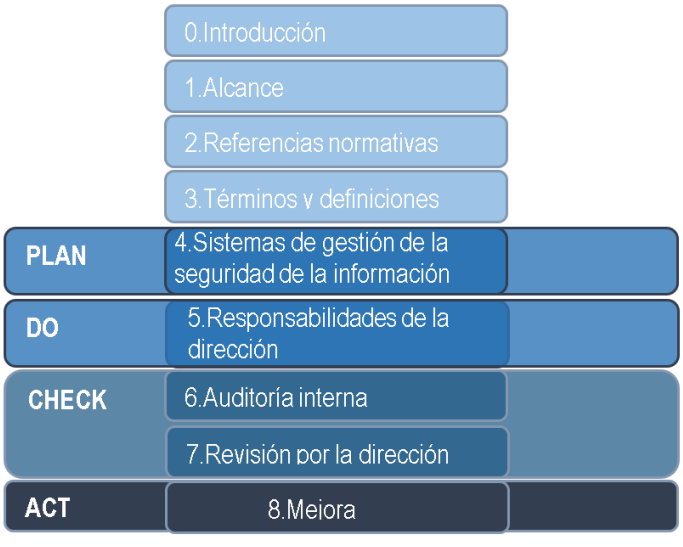
El estándar 27000:2018, describe la importancia de implementar un sistema de gestión de seguridad de la información, una descripción general del mismo y los pasos que debe seguir cualquier empresa u organización que desee certificarse en esta familia de estándares ISO.

1.4.5. Estándares Internacionales ISO 27001:2005

Este es el estándar principal en esta familia de estándares y describe los requisitos para los sistemas de gestión de seguridad de la información, Esta es la primera versión de este estándar publicada en 2005 y reemplazó al estándar BS 7799:2 utilizado anteriormente para la gestión de la seguridad de la información., también es el predecesor del estándar que se utilizará en este proyecto de titulación, por lo que el análisis estructural se realizará mediante la actualización 2013. La estructura que seguía la norma ISO 27001:2005 se muestra a continuación:

Figura 15

Estructura de la ISO 27001:2005



Nota: Elaboración propia.

1.4.6. Introducción a la norma ISO/IEC 27001/2013

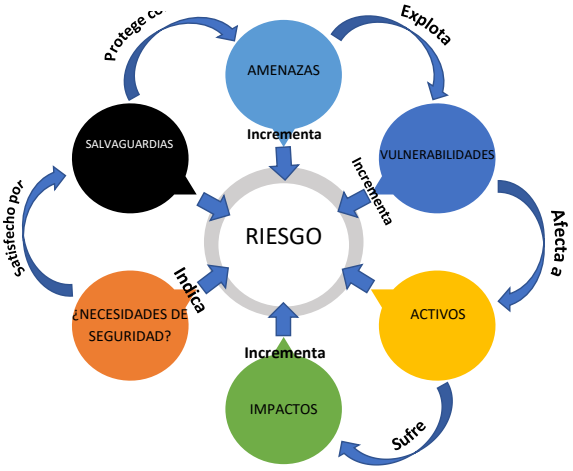
Este estándar fue desarrollado para proporcionar un modelo para establecer, implementar, operar, monitorear, validar, mantener y mejorar un SGSI. La implementación de un SGSI es una decisión estratégica para una unidad o institución. El diseño y la implementación del SGSI de una organización están influenciados por las necesidades y los objetivos, los requisitos de seguridad, los procesos utilizados, el tamaño y la estructura de la organización (Villacís, 2016).

El enfoque de este proceso en los estándares internacionales permite a los usuarios enfatizar la importancia de:

- Comprender los requisitos de seguridad de la información de su organización y la necesidad de establecer esas políticas y objetivos.
- Implementar y operar controles para mitigar los riesgos de seguridad de la información.
- Supervisar y revisar el desempeño y la eficacia del SGSI.
- Sugerir mejora continua basada en la medición de objetivo (Mujica, 2015).

Figura 16

Análisis del impacto de riesgo



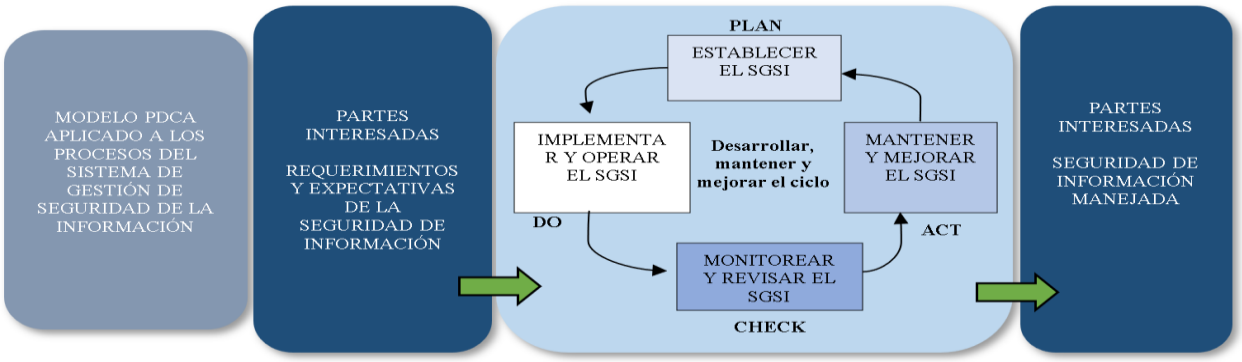
Nota: Elaboración propia.

Con este fin, la Figura 16 describe el impacto del riesgo en una organización y muestra la necesidad de implementar un SGSI.

El estándar internacional que se está tratando adopta el modelo de proceso PDCA (Planear-Hacer-Chequear-Actuar), el mismo que toma como insumo los requerimientos y expectativas de la seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que satisfacen aquellos requerimientos y expectativas. La Figura 17, muestra el esquema adoptado en la norma con el modelo PDCA.

Figura 17

Esquema con modelo PDCA



Nota: Elaboración propia.

Cabe tomar en cuenta que este estándar es aplicable a todo tipo de organizaciones, incluidas empresas comerciales, agencias gubernamentales y organizaciones sin fines de lucro (Villacís, 2016).

El proceso de evolución de la norma ISO 27001: 2005 a la norma ISO 27001: 2013 identifica diferencias en el índice de cada norma. Estas diferencias también se encuentran esencialmente en la eliminación de los Anexos B y C de la norma de 2005.

Algunos de los títulos de los contenidos han cambiado, y esto es evidente en la edición de 2013, que muestra criterios como organización, liderazgo, planificación, soporte y operaciones.

La nueva estructura de la ISO 27001:2013 se indica a continuación en la Figura 18.

Figura 18

Estructura de la ISO 27001:2013

Nota: Elaboración propia.

Así como podemos mostrar las diferencias en el Anexo A, de cada estándar en la Figura 19, la principal diferencia es el número de objetivos de control. Tomando en cuenta que la versión de 2005 tiene 11 objetivos de control, mientras que la versión de 2013 tiene 14. Para ello se han eliminado algunos controles de la versión 2005, se han consolidado otros y se han creado unos

controles nuevos. Este apéndice es de primordial importancia puesto a que es el conjunto de objetivos de control y controles que propone la norma para mitigar las amenazas.

Figura 19

Diferencias en el Anexo A de cada norma

Anexo A ISO 27001:2005 Objetivos de control	Anexo A ISO 27001:2013 Objetivos de control
• A.5 Política de seguridad • A.6 Organización de la seguridad de la información • A.7 Gestión de activos • A.8 Seguridad de los RRHH. • A.9 Seguridad física y del entorno • A.10 Gestión de comunicaciones y operaciones • A.11 Control de acceso • A.12 Adquisición, desarrollo y mantenimiento de sistemas de información. • A.13 Gestión de incidentes de la seguridad de la información. • A.14 Gestión de la continuidad del negocio. • A.15 Cumplimiento.	• A.5 Políticas de seguridad • A.6 Organización de la información • A.7 Seguridad en recursos humanos. • A.8 Gestión de activos • A.9 Control de accesos. • A.10 Criptología • A.11 Seguridad física y ambiental. • A.12 Seguridad en las operaciones. • A.13 Transferencia de información. • A.14 Adquisición de sistemas, desarrollo y mantenimiento. • A.15 Relación con proveedores. • A.16 Gestión de los incidentes de seguridad. • A.17 Continuidad de negocio. • A.18 Cumplimiento con requerimientos legales y contractuales.

Nota: Elaboración propia.

1.4.7. Alcance de la norma ISO/IEC 27001/2013

Garantiza una óptima selección de controles de seguridad y protección de información de las partes interesadas de una empresa, además, la norma es una herramienta para determinar el grado de cumplimiento de la norma de ayuda aplicada en auditores internos y externos (Recalde, 2019).

La norma incorpora el siguiente proceso:

- Establece objetivos para la seguridad de la información.
- Resuelve los riesgos de la mejor más optima.

- Verifica la legalidad de cumplimiento en cada país.
- Gestiona los controles de seguridad para cumplir los objetivos específicos de la organización.
- Determina cuales son los procesos críticos de la organización para gestionar la seguridad de la información.
- Provee a clientes y proveedores la información más relevante sobre seguridad de la información.
- Asegura una adecuada administración de los recursos que conforma la organización.

1.5. Metodologías para la gestión de riesgos

Según Viguri (2021), en vista de la necesidad actual de implementar el proceso de Gestión de Riesgos en las organizaciones, los responsables de este proceso han reconocido la importancia de encontrar métodos que simplifiquen y uniformicen dicho proceso. Debido a esta necesidad, varios organismos internacionales han creado diversos estándares y metodologías para homogeneizar lo que se considera una "buena práctica en la gestión de riesgos"

1.5.1. ISO/IEC 27005/2018

La norma ISO/IEC 27005:2018 establece las directrices indispensables y el proceso a emplearse para la gestión del riesgo en la seguridad de la información, asimismo es un soporte a los conceptos generales de la norma ISO/IEC 27001. La ventaja de la norma es que su aplicación no tiene restricciones, puede ser aplicada a todo tipo de organizaciones siempre y cuando tengan la intención clara de gestionar los riesgos que claramente causarían inconvenientes a la seguridad de la información de la empresa u organización (Castillo & Molina, 2020).

1.5.2. OCTAVE

Es una metodología autodirigida por el “equipo de análisis” que facilita el estudio de la evaluación de riesgos organizacionales enfocándose en evaluar aspectos diarios de una organización para ello OCTAVE estudia la infraestructura de información y la manera de funcionalidad mediante los elementos “TI” es decir los activos de la información que son de gran importancia como software, archivos físicos o sistemas informáticos. Es importante que los empleados conozcan que activos informáticos son importantes y cuál es la manera de protegerlos por esta razón en la evaluación mencionada anteriormente debe estar involucradas personas estratégicas para cada nivel de la empresa (López, 2016).

El proceso que debe realizar el equipo de análisis y personal de cada nivel de la empresa se divide en tres fases:

- **PRIMERA FASE:** Construir perfiles de amenazas basadas en los activos.
- **SEGUNDA FASE:** Identificar vulnerabilidades en la información.
- **TERCERA FASE:** Desarrollar estrategias y planes de seguridad.

1.5.3. NIST 800-30 (National Institute of Standards and Technology)

La NIST 800-30 es una guía que brinda apoyo en los procesos de valoración y mitigación dentro de la gestión de riesgos, en la metodología se aplican nueve pasos de evaluación de riesgos, sin embargo, para la aplicación cada paso debe ser modificado de acuerdo con el riesgo que la identidad desee e incluso puede reducirse el proceso al realizarse pasos de manera simultánea.

La gestión de riesgos es indispensable para la protección de los activos de la organización, debido a que ayuda a reconocer cuales son las vulnerabilidades desarrolladas frente a las amenazas, calcula el riesgo existente de un posible impacto sobre el activo y por supuesto identifica todos los activos encontrados en una organización. Con lo mencionado anteriormente, el responsable de seguridad con toda la información brindada es capaz de tomar

decisiones pertinentes para gestionar optimas medidas de seguridad frete al riesgo-inversión (NIST, 2018).

1.5.4. CRAMM

Metodología orientada al análisis y gestión de riesgos, la cual es destinada a proteger la integridad, confidencialidad y disponibilidad de activos y la información de un sistema. Su aplicación es para todo tipo de sistemas y redes informáticas siempre y cuando se encuentren en la fase de factibilidad debido a que su objetivo es identificar las vulnerabilidades, amenazas y posteriormente evaluar los niveles de cada riesgo encontrado (López, 2016).

Para que el nivel de riesgo pase de elevado a aceptable se consideran las siguientes tres etapas:

Figura 20

Etapas aplicadas en CRAMM.

Nota: Elaboración propia.

1.5.5. MAGERIT v3

Es una metodología sistemática de análisis y gestión de riesgos que contribuye a la seguridad informática de una organización a través de un análisis de riesgos existentes que facilita la identificación de amenazas en el sistema de información y determina la vulnerabilidad de dichas amenazas. Los resultados obtenidos permiten proceder de manera apropiada para prevenir, reducir, conocer, impedir o controlar a tiempo los riesgos encontrados e impedir problemas irreversibles dentro del entorno y organización. El objetivo de MAGERIT v3 es recalcar la existencia de riesgos a todos los responsables de las organizaciones y como deben ser

gestionados los riesgos para que no se generen ataques a los activos de la información(Fernández, 2021).

Tabla 1

Metodologías de análisis de riesgos

METODOLOGÍAS	CARACTERÍSTICAS	VENTAJAS	DESVENTAJAS
ISO / IEC 27005:2018	Determina las directrices para la gestión de riesgos, basados en ISO 27001. Aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que pueden afectar irreparablemente.	Es un estándar internacional orientado a la gestión de riesgos de la seguridad de la información. Tiene un alcance completo, tanto en el análisis como en la gestión de riesgos.	No es certificable. No brinda detalles para la valoración de las amenazas. No posee herramientas que sirvan de ayuda para su implementación.
OCTAVE	Metodología flexible y auto dirigida que optimiza los procesos de evaluación de riesgos Clasifica a los componentes de la organización en activos tomando en cuenta su importancia. Estudia la infraestructura de información y el uso.	Todo el personal de la organización es tomado en cuenta. Para el modelo de análisis involucra los siguientes elementos: procesos, activos, dependencias, recursos, vulnerabilidades, amenazas y salvaguardas.	No detalla la clasificación de los activos de información. Utiliza documentación anexa que limita la eficacia de aplicación. No identifica oportunamente los riesgos importantes para la organización.
NIST SP 800-30	Estándar desarrollado por el (NIST), para la valoración y mitigación de los riesgos de seguridad en las infraestructuras de TI. Provee los fundamentos necesarios para un programa de administración de riesgos.	Guía Asegura los sistemas informáticos que almacenan, procesan y transmiten información. Mejora la administración a partir de los resultados del análisis de riesgos.	En el modelo no tiene contemplados elementos como los procesos, los activos ni las dependencias. Problemas con empresas pequeñas por las altas limitaciones de recursos humanos.
CRAMM	Es una metodología de análisis de riesgos, desarrollada por el (CCTA) del gobierno del Reino Unido Identifica y evalúa amenazas y vulnerabilidades, así como los niveles de riesgos.	Brinda confidencialidad, integridad y disponibilidad de los sistemas de información mediante el uso de una evaluación mixta. Identifica y clasifica los activos de TI	No contempla elementos importantes como los procesos y los recursos.
MAGERIT	Es una metodología de análisis y gestión de riesgos de la información desarrollada por el consejo superior de administración electrónica. Tiene el propósito de establecer principios para el uso eficaz, eficiente y aceptable de las TI.	Ayuda a planificar las medidas para mantener los riesgos bajo control. Apoya la preparación de la organización para procesos de evaluación, auditoría, o certificación. Posee un extenso archivo de inventarios sobre amenazas y tipo de activos.	No involucra a los procesos, recursos ni vulnerabilidades como elementos del modelo a seguir. No posee un inventario completo en lo referente a políticas.

Nota. Elaboración propia, 2022

CAPÍTULO 2

Diseño del Sistema de Gestión de Seguridad de la Información

2.1. Aspectos Generales

A continuación, se describe los aspectos generales del Departamento de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte, esta información es relevante y concisa sobre varios aspectos clave.

2.1.1. Filosofía

La Dirección de Desarrollo Tecnológico e Informático, está en constante búsqueda de nuevas tecnologías de información y comunicación de la más alta calidad y con la constante preocupación por la actualización tecnológica para el mejoramiento continuo en todos los procesos de la Universidad Técnica del Norte.

2.1.2. Misión

La Dirección de Desarrollo Tecnológico e Informático, gestiona el desarrollo de la infraestructura tecnológica y TIC`s como herramientas de apoyo al servicio de la investigación, docencia, vinculación y gestión universitaria en temas del área como soporte informático de todos los servicios tecnológicos, adecuada circulación interna y externa de la información, proyectos innovadores de tecnologías de redes y desarrollo de software.

2.1.3. Visión

La Dirección de Desarrollo Tecnológico e Informático en el año 2023, contará con 95% de procesos automatizados con herramientas de inteligencia de negocios, permitiendo el 100% de uso de los módulos que conforman el SIIU, nuevos servicios tecnológicos y certificación de la ISO 29110 de desarrollo; fortalecer el funcionamiento del SIIU en el CLOUD y proveer 90% de cobertura de red inalámbrica a los campus universitarios.

2.1.4. Objetivos Estratégicos Institucionales

Objetivo Estratégico 1 - Eje Académico

Fortalecer la calidad de la educación, a través de una formación integral con pertinencia científica y social.

Objetivo Estratégico 2 - Eje Investigación

Fortalecer las políticas de investigación científica y tecnológica articulada a la formación profesional y vinculación con la Sociedad.

Objetivo Estratégico 3 - Eje Vinculación

Desarrollar programas de vinculación con la Sociedad, articulados a la docencia e investigación con responsabilidad social y ambiental que garanticen pertinencia e impacto nacional e internacional.

Objetivo Estratégico 4 - Eje Gestión

Tecnificar la gestión institucional con la aplicación de un modelo y sistema de gestión por procesos.

El DDTI en su Plan Estratégico se acoge al Objetivo Estratégico 4 del Plan Estratégico Prospectivo de Desarrollo Institucional de la Universidad Técnica del Norte mediante la política 4.4. que menciona “Implementar mecanismos para un modelo de gestión por procesos y servicios tecnológicos de acceso abierto al conocimiento a través de herramientas y recursos de aprendizaje”, con las siguientes líneas de estrategia:

- Establecer normas y protocolos de desarrollo para la automatización de procesos y políticas de responsabilidad, términos y condiciones de uso del SIIU, para la Gestión por procesos y por resultados de la UTN.
- Garantizar el servicio en la nube de herramientas de colaboración y el desarrollo de productos de software.
- Gestionar información coherente, concordante, suficiente y competente para uso institucional y de organismos externos.

- Capacitar de manera especializada a los funcionarios del DDTI para incrementar la productividad de los servicios tecnológicos.
- Optimizar la infraestructura tecnológica de la UTN para mejorar los servicios de la comunidad universitaria, difundir y ampliar el conocimiento a través de comunidades de aprendizaje, recursos y acceso tecnológico.
- Ampliar las habilidades para el uso de las TICs en el desarrollo de los procesos de formación, investigación, vinculación y gestión universitarias.
- Difundir y ampliar la información pública de la UTN a través de su portal web.
- Estandarizar los productos de software desarrollados para mejorar la calidad y seguridad de los servicios tecnológicos brindados a la comunidad universitaria

2.1.5. Valores

Calidad. Nuestros proyectos elaborados con calidad y actitud de servicio con la Universidad Técnica del Norte.

Responsabilidad. Cumplimos nuestros proyectos con responsabilidad, creando confianza en nuestros colaboradores

Creatividad. Aporte de ideas innovadoras para optimización de los procesos institucionales.

Liderazgo. Nuestro compromiso es realizar las actividades con eficiencia, comprometimiento para brindar un aporte generador de valor en las gestiones institucionales.

Trabajo en equipo. Sumamos esfuerzos y talentos para lograr nuestros objetivos y ayudarnos unos a otros.

Honestidad. Nos basamos en los reglamentos que gobiernan a la Universidad y el estatuto propio de nuestra Institución para trabajar con armonía, verdad, respeto y lealtad.

2.1.6. Directivos

Según la página web oficial de la UTN, los directivos actuales del DDTI se conforman como se indica en la Tabla 2:

Tabla 2

Directivos

DIRECTIVOS UTN
Rector
Vicerrectora Académica
Vicerrectora de Investigación
Vicerrector Administrativo
DIRECTIVOS DDTI
Director de Desarrollo Tecnológico e Informático
Sub director de Desarrollo Tecnológico e Informático
Desarrollo de Software
Comunicaciones y Redes
Atención al Usuario

Nota. Elaboración propia, 2022

2.2. Identificación del Problema

La UTN ha empleado innovadoras tecnologías a través del DDTI para la automatización de procesos y la digitalización de su información. Ubicada en la Av. 17 de Julio 5-21, en el cantón Ibarra, esta prestigiosa institución universitaria ha mejorado significativamente su infraestructura tecnológica en los últimos años. Además, ha implementado nuevos servicios, tales como la gestión en línea de usuarios, el acceso a repositorios digitales, y el almacenamiento digital de información delicada de estudiantes, docentes y personal administrativo.

La implementación de servicios innovadores que elevan el nivel de atención al usuario también conlleva la aparición de posibles vulnerabilidades de seguridad en la información, que pueden ser resultado de errores humanos, defectos en los sistemas, conductas maliciosas o intencionales. Estas amenazas presentan un riesgo significativo, como el acceso ilícito a información tanto física como digital, el uso no autorizado de sistemas informáticos, la

manipulación o sustracción de datos, y la suplantación de identidad, entre otras consecuencias graves.

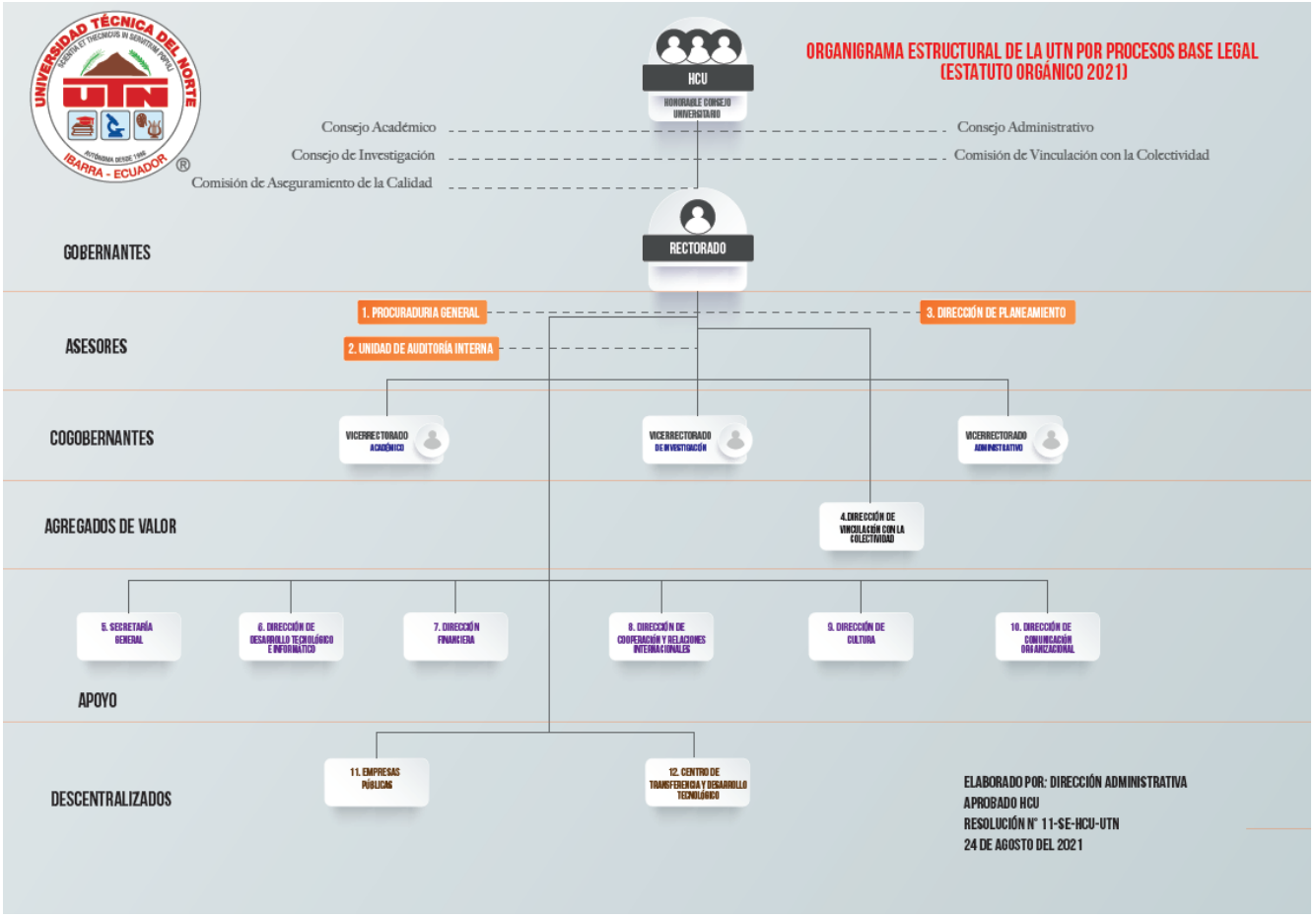
Sin embargo, a pesar de utilizar tecnologías que permiten la automatización de los procesos, la institución de educación superior carece de un Sistema de Gestión de la Seguridad de la Información (SGSI) que satisfaga sus necesidades específicas, lo que aumenta significativamente el riesgo de ataques que comprometan la seguridad de la información. El Departamento de Desarrollo Tecnológico e Informático (DDTI) tiene la responsabilidad de establecer políticas de seguridad de la información en toda la institución.

2.3. Estructura Orgánica

Nota: Tomado de Estructura Organizacional, por Universidad Técnica del Norte, 2021

Figura 21

Organigrama Estructural UTN 2021



Nota. Tomado de Estructura Organizacional, por Universidad Técnica del Norte, 2021, UTN (https://www.utn.edu.ec/estructura-organizacional/).

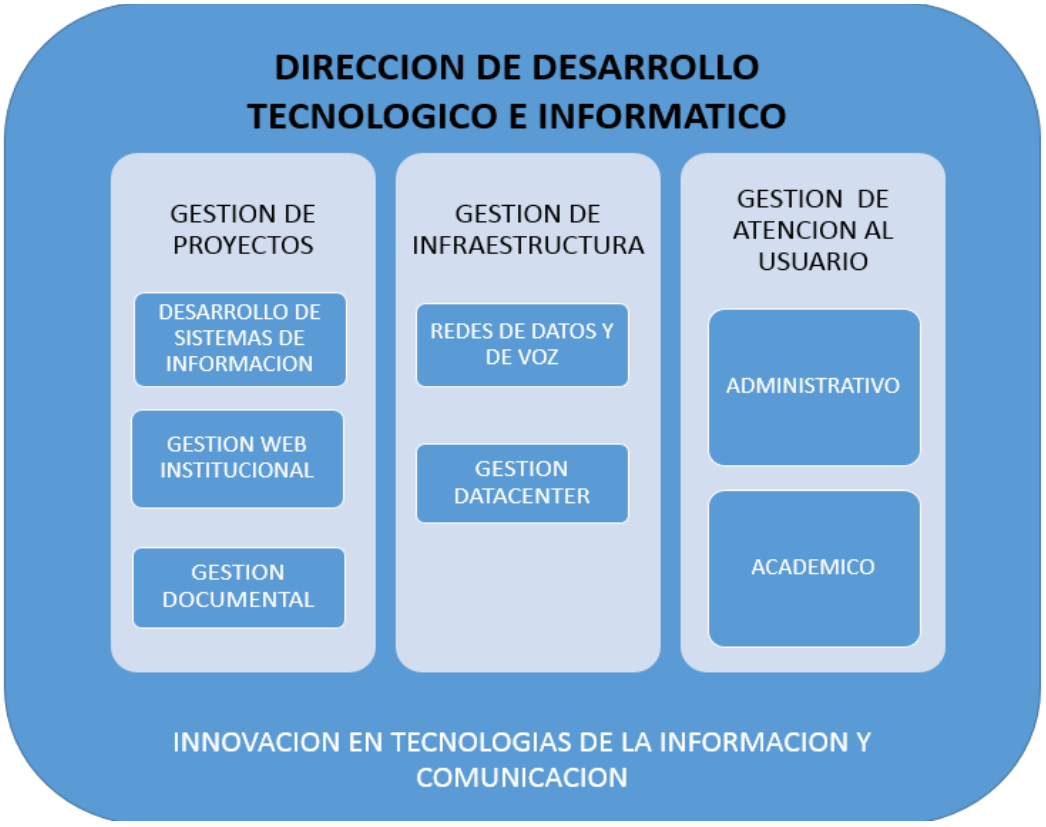
Organigrama interno del DDTI

El DDTI se divide en tres unidades, en las cuales se conforman con áreas que se organizan para cumplir los objetivos estratégicos de la institución y de esta manera apoyar para conservar la continuidad de la institución. La primera unidad es Gestión de Proyectos y se conforma por las áreas de: “Desarrollo de Sistemas de Información”, “Gestión Web Institucional” y “Gestión Documental”. Por otra parte, se tiene la Unidad de Gestión de Infraestructura conformada por las áreas de: “Redes de Datos y Voz” y “Gestión Data Center”.

Finalmente, la Unidad de Gestión de Atención al Usuario que engloba las áreas de: “Administrativo” y “Académico”.

Figura 22

Organigrama interno del DDTI.



Nota. Elaboración propia, 2022

2.4. Regulaciones de Seguridad Aplicables

El DDTI de la UTN, al pertenecer a una institución pública se rige por las siguientes normativas nacionales:

2.4.1. Normas emitidas por la Contraloría General del Estado

Son un conjunto hola manejo correcto de los recursos públicos. Consta de 17 puntos que hacen referencia a como la empresa debe cumplir con todos los puntos para fortalecer el área de tecnología (CONTRALORÍA GENERAL DEL ESTADO, 2014).

2.4.2. Constitución de la República del Ecuador

Esta norma jurídica suprema se compone de 444 artículos, los cuales están divididos en 9 títulos que a su vez se subdividen en capítulos; sin embargo, según su estudio, está dividido en la parte dogmática en la cual se encuentra Honda mentales y las garantías jurisdiccionales, y la parte orgánica en la cual organiza la estructura del Estado (CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, 2021).

2.4.3. Ley de Transparencia y acceso a la Información Pública

La Ley Orgánica de transparencia y acceso a la información pública (LOTAIP) tiene por objeto hacer efectivo el principio de publicidad de los actos, contratos y gestiones de las instituciones Del Estado y de aquellas financiadas con recursos públicos que por su naturaleza sean de interés público, además que garantiza y norma el ejercicio del derecho fundamental de las personas a la información (LEY ORGANICA DE TRANSPARENCIA Y ACCESO A LA INFORMACION PUBLICA, 2004).

2.4.4. Esquema Gubernamental de Seguridad de la Información (EGSI) – Acuerdo N° 025 del 09 de septiembre del 2019

El EGSI establece un conjunto de directrices Gestión de la Seguridad de la Información e inicia un proceso de mejora continua en las instituciones de la Administración Pública. este

esquema gubernamental no reemplaza la norma ISO/IEC 27001 sino que marca como prioridad la implementación de algunas directrices (Registro Oficial, 2020).

Su implementación incrementará la seguridad de la información en las entidades públicas, así como la confianza de los ciudadanos en la Administración Pública.

2.5. Departamento de Desarrollo Tecnológico e Informático

2.5.1. Procesos Críticos

Los procesos críticos son aquellos que añaden valor y están estrechamente vinculados con la orientación estratégica de la institución, garantizando su continuidad operativa. Dentro del marco del DDTI, se identifican como procesos críticos los siguientes:

Proceso de Base de datos: el propósito de este proceso es integrar y unificar la información producida por los distintos procesos administrativos, docentes y estudiantiles de esta institución universitaria, utilizando los diversos sistemas disponibles en esta sede académica.

Proceso de Redes: se refiere a un procedimiento que tiene como objetivo facilitar la interacción de los usuarios con los diversos recursos tecnológicos que la institución pone a su disposición, así como también establecer la comunicación entre la institución y otras entidades o individuos externos.

2.5.2. Estado Actual de la Seguridad

Para conocer el estado actual de la seguridad se realizó una entrevista al Ing. Juan Carlos García sub director del DDTI, en el Anexo 2 se encuentra el esquema de la entrevista y a continuación los resultados obtenidos de esta.

El DDTI de la UTN presenta un nivel significativo de no conformidad en relación con las regulaciones establecidas por la norma ISO/IEC 27001:2013. Los aspectos más relevantes que reflejan esta situación son los siguientes, en resumen:

- El diseño de un sistema de gestión de seguridad de la información no ha sido implementado.

- La institución no dispone de políticas de seguridad de la información disponibles al público.
- No hay una unidad especializada que tenga la responsabilidad exclusiva de manejar los asuntos relacionados con la protección y la salvaguarda de la información.
- La responsabilidad específica por cada activo de información no se encuentra claramente definida.
- No se realiza una gestión adecuada de los recursos de información en función de su importancia o nivel de criticidad.

Se han llevado a cabo ciertas acciones de manera no estructurada, entre las que se incluyen:

- Existe un procedimiento por el cual se conceden o retiran los permisos de acceso a los usuarios para todos los sistemas y servicios que son ofrecidos por el área en cuestión.
- Se ha llevado a cabo la fase inicial de recopilación de información sobre los activos de datos, donde se ha elaborado un inventario de estos.
- La instalación de un sistema de protección de red (firewall) con el objetivo de asegurar la integridad y privacidad de los datos es una medida esencial en la gestión de la seguridad informática.

2.5.3. Identificación de controles existentes

Anteriormente, se informó sobre la situación del DDTI en términos de seguridad de la información, demostrando que, aunque no disponen de documentación detallada sobre los controles y planes para implementar el tratamiento de riesgos, la institución lleva a cabo ciertas actividades de control que contribuyen de alguna manera a reducir la probabilidad de que una

amenaza se concretice y afecte un activo en particular. Estas actividades se detallan en la Tabla 3.

Tabla 3

Controles existentes en el DDTI

Amenazas	Controles implementados existentes
Naturales, Físicas o Ambientales	Planta Alterna
	Sistema de energía Estabilizada UPS
	Sistema de Climatización
	Backups
	Acceso Personal Autorizado. Controles de acceso físico
Humanas o Accidentales	Firewall
	Antivirus
	Capacitación
Técnicas	Personal capacitado para brindar soporte
Organizacionales	Licencias adquiridas para el DDTI

Nota. Elaboración propia, 2022

2.6. Consideraciones Iniciales

2.6.1. Definición de alcance y objetivos del SGSI

En consonancia con los requerimientos específicos de la institución, en este caso, el Departamento de Desarrollo Tecnológico e Informático (DDTI) de la Universidad Técnica del Norte (UTN), se precisa establecer los límites y la relevancia en relación con el sistema de gestión de seguridad de la información.

Alcance del SGSI

Este proyecto ha sido creado con el fin de diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) específico para el almacenamiento de información en el Departamento de Desarrollo Tecnológico e Informático (DDTI) de la Universidad Técnica del Norte (UTN). El diseño del SGSI establece un conjunto de políticas y controles para proteger los activos de información del departamento, considerando la importancia vital de los servicios que brinda en la

institución, los cuales son esenciales para el correcto desempeño de sus actividades, servicios y procesos.

Objetivos del SGSI

• Ob1: Garantizar la protección de los recursos de información que forman parte del DDTI de la Universidad Técnica del Norte (UTN).

• Ob2: Establecer medidas de seguridad efectivas para proteger los activos de información, con el fin de garantizar la confidencialidad, integridad y disponibilidad de dichos activos.

• Ob3: Contribuir al cumplimiento de la misión y de los objetivos fundamentales de la institución mediante una gestión adecuada de los riesgos asociados a la seguridad de la información.

2.6.2. Partes Interesadas

Las partes involucradas en la creación del diseño del SGSI se mencionan a continuación:

U.T.N. : A pesar de los avances en la infraestructura tecnológica de la institución, que han permitido ofrecer nuevos servicios, no cuenta con un Sistema de Gestión de Seguridad de la Información que satisfaga sus requerimientos, lo que aumenta el peligro de sufrir ataques que puedan vulnerar la seguridad de sus activos.

DDTI: En la actualidad, este departamento es responsable de establecer las normas de seguridad de la información para toda la institución.

Autor del Proyecto: Alumno de la Universidad Técnica del Norte que cursa la carrera de Ingeniería en Software, se encuentra trabajando en el Departamento de Desarrollo Tecnológico e Informático de la UTN para el diseño de un Sistema de Gestión de la Seguridad de la Información que satisfaga las necesidades de la institución de educación superior.

2.6.3. Necesidad para diseñar un SGSI

Diariamente, los especialistas en tecnología de la información se enfrentan a un entorno lleno de peligros que comprometen los bienes de su entidad, debido al gran volumen de datos

cruciales que se manejan dentro de ella. Es por esta razón que las entidades requieren salvaguardar la información, ya que esta es su recurso más valioso, implementando medidas de control que se adapten a sus requerimientos específicos.

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en una organización puede considerarse como un marco que permite la creación, aplicación, mantenimiento y mejora de las medidas de protección de los activos de información. Los cimientos del SGSI se construyen a través de las políticas de seguridad de la información, en las que la institución establece los requisitos de seguridad y las estrategias necesarias para garantizar el cumplimiento de sus objetivos.

El diseño del sistema de gestión de seguridad de la información se centrará en una evaluación continua para lograr una gestión efectiva y eficiente de los riesgos, y contará con el respaldo de la alta dirección y de toda la institución. La implementación de un SGSI garantizará la protección y gestión eficiente de la información, con el beneficio adicional de la mejora continua a través de auditorías internas y monitoreo, lo que asegurará que los controles estén actualizados y funcionen correctamente en todo momento.

2.6.4. Recursos disponibles

Los elementos disponibles para generar el diseño del Sistema de la Seguridad d la Información son los siguientes:

Información: Debido al apoyo que la institución brindó para la ejecución del presente proyecto de titulación se tuvo acceso de manera total y sin inconveniente a la información requerida.

- Información de los activos del DDTI.

Apoyo de la institución: La institución brindo su apoyo total para la ejecución del presente proyecto de titulación. Las entidades principales que brindaron su apoyo son:

- Apoyo de autoridades de la UTN.
- Apoyo del DDTI.

- Apoyo de la carrera de Ingeniería en Software.

Metodologías: La metodología seleccionada se ajusta de manera adecuada al tipo de organización. La metodología usada fue:

- Metodología para la gestión de riesgos (Magerit v3).

Herramientas: La herramienta facilita la gestión de riesgos ya que su análisis conlleva gran cantidad de información.

- Herramienta para la gestión de riesgos (Software PILAR).

2.6.5. Proceso crítico identificado

Teniendo en cuenta que la función principal del Departamento de Desarrollo Tecnológico e Informático (DDTI) es la atención al sistema académico, se ha determinado que la automatización de ciertas acciones es una prioridad para ofrecer una atención de alta calidad. La automatización de las actividades permitirá a la institución ahorrar tiempo, mejorar la experiencia del usuario y reducir la probabilidad de errores que podrían cometerse en las tareas cotidianas dentro de la universidad. Por ello se considera crucial dedicar esfuerzos y recursos a este proceso prioritario para el éxito a largo plazo del DDTI.

Debido a lo expuesto anteriormente, la institución ha implementado un sistema conocido como SIIU, el cual permite llevar un registro detallado de los estudiantes, profesores y personal administrativo, así como también facilita la consulta de calificaciones y la información referente a los usuarios mencionados, entre otras herramientas y funcionalidades.

En consecuencia, es posible constatar que este procedimiento es altamente sofisticado y engloba múltiples áreas de la institución, debido a la gran cantidad de datos que genera, los cuales deben ser resguardados íntegramente.

2.7. Metodología MAGERIT v3 para la gestión de riesgos

La metodología MAGERIT ha sido seleccionada como el enfoque idóneo para llevar a cabo el análisis y gestión de riesgos debido a su capacidad para abordar los riesgos relacionados con la información digital y los sistemas informáticos. Esta metodología se caracteriza por su

habilidad para reflejar de manera precisa el valor de los servicios o información analizados, y en función de ello, determinar el nivel de protección que debería implementarse. En definitiva, MAGERIT permite identificar detalladamente los riesgos a los que se encuentran expuestos los elementos de trabajo, con el objetivo de gestionarlos de manera efectiva.

La metodología MAGERIT se enfoca en evaluar, homologar y certificar los Sistemas de Gestión de la Seguridad de la Información (SGSI) de acuerdo con la norma ISO 27001:2013. Esta metodología se caracteriza por no basarse en análisis subjetivos que puedan conducir a resultados improvisados. Además de su objetivo principal, MAGERIT contempla otros fines que contribuyen a conformar una metodología completa y exhaustiva:

- Sensibilizar a los líderes de las organizaciones de información acerca de la presencia de riesgos y la importancia de administrarlos de manera efectiva.
- Desarrollar un enfoque sistemático para identificar los riesgos asociados con el uso de las tecnologías de la información y la comunicación (TIC).
- Establecer un plan de acción adecuado para mitigar los riesgos y mantenerlos bajo control.
- Proporcionar capacitación a la organización para realizar evaluaciones, auditorías, certificaciones o acreditaciones, según sea necesario.

La aplicación de normas y metodologías para el análisis de riesgos implica una serie de actividades que conllevan la necesidad de manejar grandes volúmenes de información. Por esta razón, con el fin de ayudar a las organizaciones a manejar esta complejidad, se han creado diversas herramientas que permiten una gestión más eficiente de los riesgos.

Dentro del marco de la metodología MAGERIT, se encuentra disponible el software PILAR.

PILAR

PILAR es una herramienta informática desarrollada por el Centro Criptológico Nacional (CCN) de España, con el fin de apoyar el proceso de gestión de riesgos en el marco de la

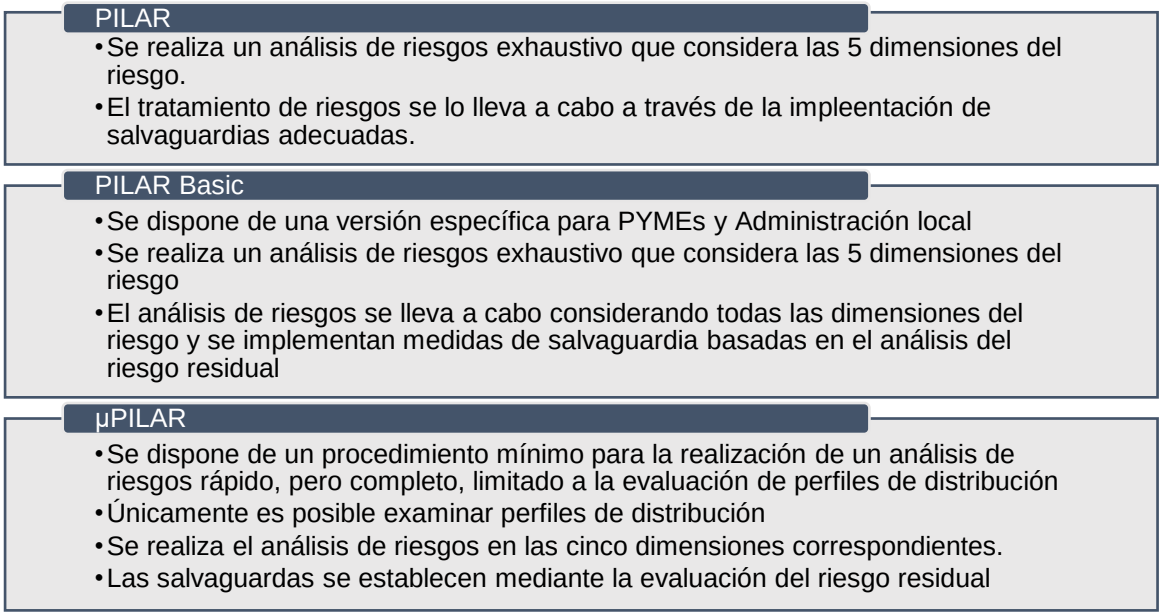
metodología MAGERIT. Según el CCN, PILAR "facilita el análisis y la valoración de riesgos de los sistemas de información, así como la identificación de salvaguardas adecuadas para su tratamiento" (Centro Criptológico Nacional, 2023).

Molina (2015) afirma que en la mayoría de las versiones de la herramienta PILAR, se ofrecen diversas salvaguardas y contramedidas para abordar los riesgos identificados, tras el análisis del riesgo residual en las diferentes etapas del proceso.

En la Figura 23, se expone un conjunto de tres distribuciones diferentes de PILAR, cada una con sus propias características distintivas.

Figura 23

Distribuciones del software PILAR



Nota: Elaboración propia, a partir de Solución PILAR, por Centro Criptológico Nacional de España, 2023, PILAR (https://pilar.ccn-cert.cni.es/index.php/pilar/que-es-pilar).

Al culminar el procedimiento, PILAR nos presenta los resultados del análisis en una presentación visual que consiste en gráficos.

2.8. Valoración de Activos

2.8.1. Identificación de Activos

Los activos en una organización son elementos que crean o almacenan información, y pueden incluir hardware, software, personal y documentos.

En la metodología Magerit V3, se divide los activos de información según las funciones que desempeñan en el proceso de tratamiento de la información. En el caso del DDTI, para su correcto funcionamiento, se requiere de diversos activos, los cuales se detallan a continuación:

Información: un activo abstracto que se almacena en diferentes soportes y equipos y se transporta por distintos servicios y procesos del DDTI.

Software: se compone de todos los programas que permiten gestionar, analizar y transformar los datos para obtener la información necesaria para los distintos servicios.

Hardware: engloba los componentes físicos que directa o indirectamente sostienen los servicios y procesos del DDTI.

Equipamiento auxiliar: se compone de los dispositivos utilizados para apoyar a los equipos principales de la infraestructura informática en situaciones críticas.

Servicios: abarcan todo aquello que satisface las necesidades de los usuarios.

Infraestructura: un conjunto de elementos que proporcionan soporte y facilitan la gestión de los activos de información.

Personas: corresponden a los diferentes grupos que participan en el sistema de información.

Redes de comunicaciones: incluyen todos los dispositivos de telecomunicaciones utilizados para conectar distintos equipos o elementos del sistema de información.

2.8.2. Etiquetado de los activos

La codificación para los activos se establece de la siguiente manera:

Tabla 4

Codificación de los activos

Activo	Etiqueta
Información	IN - ##
Software	SF - ##
Hardware	HD - ##
Equipamiento Auxiliar	AUX - ##
Servicios	SR - ##
Infraestructura	IN - ##
Personas	PR - ##
Redes de comunicaciones	RD - ##

Nota. Elaboración propia, 2022

2.8.3. Inventario de los activos

En la planificación y ejecución del Sistema de Gestión de Seguridad de la Información (SGSI), es crucial realizar un inventario detallado de los activos de información disponibles. Esto permitirá identificar cuáles activos son críticos y, por lo tanto, requieren una protección especial debido a su relevancia en la consecución de los objetivos y la misión de la institución. Se debe tener presente que la protección de estos activos es esencial para prevenir posibles incidentes que puedan afectar directamente el cumplimiento de los objetivos y metas establecidos por la institución.

Tabla 5

Listado de activos con su respectivo código asignado.

TIPO DE ACTIVO	NOMBRE	CÓDIGO ASIGNADO
Información	Base de datos	IN-01
	Archivos de datos	IN-02
	Documentación interna	IN-03
	Material impreso	IN-04
	Carpetas compartidas	IN-05
Software	Motor de base de datos	SW-01

	Repositorio de aplicaciones desarrolladas	SW-02
	Antivirus	SW-03
	Firewall	SW-04
	Licencias	SW-05
	Navegadores	SW-06
	Sistemas Operativos	SW-07
Hardware	Dispositivos de almacenamiento	HW-01
	Computadoras	HW-02
	Teléfonos IP	HW-03
	Servidores	HW-04
	Equipos para funcionamiento de red (switchs /Access point / transceivers)	HW-05
	Equipo multifuncional (impresora/Scanner)	HW-06
	Dispositivos de grabación y fotografía	HW-07
	Radios de comunicación	HW-08
Equipamiento Auxiliar	UPS	AUX-01
	Generador Eléctrico	AUX-02
	Equipos de climatización	AUX-03
	Mobiliario	AUX-04
Servicios	Telefonía	SR-01
	Internet	SR-02
	Electricidad	SR-03
	Correo institucional	SR-04
	Soporte a usuarios	SR-05
	Soporte a la red	SR-06
	Soporte a los servicios informáticos	SR-07

	Mantenimiento a los equipos	SR-08
Instalaciones	Instalación de red de datos	IF-01
	Instalación de red eléctrica	IF-02
	UPS del centro cableado	IF-03
	Espacio Físico del DDTI	IF-04
Personal	Personal Administrativo	PR-01
	Personal de desarrollo	PR-02
Redes de comunicaciones	Ethernet	RD-01
	Red Inalámbrica	RD-02
	Red LAN	RD-03
	Red Telefónica	RD-04

Nota. Elaboración propia, 2022

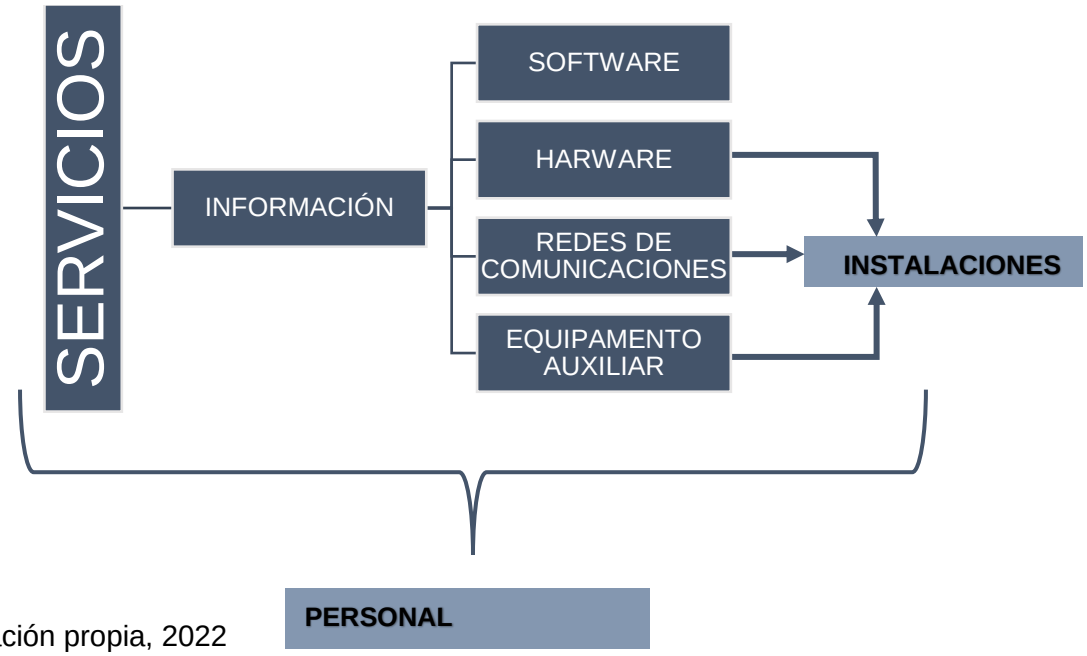
2.8.4. Dependencia de los activos

Después de la identificación de los activos, es necesario considerar las interdependencias existentes entre ellos. Si bien este análisis de riesgos no ha incluido explícitamente las interdependencias mencionadas para evitar una mayor complejidad en el análisis, es importante tener en cuenta que un riesgo elevado en los activos de nivel inferior tendrá un efecto en cascada en los activos superiores, y que el personal es un factor crítico en todos los activos.

A continuación, se presenta una visión general de las interdependencias entre las diferentes categorías de activos:

Figura 24

Dependencia de los activos



Nota. Elaboración propia, 2022

2.8.5. Criterio de valoración de los activos

Una vez que se han identificado los activos del DDTI, es necesario realizar una evaluación para asignarles un valor basado en sus características relevantes y su potencial para la institución. En este caso de estudio, se aplicará una valoración cualitativa mediante encuestas, así como una valoración cuantitativa a través de una matriz a los responsables de los procesos relacionados con cada activo. Estas herramientas están diseñadas para cumplir con los parámetros básicos de confidencialidad, integridad y disponibilidad establecidos por Magerit V3 (*Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método*, 2012).

La valoración cualitativa permitirá comprender en mayor profundidad la importancia de cada activo en el modelo de negocio y cómo su pérdida afectaría la continuidad del DDTI.

Para garantizar una evaluación precisa, se utilizarán preguntas específicas para cada parámetro:

Tabla 6

Criterios de valoración de los activos

Etiqueta	Tipo de valoración
D	Disponibilidad: propiedad o característica de los activos consistente en que las unidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
I	Integridad de los datos: propiedad o característica de los activos consistente en que el activo de información no ha sido alterado de manera no autorizada.
C	Confidencialidad de la información: propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

Nota: Elaboración basada en Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II: Catálogo de elementos, por Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012.

- **Confidencialidad:**

¿Cómo afectaría al DDTI que la información sea conocida por personas ajenas no autorizadas?

- **Integridad:**

¿Qué perjuicio causaría para el DDTI que estuviera dañado o corrupto?

- **Disponibilidad:**

¿Cómo afectaría al DDTI no poder utilizar un activo?

Conforme a la metodología Magerit versión 3, la evaluación cuantitativa depende del criterio y se fundamenta en la escala que se muestra en la Tabla 7. En el Anexo 1 se proporciona información detallada sobre la herramienta utilizada y la evaluación obtenida para cada activo en función de los parámetros evaluados.

Tabla 7

Escala de valoración de los activos

Nivel de valor	Valor	Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6 – 8	Alto	Daño grave
3 – 5	Medio	Daño importante
1 – 2	Bajo	Daño menos
0	Despreciable	Irrelevante a efectos prácticos

Nota. Elaboración basada en Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II: Catálogo de elementos, por Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012.

La Tabla 8 exhibe datos precisos sobre la evaluación, incluyendo el promedio de las tres dimensiones establecidas por Magerit v3, es importante tener en cuenta que a medida que el número obtenido se incrementa, el nivel de daño también aumenta.

Tabla 8

Información obtenida de la valoración de los activos de la información

VALORACIÓN DE LOS ACTIVOS DE LA INFORMACIÓN					
CÓDIGO ACTIVO	**Nombre de Activo**	**Valoración de Impacto** C: Confidencialidad I: Integridad D: Disponibilidad			
		C	**I**	**D**	**PT**
IN-01	Base de datos	10	10	10	**Extremo**
IN-02	Archivos de datos	10	10	10	**Extremo**
IN-03	Documentación interna	10	10	10	**Extremo**
IN-04	Material impreso	5	5	5	**Medio**
IN-05	Carpetas compartidas	5	10	10	**Alto**
SW-01	Motor de base de datos	10	10	10	**Extremo**

SW-02	Repositorio de aplicaciones desarrolladas	10	10	10	**Extremo**
SW-03	Antivirus	0	10	10	**Alto**
SW-04	Firewall	0	10	10	**Alto**
SW-05	Licencias	10	5	10	**Alto**
SW-06	Navegadores	0	10	10	**Alto**
SW-07	Sistemas Operativos	10	10	10	**Extremo**
HW-01	Dispositivos de almacenamiento	10	10	10	**Extremo**
HW-02	Computadoras	8	10	8	**Muy Alto**
HW-03	Teléfonos IP	1	8	8	**Alto**
HW-04	Servidores	2	10	10	**Alto**
HW-05	Equipos para funcionamiento de red (switchs /Access point / transceivers)	2	10	10	**Alto**
HW-06	Equipo multifuncional (impresora/Scanner)	0	5	5	**Medio**
HW-07	Dispositivos de grabación y fotografía	0	5	5	**Medio**
HW-08	Radios de comunicación	0	5	5	**Medio**
AUX-01	UPS	0	10	10	**Alto**
AUX-02	Generador Eléctrico	0	9	9	**Alto**
AUX-03	Equipos de climatización	0	10	10	**Alto**
AUX-04	Mobiliario	0	0	5	**Bajo**
SR-01	Telefonía	0	8	8	**Medio**
SR-02	Internet	0	10	10	**Alto**
SR-03	Electricidad	0	8	10	**Alto**
SR-04	Correo institucional	10	10	10	**Extremo**
SR-05	Soporte a la red	0	9	9	**Alto**
SR-06	Soporte a los servicios informáticos	0	5	8	**Medio**
SR-07	Mantenimiento a los equipos	0	5	8	**Medio**
IF-01	Instalación de red de datos	0	10	10	**Alto**
IF-02	Instalación de red eléctrica	0	10	10	**Alto**

IF-03	UPS del centro cableado	0	10	10	**Alto**
IF-04	Espacio Físico del DDTI	0	10	10	**Alto**
PR-01	Personal Administrativo	5	5	5	**Medio**
PR-02	Personal de desarrollo	10	10	10	**Extremo**
RD-01	Ethernet	0	10	10	**Alto**
RD-02	Red Inalámbrica	0	10	10	**Alto**
RD-03	Red LAN	0	10	10	**Alto**
RD-04	Red Telefónica	0	8	8	**Medio**

Nota. Elaboración propia, 2022

2.8.6. Identificación de amenazas

Es fundamental que toda institución sea consciente de que se encuentra expuesta a múltiples tipos de amenazas y por lo tanto resulta primordial llevar a cabo un proceso de identificación, análisis y evaluación de riesgos para determinar la probabilidad de ocurrencia de estas.

Para llevar a cabo la identificación de amenazas, es recomendable utilizar herramientas especializadas como el software PILAR, el cual contiene un "Catálogo de Elementos" basado en Magerit V3 que enumera y describe de manera exhaustiva diversos tipos de amenazas. Entre las amenazas que se pueden encontrar en este catálogo se incluyen:

[N] Desastres Naturales

[I] Origen Industrial

[E] Errores y fallos no intencionados

[A] Ataques intencionados

La tabla 8 muestra la información recibida por cada categoría de activos, reflejando las amenazas que aprovechan una vulnerabilidad para afectar la seguridad de la información del DDTI.

Se identificaron en total 51 amenazas distribuidas entre los 41 activos pertenecientes al DDTI de la UTN, la matriz completa de amenazas se encuentra en el Anexo 3.

Tabla 9

Amenazas por cada categoría de activos.

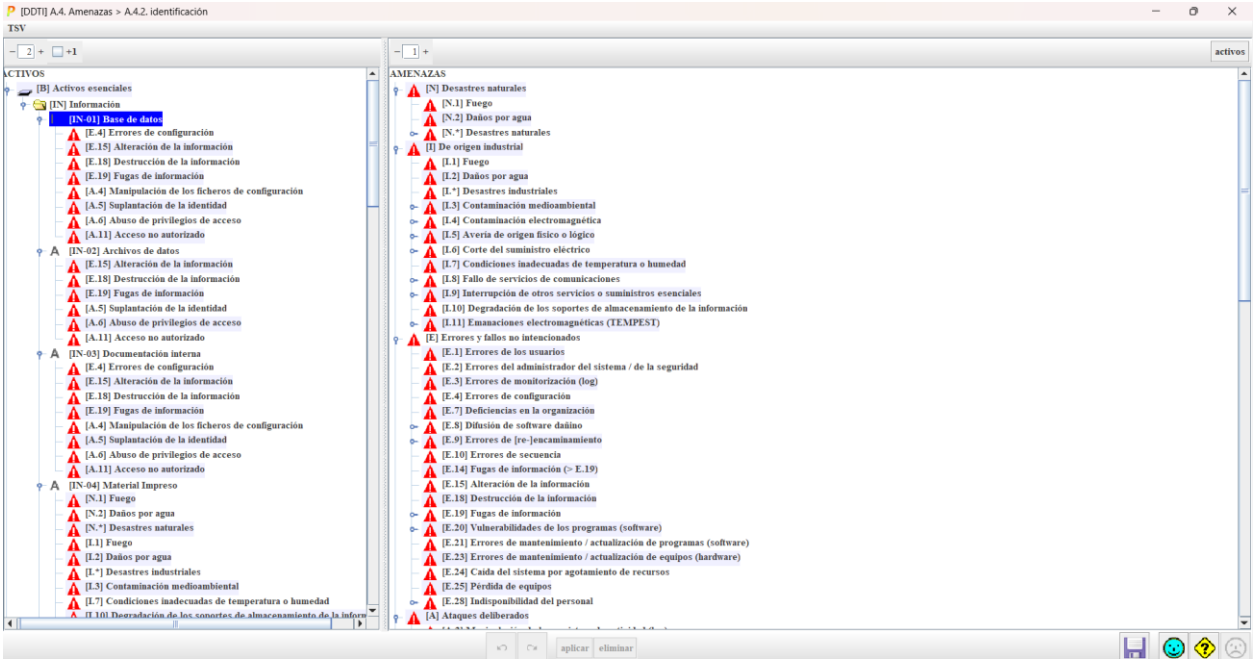
ACTIVO	AMENAZA
INFORMACIÓN	
BASE DE DATOS	
Base de datos	[E.15] Alteración de la información
Base de datos	[E.18] Destrucción de la información
Base de datos	[E.19] Fugas de información
Base de datos	[A.5] Suplantación de la identidad
Base de datos	[A.6] Abuso de privilegios de acceso
Base de datos	[A.11] Acceso no autorizado
ARCHIVO DE DATOS	
Archivo de datos	[E.15] Alteración de la información
Archivo de datos	[E.18] Destrucción de la información
Archivo de datos	[E.19] Fugas de información
Archivo de datos	[A.5] Suplantación de la identidad
Archivo de datos	[A.6] Abuso de privilegios de acceso
Archivo de datos	[A.11] Acceso no autorizado
DOCUMENTACIÓN INTERNA	
Documentación interna	[E.15] Alteración de la información
Documentación interna	[E.18] Destrucción de la información
Documentación interna	[E.19] Fugas de información
Documentación interna	[A.5] Suplantación de la identidad
Documentación interna	[A.6] Abuso de privilegios de acceso
Documentación interna	[A.11] Acceso no autorizado

Nota. Elaboración propia, 2022

Del mismo modo, PILAR detecta automáticamente las posibles amenazas a los activos previamente identificados, tal y como se indica en la Figura 24.

Figura 25

Identificación de amenazas en activos del DDTI-UTN mediante el software PILAR



Nota. Elaboración propia, 2022

2.8.7. Valoración de amenazas

Luego de haber identificado las potenciales amenazas relacionadas con cada categoría de activos, se procede a llevar a cabo una evaluación bidireccional utilizando una escala previamente definida, la cual se encuentra detallada en las Tablas 10.

Impacto: para evaluar el impacto potencial de una amenaza en un activo, se emplea la escala descrita en la Tabla 11 para cuantificar el grado de daño. No obstante, cuando se utiliza el software PILAR, se requiere la utilización de valores numéricos, por lo que se aplica una escala porcentual que oscila entre 0 y 100.

Tabla 10

Escala de Degradación del valor de un activo.

MA	100%	Muy alta	Casi seguro	Fácil
A	75%	Alta	Muy alto	Medio
M	50%	Media	Posible	Difícil
B	25%	Baja	Poco Probable	Muy dificil
MB	0%	Muy baja	Muy raro	Extremadamente dificil

Nota: Tomada de Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método ,por Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012.

Frecuencia: el término se refiere a la frecuencia con la que una amenaza se materializa, y para medirla se emplea la tasa anual de ocurrencia que se encuentra detallada en la Tabla 9

Tabla 11

Valores de probabilidad de ocurrencia de una amenaza

MA	100	Muy frecuente	A diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco Frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Nota. Tomada de Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método, por Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012.

La evaluación de cada dimensión se compone de los siguientes criterios: Activo, Amenaza, Frecuencia, Impacto, los cuales se encuentran incluidos en la matriz de valoración.

La totalidad de la matriz que contempla la evaluación de riesgos se encuentra incluida en el Anexo 4. Como ejemplo, en la tabla 12 se exhibe una sección de la matriz.

Tabla 12

Evaluación de riesgos

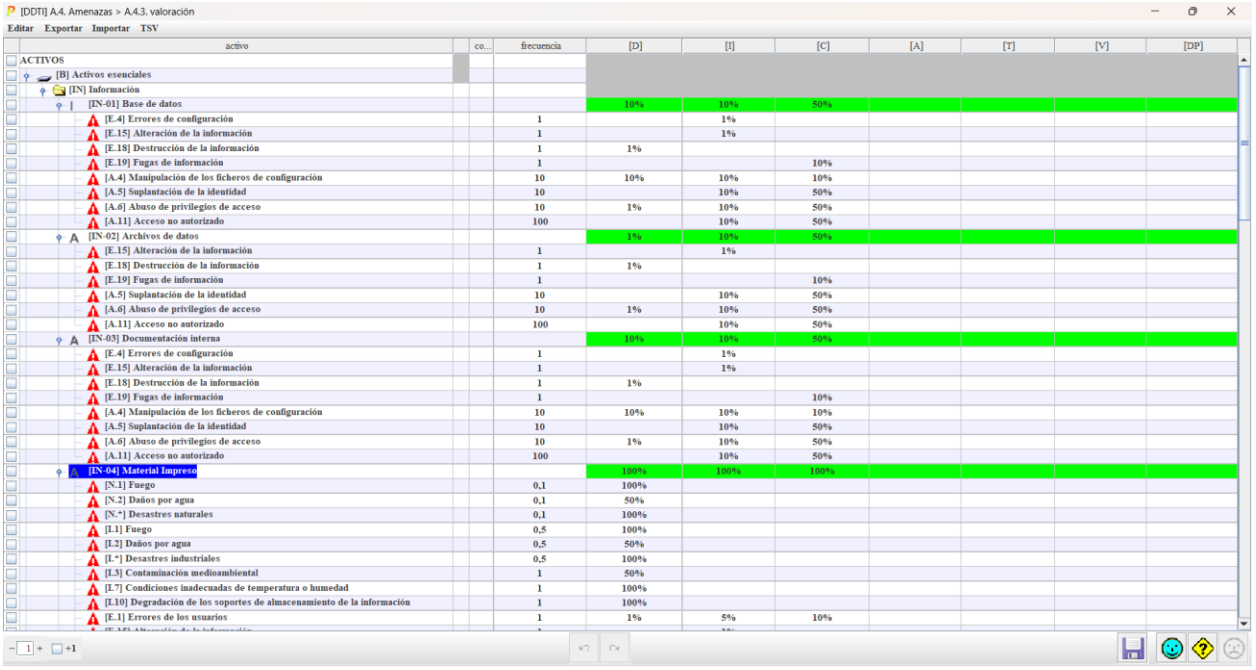
ACTIVO	AMENAZA	FRECUENCIA	D	I	C
INFORMACIÓN					
BASE DE DATOS					
Base de datos	[E.15] Alteración de la información	1		1%	
Base de datos	[E.18] Destrucción de la información	1	1%		
Base de datos	[E.19] Fugas de información	1			10%
Base de datos	[A.5] Suplantación de la identidad	10		10%	50%
Base de datos	[A.6] Abuso de privilegios de acceso	10	1%	10%	50%
Base de datos	[A.11] Acceso no autorizado	100		10%	50%
ARCHIVO DE DATOS					
Archivo de datos	[E.15] Alteración de la información	1		1%	
Archivo de datos	[E.18] Destrucción de la información	1	1%		
Archivo de datos	[E.19] Fugas de información	1			10%
Archivo de datos	[A.5] Suplantación de la identidad	10		10%	50%
Archivo de datos	[A.6] Abuso de privilegios de acceso	10	1%	10%	50%
Archivo de datos	[A.11] Acceso no autorizado	100		10%	50%
DOCUMENTACIÓN INTERNA					
Documentación interna	[E.15] Alteración de la información	1		1%	
Documentación interna	[E.18] Destrucción de la información	1	1%		
Documentación interna	[E.19] Fugas de información	1			10%
Documentación interna	[A.5] Suplantación de la identidad	10		10%	50%
Documentación interna	[A.6] Abuso de privilegios de acceso	10	1%	10%	50%
Documentación interna	[A.11] Acceso no autorizado	100		10%	50%

Nota: La tabla presenta una muestra del listado de la valoración de amenazas que podrían afectar a los activos identificados en el DDTI-UTN. En donde F: frecuencia, D: degradación en la dimensión de disponibilidad, I: degradación en la dimensión de integridad, C: degradación en la dimensión de confidencialidad. Elaboración propia

En la Figura 26 se representa la evaluación de las posibles amenazas en relación con la disminución de la calidad de los bienes y a la probabilidad de que ocurran, lo cual se basa en la información brindada por el software PILAR.

Figura 26

Valoración de amenazas por activos del DDTI-UTN en el software PILAR.



Nota: Elaboración propia

2.8.8. Evaluación de Riesgos

Una vez que se ha completado la tarea de inventariar los activos de información y se han identificado y evaluado las amenazas presentes en la institución, se procede a calcular el riesgo, siguiendo ciertos criterios.

El impacto potencial: que podría resultar de la materialización de dichas amenazas en los activos de información, y cómo esto afectaría las dimensiones de confidencialidad, integridad y disponibilidad en términos de su degradación. Para determinar el valor correspondiente a cada dimensión, se ha creado la Tabla 13, la cual se presenta a continuación:

Tabla 13

Criterios de valoración de riesgo

Valor Cuantitativo	Descripción
Muy Alto (10)	Si se materializa la amenaza, tendría desastrosas consecuencias en la organización .
Alto (9)	Si se materializa la amenaza, tendría altas consecuencias sobre la organización.
Medio (6-8)	Si se materializa la amenaza, tendría medianas consecuencias sobre la organización.
Bajo (5-3)	Si se materializa la amenaza, tendría bajas consecuencias sobre la organización.
Muy Bajo (1-2)	Si se materializa la amenaza, tendría efectos mínimos sobre la organización.
Despreciable (0)	Si se materializa la amenaza, no tendría efectos sobre la organización.

Nota: Tomada de Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II : Catálogo de elementos , por Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012.

Dicho impacto se lo puede realizar desde dos enfoques:

Impacto potencial acumulado: se refiere al valor total del activo en consideración, incluyendo tanto el valor propio como el valor acumulado de los activos que dependen directamente de él, y la evaluación de las amenazas a las que se encuentra expuesto. Este cálculo se realiza mediante la aplicación de una ecuación específica diseñada para este propósito.

Impacto potencial acumulado=% Degradación de amenaza ×Valor acumulado del activo

El Anexo 5 contiene el cálculo del impacto potencial acumulado, mientras que en la Tabla 14 se proporciona una muestra de los elementos que conforman dicha lista.

Tabla 14

Impacto potencial acumulado de afectación de activos en el DDTI-UTN

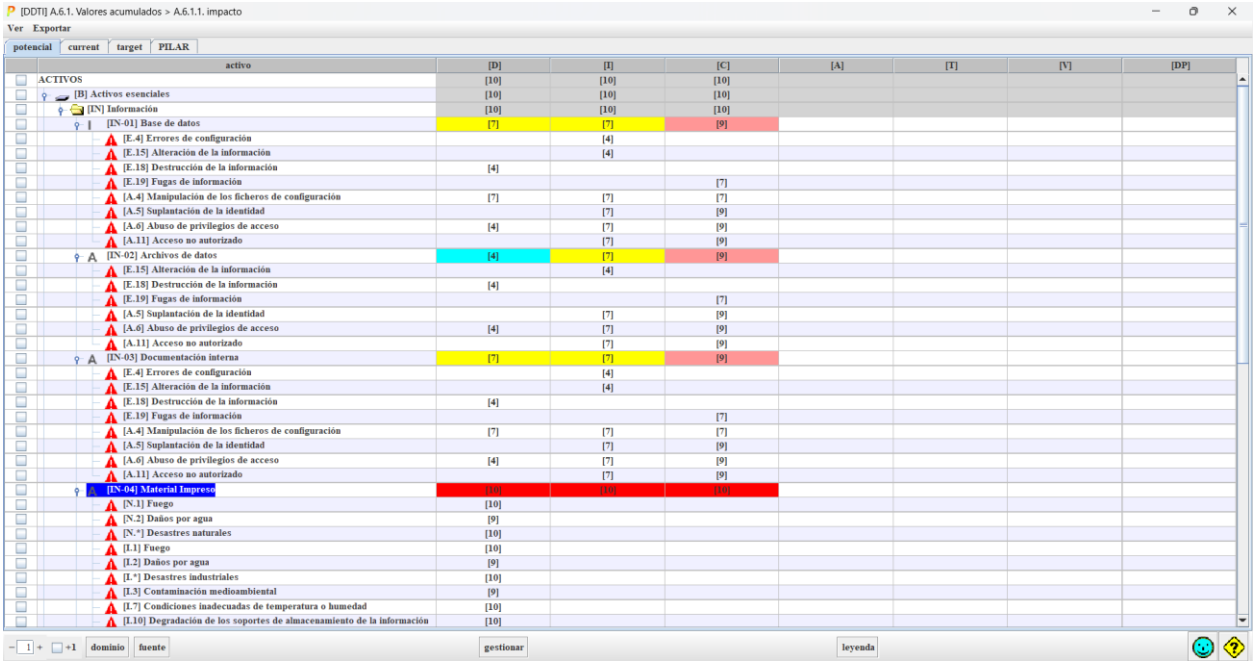
	IMPACTO POTENCIAL ACUMULADO			PESO PONDERADO
ACTIVO	**D**	**I**	**C**	
INFORMACIÓN	10	10	9	
BASE DE DATOS	4	7	9	
[E.15] Alteración de la información		4		4
[E.18] Destrucción de la información	4			4
[E.19] Fugas de información			7	7
[A.5] Suplantación de la identidad		7	9	8
[A.6] Abuso de privilegios de acceso	4	7	9	6,7
[A.11] Acceso no autorizado		7	9	8
ARCHIVO DE DATOS	4	7	9	6,7
[E.15] Alteración de la información		4		4
[E.18] Destrucción de la información	4			4
[E.19] Fugas de información			7	7
[A.5] Suplantación de la identidad		7	9	8
[A.6] Abuso de privilegios de acceso	4	7	9	6,7
[A.11] Acceso no autorizado		7	9	8,0
DOCUMENTACIÓN INTERNA	4	7	9	6,7
[E.15] Alteración de la información		4		4
[E.18] Destrucción de la información	4			4
[E.19] Fugas de información			7	7
[A.5] Suplantación de la identidad		7	9	8
[A.6] Abuso de privilegios de acceso	4	7	9	6,7
[A.11] Acceso no autorizado		7	9	8

Nota: La tabla muestra el impacto acumulado, en donde D, I, C: son la degradación en cada una de las dimensiones. Elaboración propia

La Figura 27 muestra el impacto potencial acumulado que el software PILAR ha obtenido.

Figura 27

Impacto potencia acumulado de afectación de activos en el DDTI-UTN en el software PILAR



Nota: Elaboración propia.

Impacto potencial repercutido: se trata de una evaluación integral que considera tanto el impacto directo en el activo o sistema en cuestión, como el posible efecto cascada que puede tener sobre otros elementos relacionados.

Impacto potencia repercutido=% Degradación de amenaza ×Valor propio del activo

La Tabla 15 presenta el análisis del impacto potencial repercutido.

Tabla 15

Impacto potencial repercutido de afectación de activos en el DDTI-UTN

	IMPACTO POTENCIAL REPERCUTIDO			PESO PONDERADO
ACTIVOS	**D**	**I**	**C**	
Base de datos	10	10	10	10
Archivos de datos	10	10	10	10
Documentación interna	10	10	10	10
Material impreso	10	10	9	9,7
Carpetas compartidas	5	10	10	8,3
Motor de base de datos	10	10	10	10

Repositorio de aplicaciones desarrolladas	10	10	10	10
Antivirus	10	10	10	10
Firewall	10	10	10	10
Licencias	10	10	10	10
Navegadores	10	10	10	10
Sistemas Operativos	10	10	10	10
Dispositivos de almacenamiento	10	7	9	8,7
Computadoras	10	7	9	8,7
Teléfonos IP	10	7	9	8,7
Servidores	10	7	9	8,7
Equipos para el funcionamiento de la red	10	7	9	8,7
Equipo multifuncional	10	7	9	8,7
Dispositivos de grabación y fotografía	10	7	9	8,7
Radios de comunicación	10	7	9	8,7
Ethernet	9	8	9	8,7
Red inalámbrica	9	8	9	8,7
Red LAN	9	8	9	8,7
Red telefónica	9	8	9	8,7
UPS	10	4	9	7,7
Generador eléctrico	10	4	9	7,7
Equipos de climatización	10	4	9	7,7
Mobiliario	10	4	9	7,7
Telefonía	9	9	7	8,3
Internet	9	10	10	9,7
Electricidad	9	7		8
Correo institucional	9	9	9	9
Soporte de red	10	10	9	9,7
Soporte a los servicios informáticos	9	9	7	8,3
Mantenimiento a los equipos	9	10	10	9,7
Instalación de red de datos	10		10	10
Instalación de red eléctrica	10		10	10
UPS del centro cableado	10		10	10

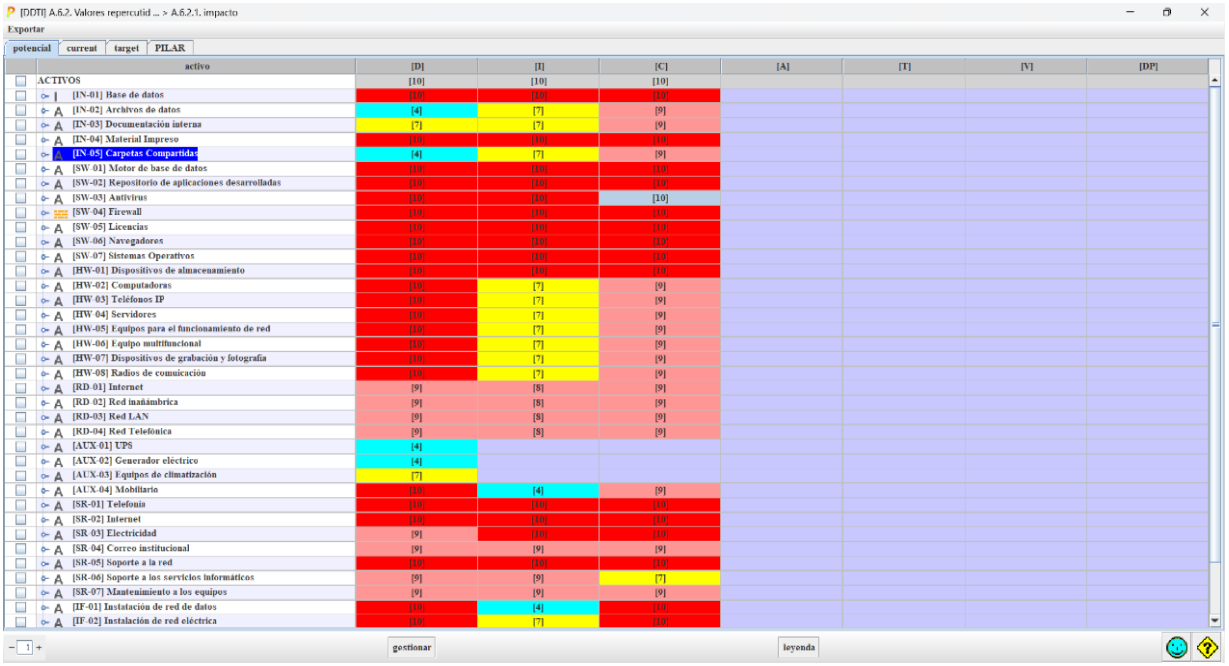
Espacio físico DDTI	10		10	10
Personal administrativo	7	9	9	8,3
Personal de desarrollo	7	9	9	8,3

Nota: La tabla exhibe una sección del listado del impacto potencial repercutido. D, I, C ,corresponde a la degradación en cada una de las dimensiones. Elaboración propia.

En la Figura 28, se muestra el impacto potencial repercutido por activo del DDTI-UTN.

Figura 28

Impacto potencial repercutido de afectación de activos en el DDTI-UTN en el software **PILAR**

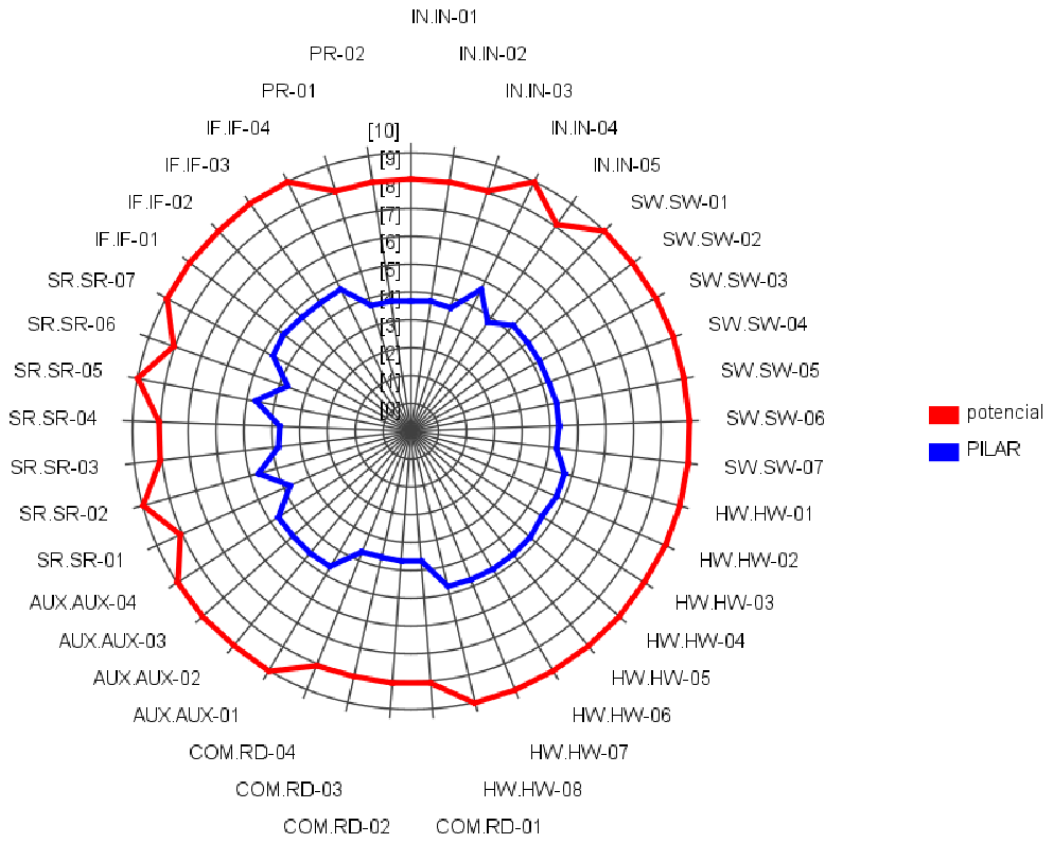


Nota: Elaboración propia.

La Figura 28 muestra un diagrama que ilustra el impacto acumulado potencial actual para cada activo, representado por la línea roja, y los valores recomendados por PILAR, representados por la línea azul.

Figura 29

Gráfico de valores de impacto potencial acumulado de los activos del DDTI-UTN



Nota: Elaboración propia.

La evaluación del impacto potencial acumulado de las amenazas sobre los activos del sistema es fundamental para la gestión efectiva de riesgos, ya que permite determinar las medidas de control necesarias. En contraste, si se evalúa el impacto potencial de las amenazas únicamente sobre el valor propio de los activos, se obtiene información limitada acerca de las consecuencias de las incidencias

Determinación del riesgo potencial

Una vez que se ha evaluado el impacto potencial, es necesario determinar el riesgo potencial, el cual se define como la medida de la posible pérdida o daño teniendo en cuenta la

probabilidad de que dicho evento ocurra. La relación entre el riesgo y el impacto, así como la probabilidad de ocurrencia, puede ser visualizada en la Tabla 16.

Tabla 16

Niveles de riesgo

IMPACTO						
	MA	Media	Alta	Muy alta	Crítico	Crítico
	A	Baja	Media	Alta	Muy alta	Crítico
	M	Muy baja	Baja	Media	Alta	Muy alta
	B	Aceptable	Muy baja	Baja	Media	Alta
	MB	Aceptable	Aceptable	Muy baja	Baja	Media
		MB	B	M	A	M A
		PROBABILIDAD				

Nota: Adecuado de“Risk management methodology in the supply chain: a case study applied” (p.1058), por Hermoso-Orzáez & Garzón-Moreno, 2022), Annals of Operations Research, 2 (313).

La valoración del riesgo se lleva a cabo de manera individualizada para cada activo, en consideración de cada amenaza y en todas las dimensiones de evaluación correspondientes.

Existen dos perspectivas desde las cuales se puede abordar el riesgo mencionado, estas son:

Riesgo potencial acumulado: Se considera el valor acumulado del impacto en un activo debido a una amenaza y la probabilidad de dicha amenaza. La fórmula utilizada para calcularlo es la siguiente:

Riesgo potencial acumulado= Probabilidad de amenaza ×Valor acumulado del impacto

La totalidad de la evaluación del riesgo potencial acumulado se encuentra detallada en el Anexo 6, donde se presenta la matriz completa. A continuación, se muestra un ejemplo de dicha matriz en la Tabla 17.

Tabla 17

Riesgo potencial acumulado de afectación de los activos del DDTI-UTN

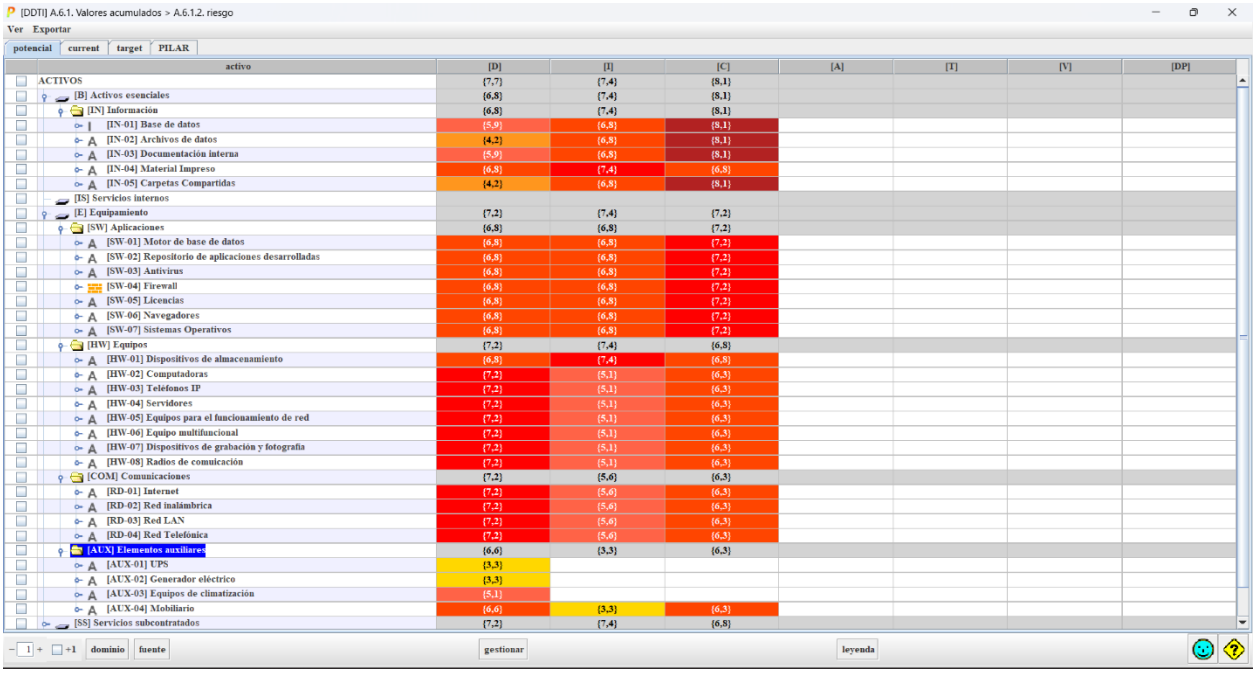
	RIESGO POTENCIAL ACUMULADO			PESO PONDERADO
ACTIVOS	**D**	**I**	**C**	
INFORMACIÓN	6,9	7,5	8,2	7,5
BASE DE DATOS	4,4	6,9	8,2	6,5
[E.15] Alteración de la información		3,4		3,4
[E.18] Destrucción de la información	3,4			3,4
[E.19] Fugas de información			5,1	5,1
[A.5] Suplantación de la identidad		6	7,3	6,7
[A.6] Abuso de privilegios de acceso	4,4	6,1	7,4	6
[A.11] Acceso no autorizado		6,9	8,2	7,6
ARCHIVO DE DATOS	4,4	6,9	8,2	6,5
[E.15] Alteración de la información		3,4		3,4
[E.18] Destrucción de la información	3,4			3,4
[E.19] Fugas de información			5,1	5,1
[A.5] Suplantación de la identidad		6	7,3	6,7
[A.6] Abuso de privilegios de acceso	4,4	6,1	7,4	6,0
[A.11] Acceso no autorizado		6,9	8,2	8
DOCUMENTACIÓN INTERNA	4,4	6,9	8,2	6,5
[E.15] Alteración de la información		3,4		3,4
[E.18] Destrucción de la información	3,4			3,4
[E.19] Fugas de información			5,1	5,1
[A.5] Suplantación de la identidad		6	7,3	6,7
[A.6] Abuso de privilegios de acceso	4,4	6,1	7,4	6
[A.11] Acceso no autorizado		6,9	8,2	7,6

Nota: La tabla exhibe el cálculo del riesgo potencial acumulado. En donde D, I y C corresponden a la degradación de cada dimensión. Elaboración propia.

La Figura 30 muestra los resultados del software PILAR en términos de los valores acumulados del riesgo potencial.

Figura 30

Riesgo potencial acumulado de afectación de los activos en el DDTI-UTN mediante el software



Nota: Elaboración propia.

Riesgo potencial repercutido: Se considera el efecto resultante de la amenaza sobre el activo y la probabilidad de que ocurra dicha amenaza. La fórmula utilizada para calcularlo es la siguiente:

Riesgo potencial repercutido= Probabilidad de amenaza ×Valor repercutido del impacto

La Tabla 18 contiene el cálculo del riesgo potencial repercutido.

Tabla 18

Riesgo potencial repercutido de afectación de activos en el DDTI-UTN

	RIESGO POTENCIAL REPERCUTIDO			PESO PONDERADO
ACTIVOS	**D**	**I**	**C**	
Base de datos	7,4	7,5	8,2	7,7
Archivos de datos	7,4	7,5	8,2	7,7
Documentación interna	7,4	7,5	8,2	7,7
Material impreso	6,9	7,5	6,4	6,9
Carpetas compartidas	4,4	7,5	8,2	6,7
Motor de base de datos	6,9	7	7,2	7
Repositorio de aplicaciones desarrolladas	6,9	7	7,2	7
Antivirus	6,9	7	7,2	7
Firewall	6,9	7	7,3	7
Licencias	6,9	7	7,2	7
Navegadores	6,9	7	7,2	7
Sistemas Operativos	6,9	7	7,2	7
Dispositivos de almacenamiento	7,3	5,2	6,4	6,3
Computadoras	7,3	5,2	6,4	6,3
Teléfonos IP	7,3	5,2	6,4	6,3
Servidores	7,3	5,2	6,4	6,3
Equipos para el funcionamiento de la red	7,3	5,2	6,4	6,3
Equipo multifuncional	7,3	5,2	6,4	6,3
Dispositivos de grabación y fotografía	7,3	5,2	6,4	6,3
Radios de comunicación	7,3	5,2	6,4	6,3
Ethernet	7,4	5,6	6,4	6,5
Red inalámbrica	7,4	5,6	6,4	6,5
Red LAN	7,4	5,6	6,4	6,5

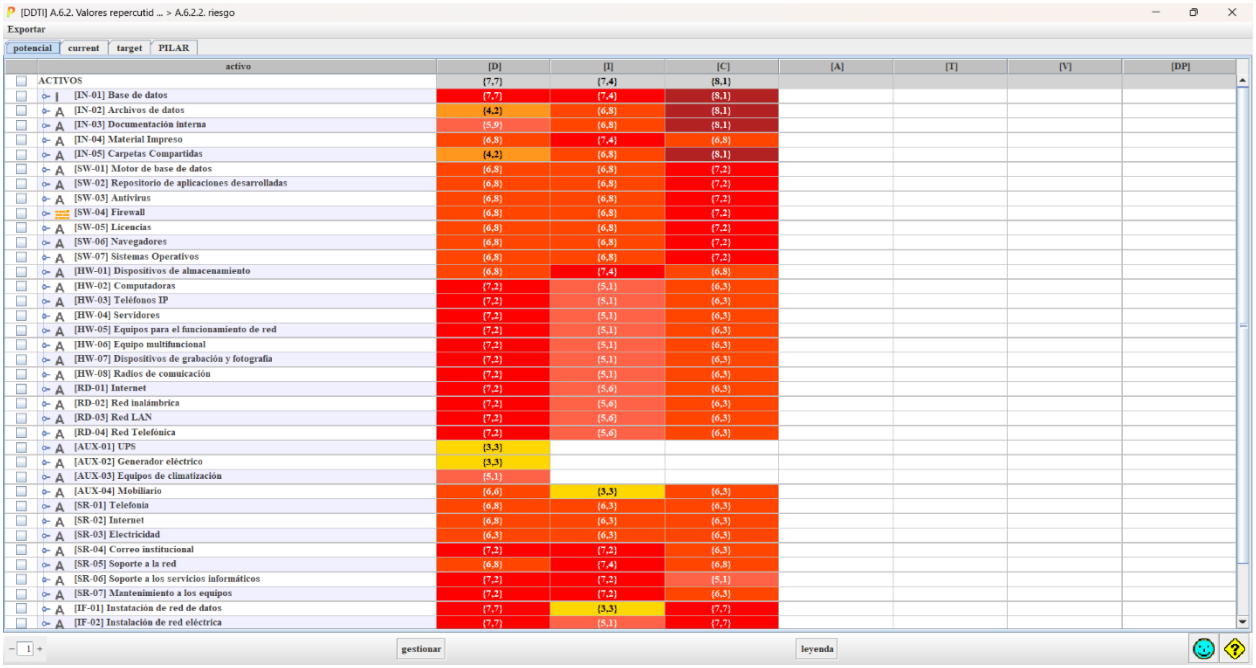
Red telefónica	7,4	5,6	6,4	6,5
UPS	6,6	3,5	6,3	5,5
Generador eléctrico	6,6	3,5	6,3	5,5
Equipos de climatización	6,6	3,5	6,3	5,5
Mobiliario	6,6	3,5	6,3	5,5
Telefonía	6,5	6,4	5,1	6,0
Internet	6,5	6,4	6,3	6,4
Electricidad	6,3	5,1		5,7
Correo institucional	7,4	7,3	6,4	7,0
Soporte de red	6,9	7,5	6,4	6,9
Soporte a los servicios informáticos	7,4	7,3	5,2	6,6
Mantenimiento a los equipos	6,5	6,4	6,4	6,4
Instalación de red de datos	6,9		7,7	7,3
Instalación de red eléctrica	6,9		7,7	7,3
UPS del centro cableado	6,9		7,7	7,3
Espacio físico DDTI	6,9		7,7	7,3
Personal administrativo	5,2	6,4	6,4	6
Personal de desarrollo	5,2	6,4	6,4	6

Nota: La tabla muestra el cálculo del riesgo potencial repercutido, D, I, C, representa la degradación en cada dimensión. Elaboración propia

En la Figura 31 se indica los valores del riesgo potencial repercutido por cada activo mediante el software PILAR.

Figura 31

Riesgo potencial repercutido en el DDTI-UTN mediante el software PILAR



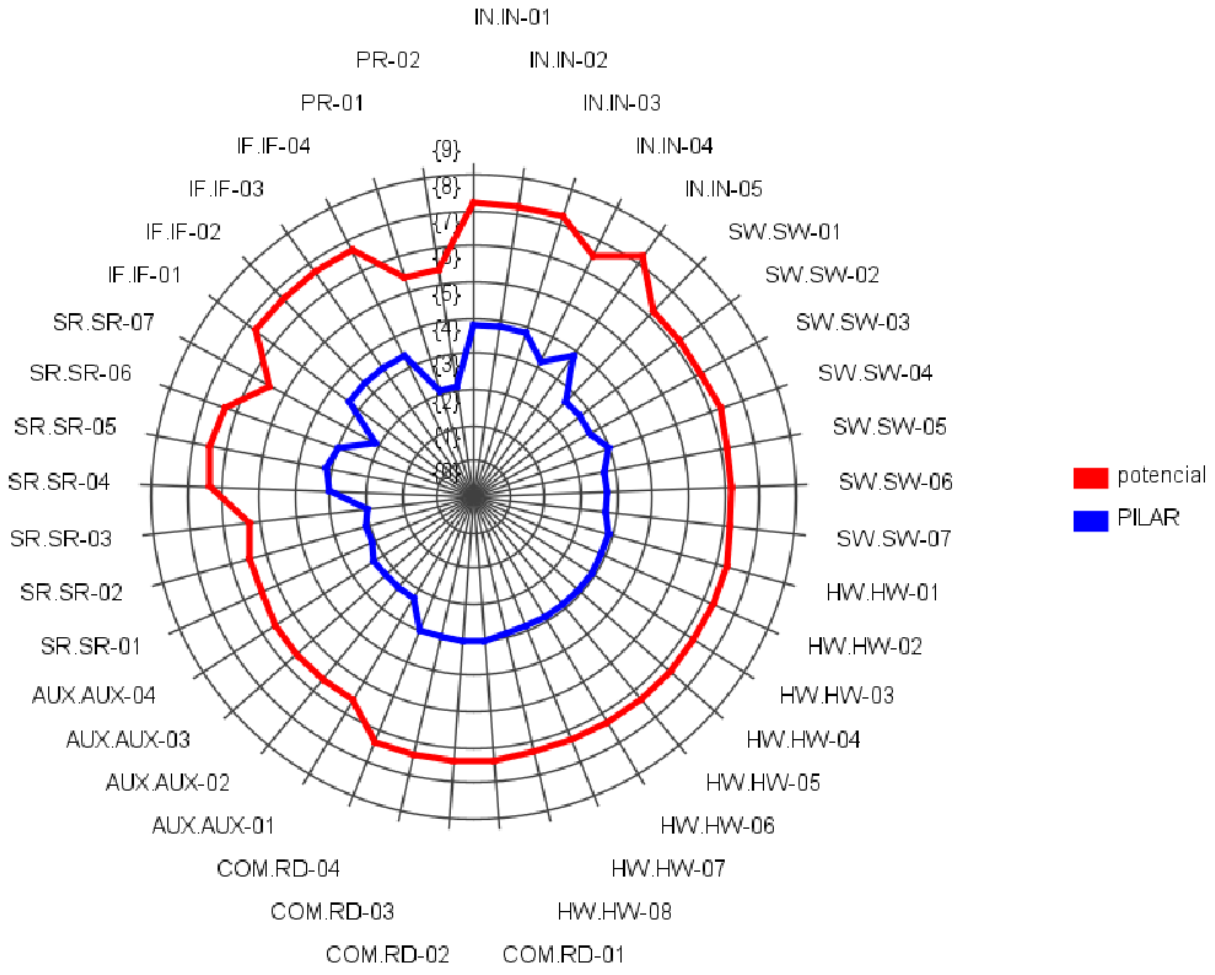
activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS	{7,7}	{7,4}	{8,1}				
[IN-01] Base de datos	{7,7}	{7,4}	{8,1}				
[IN-02] Archivos de datos	{4,2}	{6,8}	{8,1}				
[IN-03] Documentación interna	{5,9}	{6,8}	{8,1}				
[IN-04] Material Impreso	{6,8}	{7,4}	{6,8}				
[IN-05] Carpetas Compartidas	{4,2}	{6,8}	{8,1}				
[SW-01] Motor de base de datos	{6,8}	{6,8}	{7,2}				
[SW-02] Repositorio de aplicaciones desarrolladas	{6,8}	{6,8}	{7,2}				
[SW-03] Antivirus	{6,8}	{6,8}	{7,2}				
[SW-04] Firewall	{6,8}	{6,8}	{7,2}				
[SW-05] Licencias	{6,8}	{6,8}	{7,2}				
[SW-06] Navegadores	{6,8}	{6,8}	{7,2}				
[SW-07] Sistemas Operativos	{6,8}	{6,8}	{7,2}				
[HW-01] Dispositivos de almacenamiento	{6,8}	{7,4}	{6,8}				
[HW-02] Computadoras	{7,2}	{5,1}	{6,3}				
[HW-03] Teléfonos IP	{7,2}	{5,1}	{6,3}				
[HW-04] Servidores	{7,2}	{5,1}	{6,3}				
[HW-05] Equipos para el funcionamiento de red	{7,2}	{5,1}	{6,3}				
[HW-06] Equipo multifuncional	{7,2}	{5,1}	{6,3}				
[HW-07] Dispositivos de grabación y fotografía	{7,2}	{5,1}	{6,3}				
[HW-08] Radios de comuicación	{7,2}	{5,1}	{6,3}				
[RD-01] Internet	{7,2}	{5,6}	{6,3}				
[RD-02] Red inalámbrica	{7,2}	{5,6}	{6,3}				
[RD-03] Red LAN	{7,2}	{5,6}	{6,3}				
[RD-04] Red Telefónica	{7,2}	{5,6}	{6,3}				
[AUX-01] UPS	{3,3}						
[AUX-02] Generador eléctrico	{3,3}						
[AUX-03] Equipos de climatización	{5,1}						
[AUX-04] Mobiliario	{6,6}	{3,3}	{6,3}				
[SR-01] Telefonía	{6,8}	{6,3}	{6,3}				
[SR-02] Internet	{6,8}	{6,3}	{6,3}				
[SR-03] Electricidad	{6,3}	{6,3}	{6,3}				
[SR-04] Correo institucional	{7,2}	{7,2}	{6,3}				
[SR-05] Soporte a la red	{6,8}	{7,4}	{6,8}				
[SR-06] Soporte a los servicios informáticos	{7,2}	{7,2}	{5,1}				
[SR-07] Mantenimiento a los equipos	{7,2}	{7,2}	{6,3}				
[IF-01] Instatación de red de datos	{7,7}	{3,3}	{7,7}				
[IF-02] Instalación de red eléctrica	{7,7}	{5,1}	{7,7}				

Nota: Elaboración propia

La Figura 32 exhibe un diagrama en el que la línea roja refleja los niveles de riego potencial acumulado actual correspondientes a cada activo, en tanto que la línea azul indica los valores sugeridos por PILAR.

Figura 32

Gráfico de valores de riesgo acumulado de los activos del DDTI-UTN



Nota: Elaboración propia

Al calcular el riesgo potencial acumulado basándose en el valor acumulado de los activos del sistema, es posible determinar los controles necesarios para el proceso de gestión de riesgos. Sin embargo, al calcular el riesgo potencial repercutido sobre el valor propio de los activos, solo se pueden determinar las consecuencias de las amenazas y no se obtiene información sobre los controles necesarios para mitigar los riesgos.

2.8.9. Plan de tratamiento de riesgo

En el ámbito del tratamiento de riesgos, es fundamental tomar decisiones con respecto a las diversas amenazas que puedan presentarse. En consonancia con las estrategias de la institución, en el marco del DDTI se han definido una serie de acciones para el tratamiento de riesgos:

El proceso de elaboración del plan de tratamiento de riesgos requiere de la selección y aplicación de medidas adecuadas para modificar los riesgos, a fin de prevenir cualquier tipo de daño a los activos de información de la institución.

2.8.10. Criterio para el tratamiento de riesgos

Una vez definidos los niveles de riesgo en relación con las amenazas que pueden afectar a cada activo de información, se establecen los criterios de aceptación de riesgo, los cuales permiten determinar el tipo de riesgo y la necesidad de aplicar controles específicos. Para conocer con detalle las acciones a tomar, se puede consultar la Tabla 19.

Tabla 19

Criterios para tratamiento de riegos

Zona	Acción a tomar
Aceptable	Aceptar
Tolerable	Transferir
Moderada	Reducir
Inaceptable	Evitar

Nota: Adaptado de la ISO/IEC 27001, 2018

Se determinan las acciones apropiadas a tomar en función del nivel de riesgo asociado, evaluando la probabilidad e impacto de cada uno de los activos de información. Las opciones disponibles son las siguientes:

- **Aceptar:** Si el nivel de exposición es considerado adecuado, entonces se acepta el riesgo**.**

- **Transferir:** Si es posible, se puede delegar la gestión del riesgo a otra entidad o departamento que esté mejor capacitado para manejarlo.
- **Reducir:** Si se considera que el riesgo es inaceptable, se deben implementar medidas adicionales para fortalecer los controles existentes o agregar nuevos controles que permitan reducir el riesgo a niveles aceptables.
- **Evitar:** Se requieren acciones inmediatas para reducir la probabilidad de que el riesgo se materialice.

Resulta esencial que la institución realice una supervisión regular de los riesgos identificados, con el objetivo de poder discernir los factores que los originan y, de esta manera, poder asignar los recursos requeridos para abordarlos adecuadamente.

La Tabla 20 presenta una muestra de la matriz de tratamiento de riesgo, la matriz completa se puede observar en el Anexo 7.

Tabla 20

Matriz de tratamiento de riesgos

ACTIVOS	AMENAZAS	PESO PONDERADO	ACCIÓN
INSTALACIÓN DE RED DE DATOS	[A.25] Robo de equipos	7,7	Evitar
INSTALACIÓN DE RED ELÉCTRICA	[A.25] Robo de equipos	7,7	Evitar
UPS DEL CENTRO CABLEADO	[A.25] Robo de equipos	7,7	Evitar
ESPACIO FÍSICO DDTI	[A.25] Robo de equipos	7,7	Evitar
ARCHIVO DE DATOS	[A.11] Acceso no autorizado	7,6	Reducir
BASE DE DATOS	[A.11] Acceso no autorizado	7,6	Reducir
DOCUMENTACIÓN INTERNA	[A.11] Acceso no autorizado	7,6	Reducir
CARPETAS COMPARTIDAS	[A.11] Acceso no autorizado	7,6	Reducir
SOPORTE DE RED	[A.15] Modificación de la información	7,5	Evitar
MATERIAL IMPRESO	[A.15] Modificación de la información	7,5	Evitar
ETHERNET	[A.24] Denegación de servicio	7,4	Evitar

RED INALAMBRICA	[A.24] Denegación de servicio	7,4	Evitar
RED LAN	[A.24] Denegación de servicio	7,4	Evitar
RED TELEFÓNICA	[A.24] Denegación de servicio	7,4	Evitar
CORREO INSTITUCIONAL	[A.24] Denegación de servicio	7,4	Evitar
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[A.24] Denegación de servicio	7,4	Evitar
DISPOSITIVOS DE ALMACENAMIENTO	[A.24] Denegación de servicio	7,3	Evitar
COMPUTADORAS	[A.24] Denegación de servicio	7,3	Evitar
TELÉFONOS IP	[A.24] Denegación de servicio	7,3	Evitar
SERVIDORES	[A.24] Denegación de servicio	7,3	Evitar
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[A.24] Denegación de servicio	7,3	Evitar
EQUIPO MULTIFUNCIONAL	[A.24] Denegación de servicio	7,3	Evitar
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[A.24] Denegación de servicio	7,3	Evitar
RADIOS DE COMUNICACIÓN	[A.24] Denegación de servicio	7,3	Evitar
CORREO INSTITUCIONAL	[A.15] Modificación de la información	7,3	Evitar

Nota: Elaboración propia

Una vez que se han definido y asignado las alternativas de tratamiento de los riesgos, es relevante considerar qué controles son prioritarios para una adecuada gestión de riesgos. Los controles, que se refieren a actividades que buscan reducir los riesgos, son una pieza fundamental en este proceso. La norma ISO 27001:2013 proporciona una lista exhaustiva de los distintos controles que deben aplicarse en función de cada tipo de activo.

2.9. Diseño de controles

Luego de completar el proceso de evaluación de riesgos, se procede a identificar los controles pertenecientes al Anexo A de la norma ISO 27001 que se utilizarán, tomando en cuenta tanto los riesgos identificados como los recursos disponibles dentro de la institución.

2.9.1. Identificación de controles aplicables

La norma ISO 27001 incluye controles que permiten diseñar políticas para mitigar las amenazas que puedan afectar los activos de información. Estos controles establecen parámetros para determinar las acciones necesarias para tratar el riesgo o nivel residual del riesgo. En el caso del DDTI-UTN, se han considerado dominios para establecer controles de seguridad física y del entorno, seguridad de operaciones y comunicaciones, adquisición, desarrollo y mantenimiento de sistemas de información, puesta en marcha de activos de información y gestión de incidentes de seguridad de la información.

Después de analizar los riesgos por activos según el Anexo 7, se presenta en la Tabla 21 un resumen global de los dominios con sus objetivos respectivos, controles a implementar y actividades dirigidas a mitigar el riesgo en los activos de información en la entidad universitaria, mientras que en el Anexo 8 se encuentra la matriz completa por cada activo con su respectivo control.

Tabla 21

Dominios a implementar en el DDTI-UTN

Dominio	Objetivo-control	Actividad
A.7 Seguridad relativa a los recursos humanos	**A.7.1 Antes del empleo** A.7.1.1 Investigaciones de antecedentes A.7.1.2 Términos y condiciones	Verificar los antecedentes del candidato para comprobar su idoneidad
	A.7.2 Durante el empleo A.7.2.2 Concienciación, educación y formación en seguridad de la información	Sensibilizar a los funcionarios sobre las nuevas responsabilidades que conlleva la implementación del SGSI, obteniendo su aceptación mediante la firma de las políticas correspondientes
A.8 Gestión de activos	**A.8.1 Responsabilidad sobre los activos** A.8.1.1 Inventario de activos	Asignar formalmente la responsabilidad de actualizar el inventario de activos
	A.8.2 Clasificación de la información	Establecer categorías para priorizar la información

	A.8.2.1 Clasificación de la información	
A.9 Control de acceso	**A.9.1 Requisitos comerciales de control de acceso** A.9.1.1 Política de control de acceso	Asignar roles y privilegios correspondientes a cada activo para garantizar el cumplimiento de las funciones establecidas
	A.9.2 Gestión de acceso de usuario A.9.2.3 Gestión de privilegios de derechos de accesos	Establecer directrices para controlar el acceso adecuado de los usuarios a sus activos respectivos
A.11 Seguridad física y del entorno	**A.11.1 Áreas seguras** A.11.1.1 Perímetro de seguridad física A.11.1.4 Protección contra las amenazas externas y ambientales A.11.1.5 El trabajo en áreas seguras	Definir los perímetros en los que cada funcionario está autorizado a permanecer según su función
	A.11.2 Seguridad de los equipos A.11.2.1 Emplazamiento y protección de equipos A.11.2.2 Instalaciones de suministro A.11.2.4 Mantenimiento de los equipos	Seguir las recomendaciones del fabricante para la ubicación y protección adecuadas del hardware o equipo correspondiente
A.12 Seguridad de las operaciones	**A.12.1 Procedimientos** operativos y responsabilidades A.12.1.1 Documentación de procedimientos operacionales A.12.1.2 Gestión de cambios A.12.1.2 Gestión de capacidades	Mantener en toda la institución una política de documentación basada en el sistema de gestión de calidad
	A.12.3 Copias de seguridad A.12.3.1 Copias de seguridad de la información	Capacitar a los encargados de activos y administradores de plataformas sobre la política de generación y recuperación de copias de seguridad
	A.12.4 Registro de la actividad y supervisión	Establecer un procedimiento de firma digital para los registros de

	A.12.4.1 Registro de eventos A.12.4.2 Protección de la información del registro A.12.4.3 Registro de administración y operación	eventos de las aplicaciones, con el fin de mejorar la seguridad de los activos
	A.12.6 Gestión de la vulnerabilidad técnica A.12.6.1 Gestión de vulnerabilidades técnicas A.12.6.2 Restricciones en la instalación de software	Obtener información acerca de las vulnerabilidades técnicas de los sistemas de información utilizados y tomar las medidas necesarias para mitigar el riesgo correspondiente
A.13 Seguridad de las comunicaciones	**A.13.1 Gestión de la seguridad en las redes** A.13.1.1 Controles de red A.13.1.2 Seguridad de los servicios de red	Definir las direcciones IP de origen y destino, los puertos para el tráfico autorizado y establecer patrones de comportamiento normal de las aplicaciones en la red
	A.13.2 Intercambio de información con partes externas A.13.2.1 Políticas y procedimientos de transferencia de información A.13.2.3 Mensajería electrónica A.13.2.4 Acuerdos de confidencialidad o no revelación	Implementar algoritmos criptográficos para proteger los datos utilizados en la mensajería electrónica, de acuerdo con las políticas del sistema de gestión de seguridad de la información
A.14 Adquisición desarrollo y mantenimiento de los sistemas de información	**A.14.1 Requisitos de seguridad de los sistemas de información** A.14.1.1 Análisis de requisitos y especificaciones de seguridad de la información A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas A.14.1.3 Protección de las transacciones de servicios de aplicaciones	Capacitar a los empleados del departamento de desarrollo y tecnologías de la información en la política de desarrollo de software seguro, desarrollar un plan para definir los requisitos de seguridad de la información de software existente y aplicar controles de acceso y protección de datos expuestos en los servicios de red, basados en las políticas del sistema de gestión de seguridad de la información
	A.14.2 Seguridad en los procesos de desarrollo	Luego de modificar la plataforma, el líder de seguridad debe llevar a

	A.14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo A.14.2.8 Pruebas funcionales de seguridad de sistemas A.14.2.9 Pruebas de aceptación de sistemas	cabo pruebas para asegurar que los datos se mantengan protegidos en cuanto a confidencialidad, integridad y disponibilidad, de acuerdo con el Sistema de Gestión de Seguridad de la Información (SGSI). Establecer protocolos de pruebas de aceptación con cada fabricante de software utilizado en la institución antes de que se implementen en producción.
A.16 Gestión de incidentes de la seguridad de la información	**A.16.1 Gestión de incidentes de seguridad de la información y mejoras** A.16.1.7 Recopilación de evidencias	Seleccionar a un grupo de funcionarios encargados del manejo de evidencias y establecer la cadena de custodia para los incidentes de seguridad de alto impacto
A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	**A.17.1 Continuidad de la seguridad de la información** A.17.1.1 Planificación de la continuidad de la seguridad de la información	Determinar las necesidades de la institución en cuanto a seguridad de la información y continuidad en la gestión de situaciones adversas
A.18 Cumplimiento	**A.18.1 Cumplimiento de requisitos legales y contractuales** A.18.1.4 Protección y privacidad de la información de carácter personal	Definir una política de protección de datos personales y cumplir con las leyes correspondientes
	A.18.2 Revisaciones de Seguridad de la información A.18.2.3 Comprobación del cumplimiento técnico	Llevar a cabo revisiones periódicas para verificar el cumplimiento de las políticas de seguridad establecidas

Nota: Elaboración propia

2.9.2. Estimación del Impacto Residual

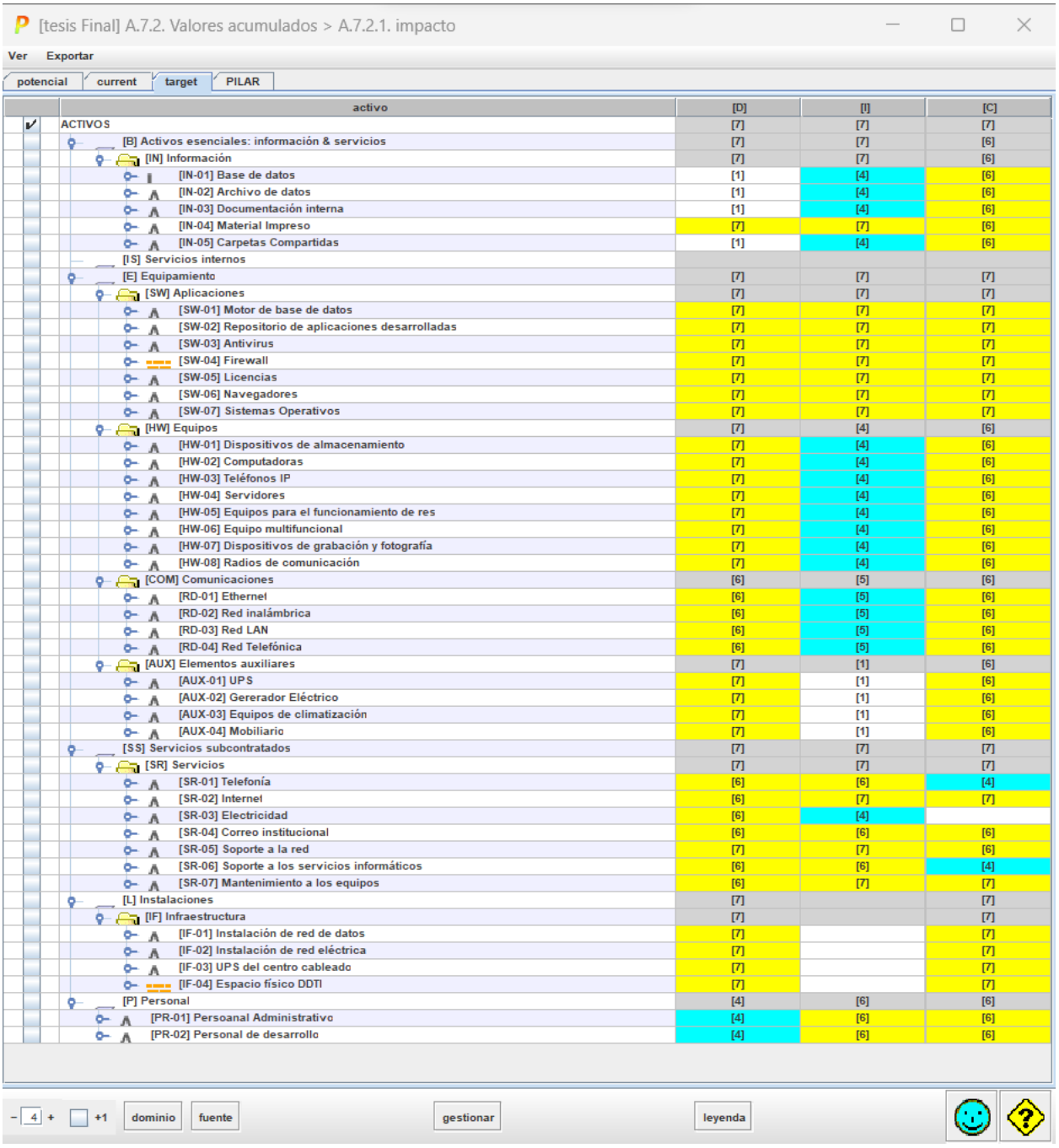
Al logran ejecutar las tareas planificadas para llevar a cabo los controles, el impacto potencial original del sistema se transforma en un impacto residual. La herramienta de software

PILAR simula la implementación de los controles y proporciona una evaluación del impacto residual acumulado y el impacto residual repercutido.

La Figura 33 muestra la acumulación del impacto residual, mientras que en la Figura 34 se puede apreciar la repercusión del impacto residual.

Figura 33

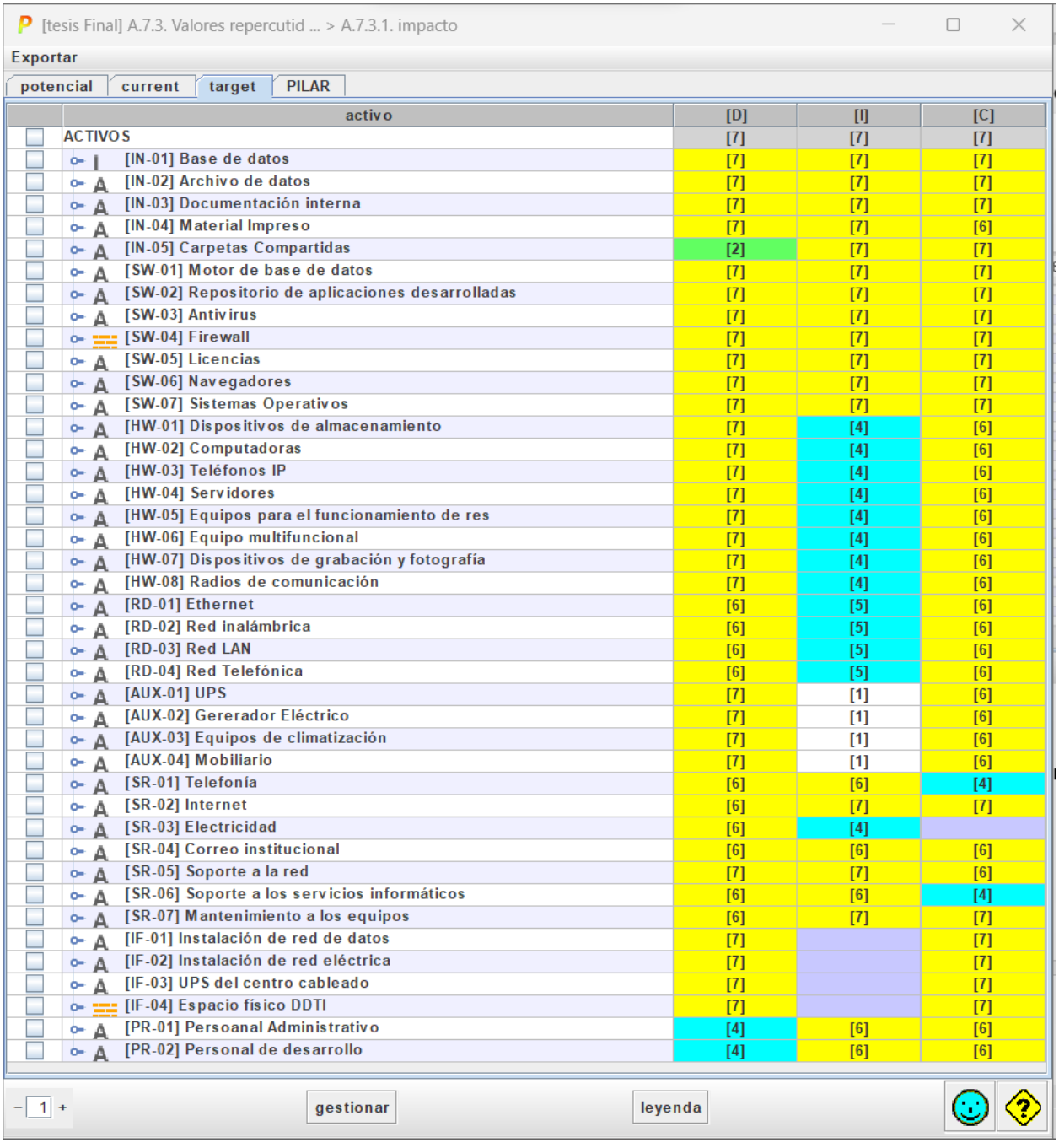
Impacto residual acumulado de los activos del DDTI-FICA mediante el software PILAR



Nota: Elaboración propia

Figura 34

Impacto residual repercutido de los activos del DDTI-UTN mediante el software PILAR



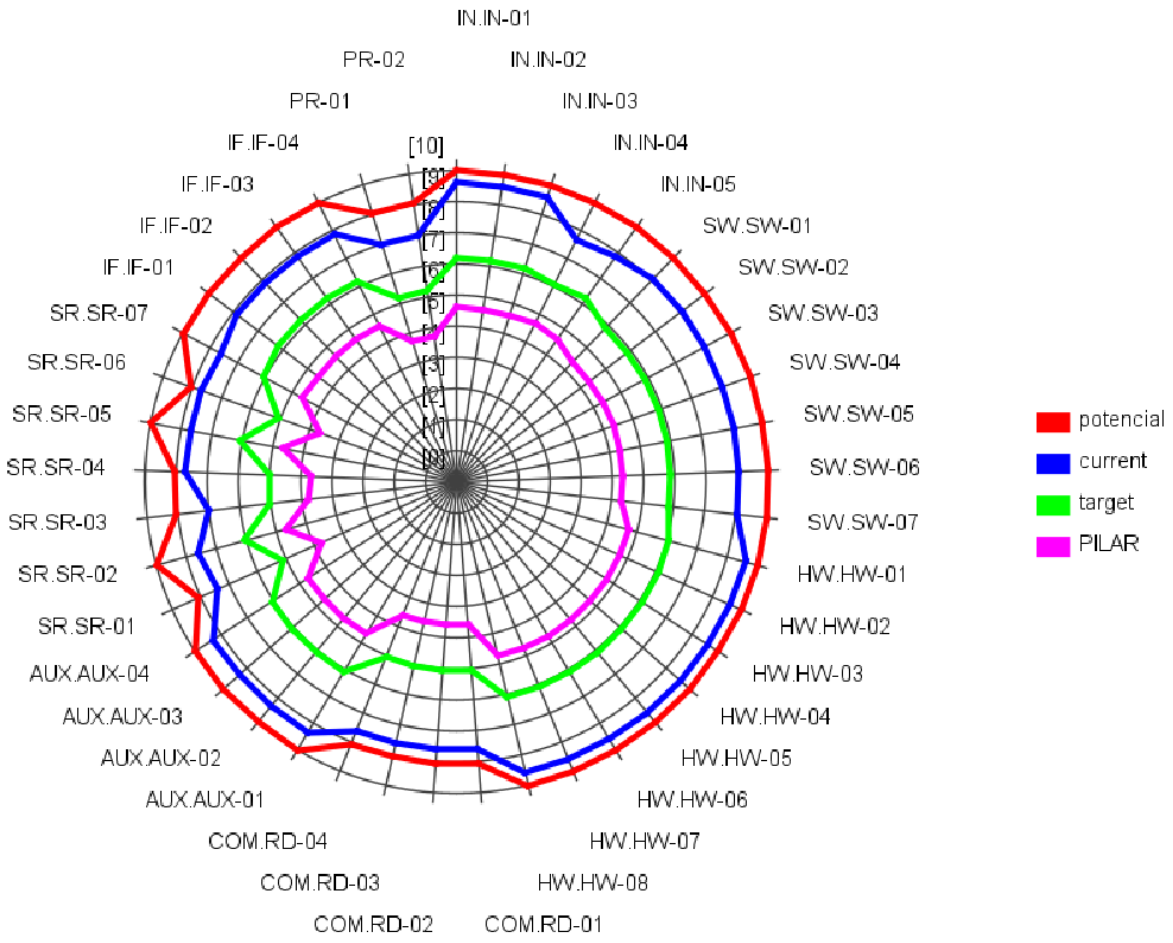
activo	[D]	[I]	[C]
ACTIVOS	[7]	[7]	[7]
[IN-01] Base de datos	[7]	[7]	[7]
[IN-02] Archivo de datos	[7]	[7]	[7]
[IN-03] Documentación interna	[7]	[7]	[7]
[IN-04] Material Impreso	[7]	[7]	[6]
[IN-05] Carpetas Compartidas	[2]	[7]	[7]
[SW-01] Motor de base de datos	[7]	[7]	[7]
[SW-02] Repositorio de aplicaciones desarrolladas	[7]	[7]	[7]
[SW-03] Antivirus	[7]	[7]	[7]
[SW-04] Firewall	[7]	[7]	[7]
[SW-05] Licencias	[7]	[7]	[7]
[SW-06] Navegadores	[7]	[7]	[7]
[SW-07] Sistemas Operativos	[7]	[7]	[7]
[HW-01] Dispositivos de almacenamiento	[7]	[4]	[6]
[HW-02] Computadoras	[7]	[4]	[6]
[HW-03] Teléfonos IP	[7]	[4]	[6]
[HW-04] Servidores	[7]	[4]	[6]
[HW-05] Equipos para el funcionamiento de res	[7]	[4]	[6]
[HW-06] Equipo multifuncional	[7]	[4]	[6]
[HW-07] Dispositivos de grabación y fotografía	[7]	[4]	[6]
[HW-08] Radios de comunicación	[7]	[4]	[6]
[RD-01] Ethernet	[6]	[5]	[6]
[RD-02] Red inalámbrica	[6]	[5]	[6]
[RD-03] Red LAN	[6]	[5]	[6]
[RD-04] Red Telefónica	[6]	[5]	[6]
[AUX-01] UPS	[7]	[1]	[6]
[AUX-02] Gererador Eléctrico	[7]	[1]	[6]
[AUX-03] Equipos de climatización	[7]	[1]	[6]
[AUX-04] Mobiliario	[7]	[1]	[6]
[SR-01] Telefonía	[6]	[6]	[4]
[SR-02] Internet	[6]	[7]	[7]
[SR-03] Electricidad	[6]	[4]	
[SR-04] Correo institucional	[6]	[6]	[6]
[SR-05] Soporte a la red	[7]	[7]	[6]
[SR-06] Soporte a los servicios informáticos	[6]	[6]	[4]
[SR-07] Mantenimiento a los equipos	[6]	[7]	[7]
[IF-01] Instalación de red de datos	[7]		[7]
[IF-02] Instalación de red eléctrica	[7]		[7]
[IF-03] UPS del centro cableado	[7]		[7]
[IF-04] Espacio físico DDTI	[7]		[7]
[PR-01] Persoanal Administrativo	[4]	[6]	[6]
[PR-02] Personal de desarrollo	[4]	[6]	[6]

Nota: Elaboración propia

La Figura 35 exhibe de manera concisa y gráfica los efectos posibles, actuales, deseados y sugeridos por el programa PILAR.

Figura 35

Gráfico de valores de impacto de activos del DDTI-UTN



Nota: Elaboración propia

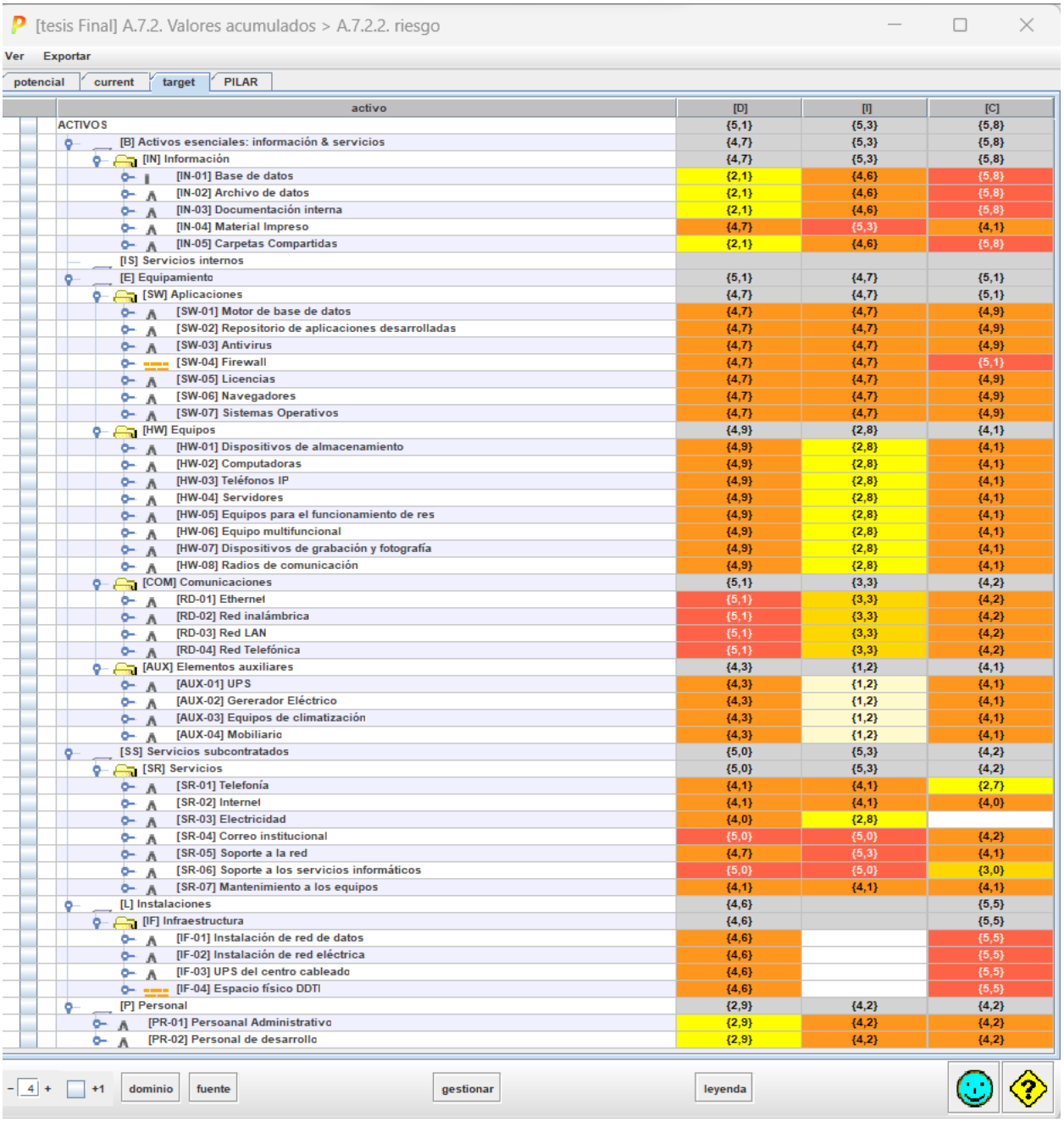
2.9.3. Estimación del Impacto Residual

De forma similar a como el impacto residual es evaluado, el software denominado PILAR emula la aplicación de controles y proporciona una evaluación del riesgo residual acumulado y del riesgo residual repercutido.

La Figura 36 muestra la acumulación del riesgo residual, mientras que en la Figura 37 se puede apreciar la repercusión del riesgo residual.

Figura 36

Riesgo residual acumulado de los activos del DDTI-UTN mediante el software PILAR

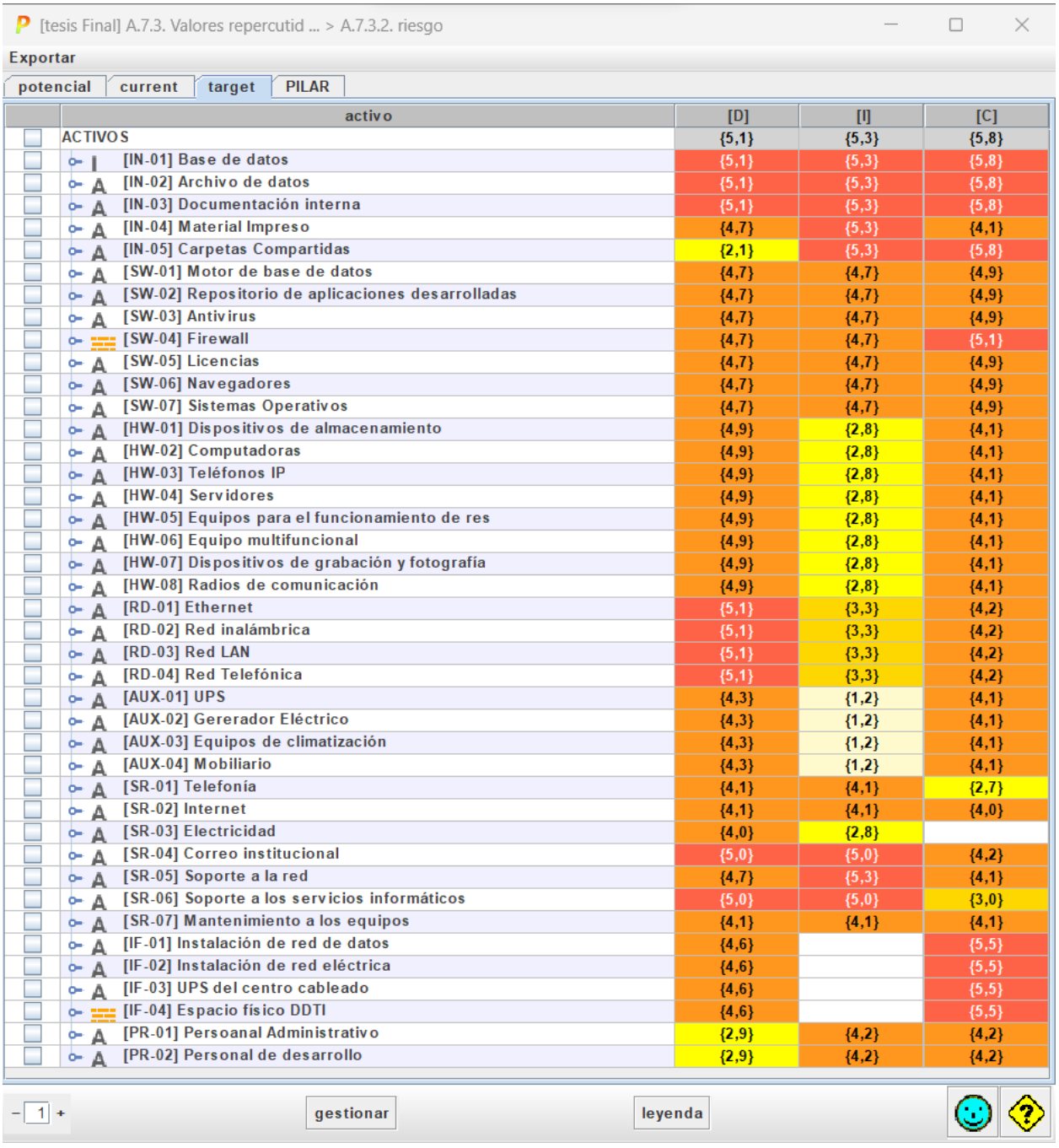


activo	[D]	[I]	[C]
ACTIVOS	{5,1}	{5,3}	{5,8}
[B] Activos esenciales: información & servicios	{4,7}	{5,3}	{5,8}
[IN] Información	{4,7}	{5,3}	{5,8}
[IN-01] Base de datos	{2,1}	{4,6}	{5,8}
[IN-02] Archivo de datos	{2,1}	{4,6}	{5,8}
[IN-03] Documentación interna	{2,1}	{4,6}	{5,8}
[IN-04] Material Impreso	{4,7}	{5,3}	{4,1}
[IN-05] Carpetas Compartidas	{2,1}	{4,6}	{5,8}
[IS] Servicios internos			
[E] Equipamiento	{5,1}	{4,7}	{5,1}
[SW] Aplicaciones	{4,7}	{4,7}	{5,1}
[SW-01] Motor de base de datos	{4,7}	{4,7}	{4,9}
[SW-02] Repositorio de aplicaciones desarrolladas	{4,7}	{4,7}	{4,9}
[SW-03] Antivirus	{4,7}	{4,7}	{4,9}
[SW-04] Firewall	{4,7}	{4,7}	{5,1}
[SW-05] Licencias	{4,7}	{4,7}	{4,9}
[SW-06] Navegadores	{4,7}	{4,7}	{4,9}
[SW-07] Sistemas Operativos	{4,7}	{4,7}	{4,9}
[HW] Equipos	{4,9}	{2,8}	{4,1}
[HW-01] Dispositivos de almacenamiento	{4,9}	{2,8}	{4,1}
[HW-02] Computadoras	{4,9}	{2,8}	{4,1}
[HW-03] Teléfonos IP	{4,9}	{2,8}	{4,1}
[HW-04] Servidores	{4,9}	{2,8}	{4,1}
[HW-05] Equipos para el funcionamiento de res	{4,9}	{2,8}	{4,1}
[HW-06] Equipo multifuncional	{4,9}	{2,8}	{4,1}
[HW-07] Dispositivos de grabación y fotografía	{4,9}	{2,8}	{4,1}
[HW-08] Radios de comunicación	{4,9}	{2,8}	{4,1}
[COM] Comunicaciones	{5,1}	{3,3}	{4,2}
[RD-01] Ethernet	{5,1}	{3,3}	{4,2}
[RD-02] Red inalámbrica	{5,1}	{3,3}	{4,2}
[RD-03] Red LAN	{5,1}	{3,3}	{4,2}
[RD-04] Red Telefónica	{5,1}	{3,3}	{4,2}
[AUX] Elementos auxiliares	{4,3}	{1,2}	{4,1}
[AUX-01] UPS	{4,3}	{1,2}	{4,1}
[AUX-02] Gererador Eléctrico	{4,3}	{1,2}	{4,1}
[AUX-03] Equipos de climatización	{4,3}	{1,2}	{4,1}
[AUX-04] Mobiliario	{4,3}	{1,2}	{4,1}
[SS] Servicios subcontratados	{5,0}	{5,3}	{4,2}
[SR] Servicios	{5,0}	{5,3}	{4,2}
[SR-01] Telefonía	{4,1}	{4,1}	{2,7}
[SR-02] Internet	{4,1}	{4,1}	{4,0}
[SR-03] Electricidad	{4,0}	{2,8}	
[SR-04] Correo institucional	{5,0}	{5,0}	{4,2}
[SR-05] Soporte a la red	{4,7}	{5,3}	{4,1}
[SR-06] Soporte a los servicios informáticos	{5,0}	{5,0}	{3,0}
[SR-07] Mantenimiento a los equipos	{4,1}	{4,1}	{4,1}
[L] Instalaciones	{4,6}		{5,5}
[IF] Infraestructura	{4,6}		{5,5}
[IF-01] Instalación de red de datos	{4,6}		{5,5}
[IF-02] Instalación de red eléctrica	{4,6}		{5,5}
[IF-03] UPS del centro cableado	{4,6}		{5,5}
[IF-04] Espacio físico DDTI	{4,6}		{5,5}
[P] Personal	{2,9}	{4,2}	{4,2}
[PR-01] Persoanal Administrativo	{2,9}	{4,2}	{4,2}
[PR-02] Personal de desarrollo	{2,9}	{4,2}	{4,2}

Nota: Elaboración propia

Figura 37

Riesgo residual repercutido de los activos del DDTI-FICA mediante el software PILAR



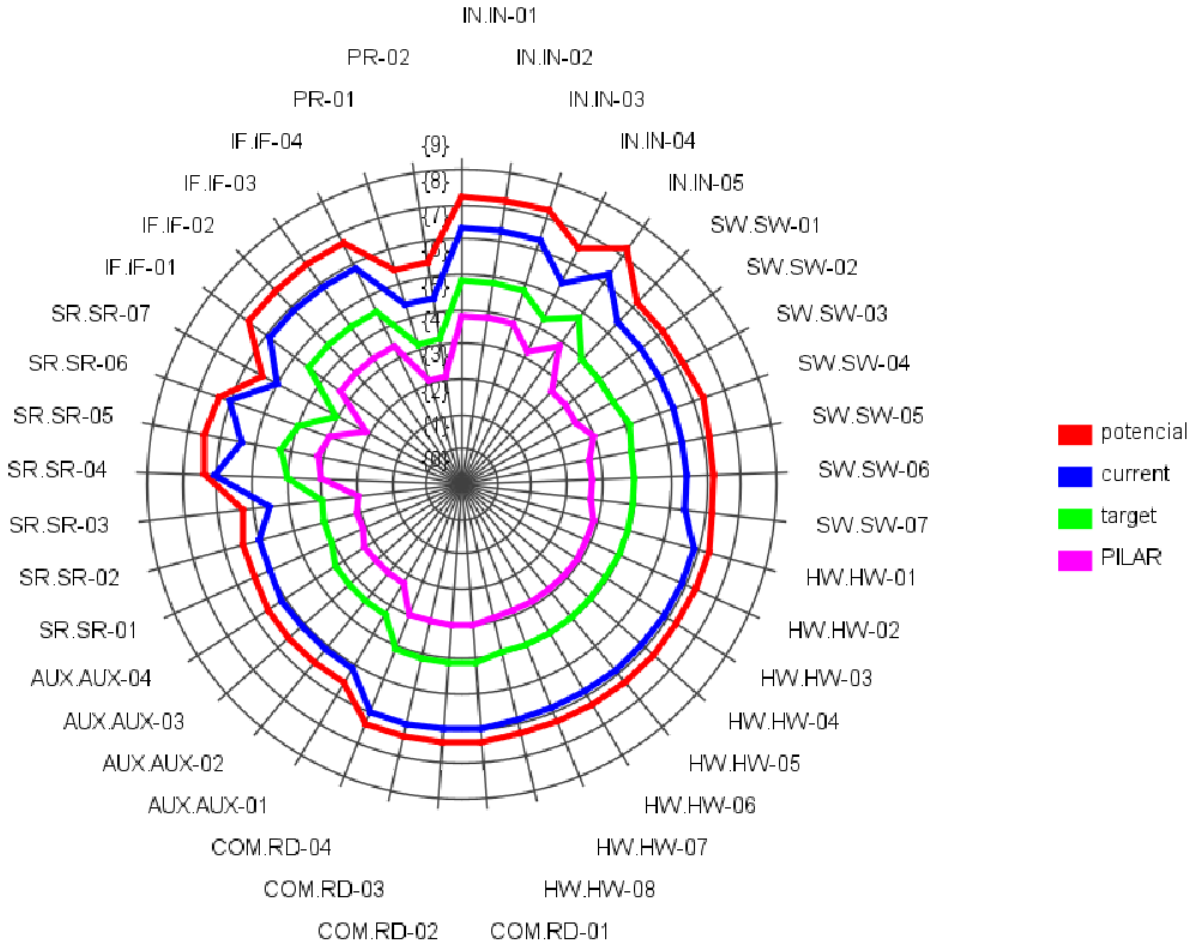
activo	[D]	[I]	[C]
ACTIVOS	{5,1}	{5,3}	{5,8}
[IN-01] Base de datos	{5,1}	{5,3}	{5,8}
[IN-02] Archivo de datos	{5,1}	{5,3}	{5,8}
[IN-03] Documentación interna	{5,1}	{5,3}	{5,8}
[IN-04] Material Impreso	{4,7}	{5,3}	{4,1}
[IN-05] Carpetas Compartidas	{2,1}	{5,3}	{5,8}
[SW-01] Motor de base de datos	{4,7}	{4,7}	{4,9}
[SW-02] Repositorio de aplicaciones desarrolladas	{4,7}	{4,7}	{4,9}
[SW-03] Antivirus	{4,7}	{4,7}	{4,9}
[SW-04] Firewall	{4,7}	{4,7}	{5,1}
[SW-05] Licencias	{4,7}	{4,7}	{4,9}
[SW-06] Navegadores	{4,7}	{4,7}	{4,9}
[SW-07] Sistemas Operativos	{4,7}	{4,7}	{4,9}
[HW-01] Dispositivos de almacenamiento	{4,9}	{2,8}	{4,1}
[HW-02] Computadoras	{4,9}	{2,8}	{4,1}
[HW-03] Teléfonos IP	{4,9}	{2,8}	{4,1}
[HW-04] Servidores	{4,9}	{2,8}	{4,1}
[HW-05] Equipos para el funcionamiento de res	{4,9}	{2,8}	{4,1}
[HW-06] Equipo multifuncional	{4,9}	{2,8}	{4,1}
[HW-07] Dispositivos de grabación y fotografía	{4,9}	{2,8}	{4,1}
[HW-08] Radios de comunicación	{4,9}	{2,8}	{4,1}
[RD-01] Ethernet	{5,1}	{3,3}	{4,2}
[RD-02] Red inalámbrica	{5,1}	{3,3}	{4,2}
[RD-03] Red LAN	{5,1}	{3,3}	{4,2}
[RD-04] Red Telefónica	{5,1}	{3,3}	{4,2}
[AUX-01] UPS	{4,3}	{1,2}	{4,1}
[AUX-02] Gererador Eléctrico	{4,3}	{1,2}	{4,1}
[AUX-03] Equipos de climatización	{4,3}	{1,2}	{4,1}
[AUX-04] Mobiliario	{4,3}	{1,2}	{4,1}
[SR-01] Telefonía	{4,1}	{4,1}	{2,7}
[SR-02] Internet	{4,1}	{4,1}	{4,0}
[SR-03] Electricidad	{4,0}	{2,8}	
[SR-04] Correo institucional	{5,0}	{5,0}	{4,2}
[SR-05] Soporte a la red	{4,7}	{5,3}	{4,1}
[SR-06] Soporte a los servicios informáticos	{5,0}	{5,0}	{3,0}
[SR-07] Mantenimiento a los equipos	{4,1}	{4,1}	{4,1}
[IF-01] Instalación de red de datos	{4,6}		{5,5}
[IF-02] Instalación de red eléctrica	{4,6}		{5,5}
[IF-03] UPS del centro cableado	{4,6}		{5,5}
[IF-04] Espacio físico DDTI	{4,6}		{5,5}
[PR-01] Persoanal Administrativo	{2,9}	{4,2}	{4,2}
[PR-02] Personal de desarrollo	{2,9}	{4,2}	{4,2}

Nota: Elaboración propia

La Figura 38 exhibe un diagrama conciso que resume los riesgos posibles, actuales, deseados y recomendados por el programa PILAR.

Figura 38

Gráfico de valores de riesgo de activos del DDTI-UTN



Nota: Elaboración propia

2.10. Roles y Responsabilidades

En la Tabla 22 se muestra los roles y responsabilidades del personal administrativo dentro del Departamento de Desarrollo Tecnológico e Informático, proporcionando de esta manera una base sólida para comprender su funcionamiento interno.

Tabla 22

Tabla de roles y responsabilidades

Cargo	Responsabilidades
Jefe de proyecto	El jefe del proyecto tiene la responsabilidad de asignar los recursos necesarios, establecer prioridades y coordinar las interacciones con los clientes y usuarios para garantizar que el equipo esté enfocado en alcanzar los objetivos institucionales.
	Además, el líder del proyecto establece prácticas que aseguran la calidad e integridad de los artefactos del proyecto.
	El jefe del proyecto también supervisa la creación de la arquitectura del sistema y optimiza los procesos institucionales para minimizar los tiempos y costos, así como para proporcionar acceso a información integrada, confiable, precisa y oportuna.
	Impulsa y desarrolla proyectos de Tecnología de Información y Comunicación (TIC) para garantizar un buen servicio a la colectividad y optimizar los recursos de la Universidad Técnica del Norte.
Análisis de sistemas	La captura, especificación y validación de los requisitos mediante entrevistas con el cliente y los usuarios, con el objetivo de interactuar de manera efectiva con ellos.
	Elaboración del Modelo de Análisis y Diseño, lo cual implica la creación de un marco conceptual que permita comprender la naturaleza y complejidad del sistema.
	La colaboración en la elaboración de las pruebas funcionales y el modelo de datos es una tarea importante, que implica la participación activa en la definición de los criterios de calidad y en la creación de los modelos que permitan validar la funcionalidad del sistema.
Programador	Generación de prototipos.
	Participación activa en la creación de pruebas funcionales y en la definición del modelo de datos, así como en la verificación conjunta con el usuario para su validación.
Ingeniero de Software	Llevar a cabo diversas actividades para garantizar la calidad del producto final. Entre estas actividades se encuentran la gestión de requisitos, la gestión de configuración y cambios, la elaboración del modelo de datos, la preparación de las pruebas funcionales y la elaboración de la documentación.

Administrador de la red	Impulsar y desarrollar proyectos relacionados con la Tecnología de Información y Comunicación (TIC) que permitan a la Universidad Técnica del Norte funcionar adecuadamente, proporcionando un buen servicio a la comunidad, optimizando el tiempo y reduciendo costos innecesarios.
	Personal con certificaciones internacionales en redes para garantizar la eficiencia y calidad de los servicios ofrecidos.
	Proponer la adquisición de paquetes de software, licencias y hardware adecuados para satisfacer las necesidades tecnológicas de la universidad.
	Asegurar el monitoreo permanente de la red de la universidad las 24 horas del día, garantizando su operatividad al 100%.
	Contar con equipos de monitoreo para supervisar constantemente el funcionamiento de la red universitaria.
Webmaster	Reforzar la gestión de investigación mediante la adopción de medidas efectivas que fomenten y fortalezcan el desarrollo de esta área clave.
	Introducir innovadoras tecnologías en la administración del GeoPortal y en la gestión de las NTIC´s en contextos virtuales, para garantizar una eficaz gestión y un óptimo rendimiento.
	Contribuir activamente en la asistencia y resolución de problemas informáticos relacionados con los planes y proyectos de diversas áreas de la institución, con el fin de mejorar y optimizar los procesos en la institución.
Ingeniero de Hardware	Implementar políticas y procedimientos que rijan la operación y el control de los sistemas informáticos, con el objetivo de garantizar su adecuado funcionamiento y seguridad.
	Coordinar la adquisición de software y hardware especializado que cumpla con las necesidades de la institución, con el fin de resolver de manera satisfactoria los problemas informáticos que puedan surgir.
	Planificar el mantenimiento regular de los equipos informáticos de la Universidad Tecnológica Nacional, a fin de prolongar su vida útil y prevenir fallas o mal funcionamiento.
	Establecer políticas y prácticas para reciclar los materiales y suministros utilizados en los sistemas informáticos, con el propósito de reducir su impacto ambiental y promover la sostenibilidad.

	Diseñar un plan de contingencia para proteger el hardware y la información contenida en los sistemas informáticos ante la ocurrencia de eventos naturales o causados por el hombre.
	Capacitar al personal docente y administrativo de la institución en el uso de medidas y reglas de acceso restringido a los sistemas informáticos, para garantizar la seguridad y la privacidad de la información.
	Contratar servicios de mantenimiento correctivo para los equipos informáticos de la institución, para garantizar su reparación en caso de averías o fallas técnicas.
	Administrar el catálogo electrónico de los equipos informáticos disponibles en el Sistema Nacional de Compras Públicas, para facilitar la gestión y la adquisición de los mismos por parte de la institución.
	Gestionar los contratos de mantenimiento preventivo y correctivo de la institución, para garantizar que se cumplan los acuerdos y se mantengan los equipos en buen estado.
	Administrar los contratos de servicio de mantenimiento correctivo de los proyectores digitales de la institución, para garantizar su funcionamiento adecuado y su reparación en caso de averías.
	Ofrecer soporte técnico en el lugar para resolver problemas técnicos relacionados con los sistemas informáticos, con el fin de minimizar el tiempo de inactividad y mantener la continuidad operativa de la institución.

Nota: Elaboración propia

2.11. Políticas, estándares y procedimientos.

A continuación, se expondrá las distintas políticas que establecen las directrices generales, los estándares que definen los criterios específicos de calidad y los procedimientos que describen pasos detallados para efectuar el SGSI.

2.11.1. Diseño de políticas

Luego de realizar un análisis exhaustivo de los activos de información, así como de sus amenazas, probabilidad e impacto asociados, se ha concluido que existe un alto nivel de riesgo al que estos activos se encuentran expuestos. Por ende, resulta crucial establecer un conjunto de políticas de seguridad de la información, las cuales deberán ser elaboradas y aprobadas por

la máxima autoridad, en colaboración con el comité de seguridad de la información y deberán ser socializadas con todo el personal de la institución. A continuación, se presentan las políticas y controles de seguridad de la información que se han diseñado, teniendo como base los dominios, objetivos de control y controles estipulados en el Anexo A de la norma ISO 27001:2013.

Políticas de seguridad de la información

Su base se establece en el Dominio 5 del Anexo A de la norma ISO 27001:2013.

- Las propuestas de políticas de seguridad de la información se centran en satisfacer las necesidades del Departamento de Desarrollo Tecnológico e Informático de la Institución de Educación Superior, con el objetivo de prevenir, reducir y eliminar los riesgos en el mejor de los casos.
- Es crucial implementar las medidas necesarias para garantizar una gestión adecuada de los activos de información relacionados con el almacenamiento de datos del Departamento de Desarrollo Tecnológico e Informático, así como para establecer los mecanismos necesarios para su implementación y protegerlos de posibles amenazas.
- Se requiere el compromiso de todos los funcionarios y proveedores para mantener la información confidencial de la institución, lo que implica la prohibición de divulgar cualquier tipo de información sin la debida autorización del área correspondiente.

Objetivos

- Garantizar la confidencialidad, integridad y disponibilidad de los activos de información del Departamento de Desarrollo Tecnológico e Informático a fin de minimizar la probabilidad de riesgos y amenazas que puedan afectar el normal desarrollo de las actividades de dicho departamento.

- Fomentar una cultura de seguridad de la información en toda la institución, promoviendo campañas de concienciación y aplicando sanciones en caso de incumplimiento.

Alcance

La política de seguridad de la información elaborada para el DDTI de la UTN se extiende a todo el personal y proveedores, con el objetivo de reducir al mínimo los peligros potenciales que pudieran tener consecuencias desfavorables en la entidad.

Organización de la seguridad de la información

Su base se establece en el dominio 6 del anexo A de la norma ISO 27001:2013.

Roles y responsabilidades

El DDTI, asumirá la responsabilidad de impartir capacitación a todos los miembros de la institución en materia de seguridad de la información. Para apoyar esta tarea, se establecerá un comité de seguridad de la información cuya función será celebrar reuniones periódicas con el objetivo de analizar y mejorar las políticas ya establecidas.

Los miembros que conformen el Comité de Seguridad de la Información pueden incluir a:

- Director del Departamento de Desarrollo Tecnológico e Informático.
- Oficial de seguridad de la información.
- Representantes importantes de los departamentos de la institución que administran datos críticos.
- Representantes legales y de recursos humanos.
- Auditores internos y/o externos.

Responsabilidades del comité de seguridad de la información

- Aprobar y gestionar de las políticas y normas relacionadas con la seguridad de la información**.**

- Vigilar y supervisar de cerca los cambios importantes de los riesgos que puedan afectar a los recursos de información, considerando las amenazas presentes.
- Mantener una supervisión constante de los incidentes que tengan un impacto alto, de manera que se puedan tomar las medidas necesarias de manera oportuna.
- Asegurar que se implementen los controles necesarios para los nuevos sistemas o servicios, con el fin de garantizar la seguridad de la información.
- Fomentar y difundir la importancia de la seguridad de la información en toda la institución, para garantizar que todos los empleados tomen medidas adecuadas para proteger la información.
- El comité debe reunirse de manera periódica (cada dos meses) o cuando las circunstancias lo requieran, y se deben llevar registros y actas detalladas de todas las reuniones.
- Establecer y mantener actualizado un registro detallado de las nuevas amenazas y vulnerabilidades en materia de seguridad de la información.
- Coordinar el proceso para garantizar la continuidad de los servicios y sistemas de información de la institución en caso de incidentes imprevistos.
- Fortalecer y mantener el contacto con grupos de interés especializados en el ámbito de la seguridad de la información.

2.11.2. Diseño de estándares

Políticas de gestión de activos

Su base se establece en el dominio 8 del anexo A de la norma ISO 27001:2013.

1. **Responsabilidad por los activos**

Objetivo: Identificación de los activos organizacionales y establecimiento de las tareas que deben llevarse a cabo para garantizar su protección adecuada.

Controles

- El Departamento de Desarrollo Tecnológico e Informático es responsable de mantener un registro actualizado de todos los activos de información y su gestión correspondiente.
- Cada activo de información debe tener un propietario designado, quien será responsable de proteger el activo y definir los permisos de acceso para los usuarios o grupos de usuarios autorizados.
- Para garantizar el uso adecuado de los activos de información, se deben establecer políticas documentadas y revisarlas regularmente, con el entendimiento de que los activos de información asignados a un empleado solo deben utilizarse para fines laborales.
- Se recomienda que se realice un acta de entrega-recepción al asignar los activos de información para establecer el uso responsable y garantizar la devolución de los mismos al finalizar el empleo, con la firma correspondiente.
- En caso de que se detecte el deterioro del activo de información asignado, se aplicarán las sanciones correspondientes según el tipo de daño.

2. Clasificación de la información

Objetivo: Garantizar que la información sea debidamente resguardada en función de su relevancia para la empresa.

Controles

- Una vez que se ha establecido la propiedad de la información, es necesario llevar a cabo una clasificación basada en su nivel de importancia**.**
- La información debe ser etiquetada de acuerdo con las directrices de etiquetado adoptadas por la Departamento de Desarrollo Tecnológico e Informático, considerando los diferentes formatos físicos y electrónicos disponibles.

- Al manipular la información, es crucial considerar tanto su clasificación como su propiedad, especialmente para garantizar la confidencialidad de la información crítica o sensible para el Departamento de Desarrollo Tecnológico e Informático.

3. Manejo de medios

Objetivo: Evitar la exposición, cambio, eliminación o destrucción no autorizadas de la información guardada en los soportes digitales.

Controles

- La administración de los dispositivos de almacenamiento extraíbles será efectuada en línea con el modelo de categorización implementado por el Departamento de Desarrollo Tecnológico e Informático.
- Se requiere establecer un protocolo seguro y apropiado para el retiro adecuado de los dispositivos de almacenamiento extraíbles.
- Para proteger la confidencialidad de la información exclusiva de la institución, se debe garantizar medidas de seguridad apropiadas contra la divulgación, mal uso o acceso no autorizado durante el transporte de dichos dispositivos.

Políticas de control de acceso

Su base se establece en el dominio 9 del anexo A de la norma ISO 27001:2013.

Objetivo: Garantizar que únicamente los usuarios autorizados tengan acceso a los sistemas y servicios, y evitar cualquier tipo de acceso no autorizado.

Controles

- El departamento responsable de la gestión de los sistemas informáticos debe establecer políticas y normas para regular el acceso y restringirlo, si fuera

necesario. Estas políticas deben ser documentadas, revisadas y aprobadas por el comité encargado de la seguridad de la información.

- En función de las responsabilidades asignadas a cada empleado o proveedor, se les concederá acceso a la red y a los servicios autorizados de la misma.
- Se debe establecer un proceso formal para registrar y cancelar los derechos de acceso de los usuarios a los sistemas de información exclusivos de la institución.
- La asignación y uso de derechos de acceso privilegiados deben ser restringidos y controlados mediante la autenticación. Debe considerarse también la gestión de aspectos relacionados con el teletrabajo.
- En función de la clasificación y propiedad de los activos de información, es necesario revisar regularmente los derechos de acceso de los usuarios.
- Los derechos de acceso deben retirarse cuando finaliza el empleo o cuando se produce un cambio en las funciones del usuario dentro de la institución.
- Todos los usuarios de los sistemas de información de la institución tienen la responsabilidad de cumplir con las mejores prácticas y políticas definidas en cuanto al uso de la información.
- Con el propósito de limitar el ingreso no autorizado a sistemas de información y aplicaciones, se requiere implementar un sistema de gestión de contraseñas. Se recomienda seguir ciertas pautas para la creación y uso de contraseñas:
    a. No se deben utilizar términos comunes o información personal para crear las contraseñas.
    b. La longitud mínima de la contraseña debe ser de ocho caracteres alfanuméricos.
    c. Es obligatorio cambiar la contraseña la primera vez que se ingresa al sistema de información.

d. La contraseña debe ser actualizada al menos cada 30 días o según lo indique el Departamento de Desarrollo Tecnológico e Informático.
e. Las contraseñas no deben ser compartidas ni expuestas a la vista de terceros.
f. Se debe evitar usar las mismas contraseñas para asuntos personales y laborales.

- Si un funcionario o proveedor necesita acceso a los sistemas de información o aplicaciones, debe hacer una solicitud al Departamento de Desarrollo Tecnológico e Informático.
- El Departamento de Desarrollo Tecnológico e Informático tiene la responsabilidad de controlar el acceso a los códigos fuente de los programas.
- Los proveedores pueden usar sus dispositivos móviles personales en el entorno laboral, pero no pueden acceder a la información de la institución.

Políticas de criptografía

Su base se establece en el dominio 10 del anexo A de la norma ISO 27001:2013.

Objetivo: Garantizar una utilización idónea y efectiva de la criptografía con el fin de salvaguardar la privacidad, veracidad y/o coherencia de los datos.

Controles

- Es necesario que el Departamento de Desarrollo Tecnológico e Informático establezca y aplique principios rigurosos en cuanto a la implementación de controles criptográficos, a fin de salvaguardar adecuadamente la información de la institución.
- El Departamento de Desarrollo Tecnológico e Informático debe establecer y emplear procedimientos claros para la gestión, seguridad y vida útil de las claves

criptográficas, con el fin de garantizar la protección adecuada de la información sensible.

Políticas de seguridad física y del entorno

Su base se establece en el dominio 11 del anexo A de la norma ISO 27001:2013.

Objetivo: Garantizar la integridad de la información y los sistemas de la organización mediante el uso de procedimientos de seguridad física para evitar el acceso no autorizado y proteger contra la interferencia y los daños.

Controles

- Es imperativo que el Departamento de Desarrollo Tecnológico e Informático establezca medidas de seguridad perimetral para proteger la infraestructura de procesamiento y almacenamiento de información de posibles amenazas.
- Es necesario implementar medidas de control de acceso físico al Departamento de Desarrollo Tecnológico e Informático, como cerraduras electrónicas, biométricas o con combinación, para verificar la identidad del personal autorizado y garantizar la seguridad del departamento.
- Todos los empleados de la institución deben tener una identificación que les permita acceder de manera segura al departamento, y a los visitantes se les debe proporcionar una identificación provisional. Además, es importante llevar un registro de entrada y salida del departamento.
- Se debe contar con protección física para prevenir posibles daños causados por desastres naturales o provocados por el hombre, como incendios, terremotos o explosiones.

- El Departamento de Desarrollo Tecnológico e Informático debe cumplir con los requisitos mínimos de seguridad en su infraestructura para garantizar el correcto funcionamiento de las operaciones.
- Cualquier retirada o traslado de equipos debe ser autorizado por el líder del Departamento de Desarrollo Tecnológico e Informático.
- El Departamento de Desarrollo Tecnológico e Informático debe tener un sistema de cableado estructurado que garantice la seguridad de los equipos y separe el cableado eléctrico de la red de datos para evitar interferencias y prevenir la interceptación de datos.
- Es importante llevar a cabo mantenimientos programados en los equipos del Departamento de Desarrollo Tecnológico e Informático, probar el sistema de energía ininterrumpida y adquirir un sistema de detección y supresión de incendios y un sistema de aire acondicionado.
- Todos los usuarios deben proteger sus equipos con contraseñas y protectores de pantalla cuando no estén en uso, y los puestos de trabajo deben mantenerse limpios de papeles y medios de almacenamiento extraíbles.

Políticas de seguridad de las operaciones

Su base se establece en el dominio 12 del anexo A de la norma ISO 27001:2013.

Objetivo: Garantizar el óptimo desempeño y seguridad de las plataformas de procesamiento de datos.

Controles

- Es necesario mantener una documentación actualizada y accesible de los procedimientos operativos para garantizar su uso y actualización cuando sea necesario.

- El comité de seguridad de la información debe reunirse periódicamente para considerar y aprobar las solicitudes de cambios en los activos clasificados según su importancia.
- Todos los sistemas de información de la institución deben sincronizar sus relojes con una única fuente de tiempo de referencia.
- El Departamento de Desarrollo Tecnológico e Informático debe realizar una evaluación del uso y capacidad de los sistemas de información actuales y futuros para optimizar su rendimiento y cumplir con los objetivos organizacionales.
- El Departamento de Desarrollo Tecnológico e Informático debe proporcionar controles de prevención y detección de software malicioso y medidas para la recuperación de incidentes.
- Es obligatorio realizar copias de seguridad de la información crítica y sensible, con una persona responsable asignada por el comité de seguridad de la información para su almacenamiento y verificación del funcionamiento adecuado.
- Las actividades de los administradores y usuarios de los sistemas de información deben registrarse y almacenarse adecuadamente para su posterior revisión.
- El Departamento de Desarrollo Tecnológico e Informático está autorizada para instalar software en los sistemas de información, y no se permite la instalación de software ajeno a la institución.
- El Departamento de Desarrollo Tecnológico e Informático debe realizar pruebas de penetración éticas para mantener el control sobre las vulnerabilidades técnicas de los sistemas de información.

Políticas de seguridad en las comunicaciones

Su base se establece en el dominio 13 del anexo A de la norma ISO 27001:2013.

Objetivo: Garantizar la seguridad de los datos que transitan por las redes y de los sistemas que sustentan el procesamiento de información.

Controles

- Es necesario que el Departamento de Desarrollo Tecnológico e Informático implemente medidas de seguridad y de transmisión segura para la transferencia de información a través de la red, tanto para los servicios propios como para los contratados.
- Es recomendable diseñar y aplicar el uso de vlans para separar las redes según las áreas o unidades de trabajo dentro de la institución.
- Es importante utilizar firewall, IPS, IDS y llevar un registro de incidentes para controlar las eventualidades y el comportamiento de la red.
- Se recomienda contar con autorización del Departamento de Desarrollo Tecnológico e Informático para conectar cualquier dispositivo a la red.
- Se deben establecer controles para garantizar la transferencia segura de información mediante el uso de métodos de encriptación o protocolos seguros que impidan la modificación, interceptación o eliminación de información.
- Es fundamental documentar adecuadamente la configuración realizada en los equipos, como routers, switches, firewall, etc.
- Los servicios externos deben contar con cláusulas definidas para garantizar la transferencia de información segura.
- La información transmitida por mensajería electrónica debe protegerse adecuadamente, y los usuarios no deben abrir correos electrónicos desconocidos que contengan archivos adjuntos. Es importante contar con un antivirus legal.

- El Departamento de Desarrollo Tecnológico e Informático debe determinar el tamaño máximo permitido para los archivos adjuntos, y se debe realizar mantenimiento periódico de las cuentas de correo electrónico.
- Toda información transmitida por la red interna de la institución puede ser auditada por el Departamento de Desarrollo Tecnológico e Informático cuando lo considere necesario.

Políticas para adquisición, desarrollo y mantenimiento de sistemas de información

Su base se establece en el dominio 14 del anexo A de la norma ISO 27001:2013.

Objetivo: Asegurar la inclusión de medidas de seguridad de la información en todos los sistemas de información durante todo su ciclo de vida es una estrategia clave. Es importante tener en cuenta que esta estrategia también debe considerar los requisitos de seguridad para los sistemas de información que brindan servicios a través de redes públicas.

Controles

- Los requerimientos de seguridad de la información deben ser incluidos en los requisitos de los nuevos sistemas de información o en las mejoras a los sistemas existentes, para garantizar la seguridad de la información.
- Es necesario proteger la información transmitida a través de redes públicas de cualquier actividad fraudulenta, disputa contractual, revelación o modificación no autorizadas, mediante medidas de seguridad adecuadas.
- Es fundamental proteger la información involucrada en las transacciones de servicios de aplicaciones para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada, revelación, duplicación o reproducción de mensajes no autorizados, mediante medidas de seguridad adecuadas.

- Las reglas para el desarrollo de aplicaciones y sistemas deben ser establecidas y aplicadas dentro de la institución, para asegurar que se sigan buenas prácticas de desarrollo seguro.
- El desarrollo de cambios a lo largo del ciclo de vida del desarrollo debe ser controlado mediante procedimientos formales de control de cambios, para garantizar que los cambios sean gestionados de manera adecuada y segura.
- Al modificar los sistemas operativos, es importante revisar y probar las aplicaciones críticas para asegurar que no se afecten las operaciones o la seguridad de la institución.
- Las modificaciones en los paquetes de software deben ser desaconsejadas, y todos los cambios necesarios deben estar sujetos a un control riguroso para garantizar que se gestionen de manera segura.
- Los principios de ingeniería de sistemas seguros deben ser establecidos, documentados, mantenidos y aplicados en todos los esfuerzos de implementación de sistemas de información, para garantizar que se sigan buenas prácticas de seguridad.
- La institución debe establecer y proteger adecuadamente los ambientes de desarrollo seguros para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida del sistema, para garantizar que se desarrollen de manera segura.
- El desarrollo de software externalizado debe ser supervisado y controlado por la institución para garantizar que se sigan buenas prácticas de desarrollo seguro.
- Las pruebas de seguridad funcional deben ser llevadas a cabo durante el desarrollo, para asegurar que el sistema esté libre de vulnerabilidades y que cumpla con los estándares de seguridad.

- Los programas de pruebas de aceptación y criterios relacionados deben ser establecidos para nuevos sistemas de información, actualizaciones y nuevas versiones, para garantizar que los sistemas sean seguros y funcionales.
- Es necesario seleccionar cuidadosamente los datos de prueba, protegerlos y controlarlos, para garantizar que se utilicen de manera segura y adecuada.

Políticas de relación con los proveedores

Su base se establece en el dominio 15 del anexo A de la norma ISO 27001:2013.

Objetivo: Mantener un nivel de seguridad de la información y la prestación de servicios en línea que sea compatible con los acuerdos establecidos con los proveedores.

Controles

- En cuanto a la información, se acordará con los proveedores de servicios los términos para su acceso, manejo o modificación.
- Departamento de Desarrollo Tecnológico e Informático, en colaboración con los proveedores de servicios, debe establecer y registrar las políticas de seguridad de la información con el objetivo de reducir los riesgos relacionados con el acceso de los proveedores a los activos del departamento en cuestión.
- El Departamento de Desarrollo Tecnológico e Informático deberá supervisar y auditar regularmente los servicios ofrecidos por los proveedores para garantizar su control y calidad.

Políticas para la gestión de incidentes de seguridad de información

Su base se establece en el dominio 16 del anexo A de la norma ISO 27001:2013.

Objetivo: Garantizar la aplicación de un enfoque efectivo y coherente en la administración de incidentes de seguridad de la información, lo cual involucra la notificación y la comunicación de vulnerabilidades y sucesos de seguridad.

Controles

- El comité de seguridad de la información debe establecer un conjunto claro de responsabilidades y procedimientos para garantizar que se pueda proporcionar una respuesta eficaz y eficiente a los incidentes de seguridad de la información que puedan surgir.
- Es importante mantener un registro detallado de los incidentes relacionados con la seguridad de la información que sean reportados al Departamento de Desarrollo Tecnológico e Informático, para que puedan ser revisados posteriormente con el fin de mejorar los procedimientos y evitar futuros incidentes.
- Todos los incidentes de seguridad de la información deben ser evaluados en función de su nivel de criticidad y tratados en consecuencia, para garantizar que se tomen medidas adecuadas para mitigar los riesgos y minimizar los daños.
- Es crucial aprender de los incidentes de seguridad de la información ocurridos en el pasado y de las acciones tomadas para fortalecer las políticas y procedimientos de seguridad, con el objetivo de prevenir incidentes futuros y proteger adecuadamente la información sensible de la institución.

Políticas para la continuidad del negocio

Su base se establece en el dominio 17 del anexo A de la norma ISO 27001:2013.

Objetivo: Es fundamental integrar la seguridad de la información en el marco de la gestión de continuidad de negocio de la organización, a fin de asegurar la sostenibilidad operativa y la salvaguarda de los recursos estratégicos de la compañía.

Controles

El Departamento de Desarrollo Tecnológico e Informático tiene la responsabilidad de identificar y documentar los requisitos normativos y contractuales para la seguridad de la información, a fin de prevenir posibles sanciones a la organización o a sus funcionarios por incumplimientos.

- Es necesario que el Departamento de Desarrollo Tecnológico e Informático realice revisiones periódicas de los controles, políticas y procedimientos que ha definido en relación con la seguridad de la información.
- El Departamento de Desarrollo Tecnológico e Informático debe establecer los requisitos y medidas de seguridad necesarias para afrontar situaciones desfavorables en relación con la información.
- Para garantizar la seguridad de la información, es imprescindible almacenarla en un lugar seguro y las instalaciones de procesamiento de información deben contar con la redundancia necesaria para cumplir con los requisitos de disponibilidad.

Políticas de cumplimiento

Su base se establece en el dominio 18 del anexo A de la norma ISO 27001:2013.

Objetivo: Prevenir el quebrantamiento de las disposiciones legales, normativas o contractuales que atañen a la seguridad de la información o a los estándares de seguridad exigidos.

Controles

- El Departamento de Desarrollo Tecnológico e Informático debe ser responsable de establecer, documentar y mantener actualizados todos los requisitos legales, normativos y contractuales relacionados con cada sistema de información.
- El Departamento de Desarrollo Tecnológico e Informático debe implementar procedimientos adecuados para cumplir con los requisitos legales, normativos y

contractuales en relación con los derechos de propiedad intelectual y el uso de productos de software propietario.

- Es importante proteger los registros de la información almacenada en los sistemas informáticos, mediante medidas que prevengan hurto, destrucción, modificación, acceso no autorizado o divulgación.
- Debe garantizarse la protección de la privacidad y datos personales según lo estipulado en la legislación y normativas aplicables.
- El Departamento de Desarrollo Tecnológico e Informático debe realizar revisiones regulares para asegurar el cumplimiento de las políticas de seguridad de la información establecidas.

2.11.3. Diseño de procedimientos

Una vez que se han determinado las políticas adecuadas para cada uno de los controles a ser implementados, con el objetivo de satisfacer las necesidades del DDTI, se detallan los procedimientos siguientes, los cuales aún no han sido aplicados en la organización y se alinean con algunos de los controles previamente mencionados:

PROCEDIMIENTO DE ELABORACIÓN Y EJECUCIÓN DEL PLAN DE CAPACITACIÓN

Su base se establece en el dominio 7.2.2 del anexo A de la norma ISO 27001:2013

Objetivo: Implementar actividades destinadas a educar al personal acerca de las medidas de seguridad y confidencialidad que influyen en el cumplimiento de sus funciones.

Contenido

1. Analizar y determinar los requerimientos de formación en materia de seguridad de la información.
2. Identificar proveedores externos que puedan cubrir las necesidades de capacitación en seguridad de la información.

3. Evaluar los cronogramas de los proveedores en función de las necesidades específicas de la institución.
4. En caso de que los cronogramas sean adecuados, elaborar un plan de capacitación que incluya los beneficiarios, el presupuesto y se ajuste a las necesidades de la institución. Si los cronogramas no son adecuados, coordinar con el proveedor para ajustarlos o buscar otros proveedores de capacitación.
5. Revisar el plan de capacitación en coordinación con el asistente de talento humano y realizar los ajustes necesarios.
6. Durante la reunión, se llevará a cabo una revisión exhaustiva del cronograma de capacitación, se realizarán ajustes necesarios y se aprobará el plan.
7. Una vez aprobado el cronograma de capacitación, se difundirá entre los jefes de área y se emitirán las observaciones pertinentes.
8. Con base en el cronograma de capacitación aprobado, se elaborará un calendario mensual de capacitación y se coordinará la ejecución de los eventos de manera eficiente.
9. Se llevará a cabo una negociación y ajuste con los instructores para establecer el calendario mensual de capacitación de manera óptima.
10. Es necesario coordinar con el personal pertinente la aprobación del calendario de capacitación para asegurarse de que se cumplan los objetivos establecidos.
11. En caso de que el evento sea interno:
    a. Coordinar la inscripción de los participantes del evento de capacitación y establecer los términos de facturación y pago con el proveedor correspondiente.
    b. Enviar invitaciones por correo electrónico al personal involucrado para asistir al evento de capacitación.

c. Después del evento, recibir y archivar copias del certificado como evidencia de asistencia al evento de capacitación.
d. Recopilar copias de toda la documentación original del curso.
e. Evaluar si el beneficiario de la capacitación debe compartir sus conocimientos con el personal de la institución.
f. Si no es necesario compartir conocimientos, proceder con el pago al proveedor. Si es necesario compartir conocimientos, continuar con la actividad 12.

12. En caso de que el evento sea externo, las tareas que se deben llevar a cabo son las siguientes:
    a. Coordinar todos los aspectos logísticos del evento de capacitación interna, como el lugar, transporte, alimentación, materiales de apoyo, entre otros, asegurándose de que se cumplan todas las necesidades de los participantes.
    b. Crear y enviar las invitaciones para el evento de capacitación interna, informando a los participantes acerca de los objetivos, fechas, horarios y otros detalles relevantes.
    c. Llevar a cabo el evento de capacitación interna, asegurándose de que el contenido se presente de manera efectiva y que se cumplan todos los objetivos de aprendizaje.
    d. Al término del evento, llevar a cabo la evaluación del mismo, para determinar qué aspectos funcionaron bien y cuáles se pueden mejorar en el futuro.
    e. Entregar los certificados de capacitación a los participantes y registrar el evento de capacitación.

f. Si la institución se encarga de realizar la evaluación, se debe continuar con la actividad "g", de lo contrario, continuar con la actividad "i".
g. Realizar el análisis y tabulación de las evaluaciones de capacitación llevadas a cabo por los participantes, para determinar las áreas de mejora.
h. Entregar los resultados de las evaluaciones realizadas por los participantes del evento de capacitación interna, ya sea a cargo del instructor interno o externo.
i. Archivar los resultados tabulados de las evaluaciones en las carpetas de capacitaciones, para poder consultarlos en el futuro.
j. Si el evento se lleva a cabo con un instructor interno, coordinar con él la facturación y forma de pago y pagar al proveedor correspondiente. En caso contrario, solo se debe hacer el pago al proveedor.

PROCEDIMIENTO DE GESTIÓN Y CLASIFICACIÓN DE ACTIVOS

Su base se establece en el dominio 8 del anexo A de la norma ISO 27001:2013

Objetivo: Realizar tareas que posibiliten la categorización, reconocimiento y medición precisa de los activos en posesión de la entidad.

Contenido

1. Identificación y cuantificación adecuada de los activos de información: Los profesionales responsables de los procesos correspondientes deben llevar a cabo actividades que permitan identificar los activos de información bajo su cargo, a través de un registro que contemple información detallada como el ID del activo, su nombre, descripción, ubicación, medio de conservación, responsable y propietario. Se debe designar una parte específica de la institución para llevar el control de todos los activos de información.

2. Definición de los activos de información: Los colaboradores designados de los procesos deben establecer los criterios para la inclusión de los activos de información en la matriz de inventarios de activos, su clasificación y publicación, teniendo en cuenta los requerimientos legales, el valor, la criticidad, la susceptibilidad o la divulgación para determinar cuáles activos son más críticos e impactantes para la institución.
3. Revisión periódica de los activos de información: Se establecerá una periodicidad anual para la revisión y actualización del inventario de activos de información, aunque podrá cambiar si surgen necesidades adicionales.
4. Consolidación y actualización de los activos de información: La consolidación del inventario y su actualización deben llevarse a cabo anualmente o cada vez que la institución lo considere necesario.

PROCEDIMIENTO DE CONTROL DE ACCESO U SALIDA DE VISITANTES

Su base se establece en el dominio 9 del anexo A de la norma ISO 27001:2013

Objetivo: Controlar y documentar la entrada y salida de visitantes y equipos en las instalaciones de la organización con el objetivo de proteger la integridad y la seguridad de los empleados, así como los bienes e infraestructura de la institución.

Contenido

Procedimiento de acceso:

1. Solicitar al visitante una identificación personal (preferentemente la cédula de ciudadanía) y obtener información acerca de la persona que desea visitar.
2. Verificar la identidad del visitante mediante la documentación presentada y contactar telefónicamente al destinatario para obtener la autorización de ingreso.
3. Si el visitante no tiene permiso para ingresar, devolver su documento de identificación y explicar las razones por las cuales no puede ser atendido,

informando de una posible cita en el futuro (si es necesario) y finalizando el proceso. Si el visitante es autorizado para ingresar, registrar su información en el registro de visitas, retener su documento de identificación y entregar una credencial de "visitante".

4. Identificar visualmente si el visitante lleva algún tipo de equipo.
5. Si el visitante lleva algún equipo, registrar la información del mismo en el registro de visitas, autorizar su ingreso, proporcionar información sobre cómo llegar a su destino y dar instrucciones sobre el uso de la credencial.
6. Si el visitante no lleva ningún equipo, permitir su ingreso, proporcionar información sobre cómo llegar a su destino y dar instrucciones sobre el uso de la credencial.

Procedimiento de salida:

7. Al momento de que el visitante abandone las instalaciones, es necesario solicitarle que entregue su tarjeta de visita y su documento de identificación para registrar su salida.
8. Es importante verificar si el visitante se retira con algún equipo o material del departamento.
9. Si el visitante no lleva ningún equipo consigo, registrar la hora de salida en la bitácora y permitir su salida. En caso contrario, proceder a la actividad 10.
10. Verificar si los equipos que el visitante se lleva corresponden a los mismos que había ingresado en su momento, basándose en la información de la bitácora.
11. Si los equipos que el visitante se lleva coinciden con los que había ingresado, registrar la hora de salida en la bitácora y permitir que abandone el lugar. En caso contrario, continuar con la actividad 12.
12. Solicitar autorización para la salida de los equipos y verificar cuáles serán retirados.

13. Es necesario verificar si hay alguna situación de seguridad que requiera atención especial.
14. Si no se presenta ninguna novedad, registrar la hora de salida en la bitácora y permitir que el visitante se retire. Si existe alguna situación, se debe notificar al jefe de servicios generales y tomar las medidas necesarias, además de registrar el detalle en la bitácora.

PROCEDIMIENTO PARA MANTENIMIENTO DE EQUIPOS INFORMÁTICOS

Su base se establece en el dominio 11.2.4 del anexo A de la norma ISO 27001:2013

Objetivo: Optimiza el uso de recursos tecnológicos de la organización para proporcionar a los usuarios acceso actualizado, oportuno y confiable a recursos e información en línea mediante la garantía de la disponibilidad de los recursos de hardware y software de cómputo y comunicación.

Contenido

1. Supervisar la infraestructura de Windows, servidores virtuales, infraestructura de Linux, hosts de virtualización, servidores de prueba, equipos de comunicación y data centers.
2. Se debe verificar si durante el monitoreo se registró algún incidente.
3. En caso de no existir incidentes, se registra el monitoreo en la bitácora y finaliza el procedimiento.
4. Si se registran incidentes, se debe analizar la situación y determinar sus causas para identificar el origen del incidente.
5. Se debe verificar si el incidente está registrado en la base de conocimiento.
6. Si el incidente está registrado en la base de conocimiento, se busca la solución en la base y se avanza a la actividad 12.

7. Si el incidente no está registrado en la base de conocimiento, se debe determinar si el origen del incidente es interno o externo.
8. Se debe verificar si el origen del incidente es interno.
9. Si el origen del incidente es interno, se avanza a la actividad 11.
10. Si el origen del incidente es externo, se informa al jefe de tecnología sobre el incidente para que coordine con el proveedor las acciones a tomar y se avanza a la actividad 12.
11. Se informa al jefe de tecnología sobre el incidente, se analiza y definen las acciones a tomar.
12. Se ejecutan las acciones definidas y se determina si los incidentes han sido eliminados.
13. Se debe verificar si el incidente ha sido solucionado.
14. Si el incidente no ha sido solucionado, se definen nuevas acciones para eliminarlo y se coordina con el proveedor si es necesario, regresando a la actividad 18.
15. Si el incidente ha sido solucionado, se informa a los usuarios sobre la solución de novedades, si corresponde.
16. Se registra en la bitácora de administración de equipos las acciones tomadas.
17. Semestralmente se realiza el mantenimiento periódico de los equipos de usuario final.
18. Se debe verificar si existen incidentes.
19. Si existen incidentes, se analiza la situación y se determinan las causas para identificar el origen del incidente, regresando a la actividad 5.
20. Si no existen incidentes, se registra el monitoreo en la bitácora.

PROCEDIMIENTO DE GESTIÓN DE CAMBIOS

Su base se establece en el dominio 12.1.2 del anexo A de la norma ISO 27001:2013

Objetivo: Establecer un conjunto de directrices para la gestión de cambios relacionados con la infraestructura tecnológica del centro de datos principal de la organización. Estas directrices buscan garantizar la reducción de riesgos que puedan afectar negativamente la confidencialidad, disponibilidad o integridad de la información de la plataforma tecnológica.

Contenido

1. Registro del Cambio: En esta actividad, el solicitante ingresa la información correspondiente al cambio propuesto a través del formulario de requerimiento de cambios.
2. Validación del Cambio: En esta actividad se revisa minuciosamente todo lo relacionado con el tipo de cambio solicitado para verificar la exactitud de los procedimientos, documentación, factibilidad, impacto, planeación, etc. De esta manera, se determina si el cambio procede o no. Si el cambio no procede, se devuelve el formulario al usuario para que lo corrija y vuelva a la actividad 1. Si el cambio procede, el proceso continúa a la actividad "Validar Riesgos de Seguridad" y luego a la actividad 3.
3. Validar Riesgos de Seguridad: En esta actividad se valida si el cambio propuesto afecta la disponibilidad, confidencialidad e integridad de la información.
4. Determinar la Prioridad: Se determina si el cambio es estándar, normal o de emergencia. Si y solo si el cambio es estándar, el proceso continúa a la actividad "Actualizar Cronogramas" y luego a la actividad 6.
5. Evaluación del Cambio: Se evalúa si la solicitud de cambio (RFC) será autorizada o rechazada. Si es autorizado, el proceso continúa a la actividad "Actualizar Cronogramas" y luego a la actividad 6. Si es rechazado, el proceso continúa a la actividad "Enviar Notificación de Rechazo" y luego a la actividad 10.
6. Actualizar Cronogramas: Se detallan las actividades, fecha y hora de la ejecución del cambio.

7. Implementación del Cambio: En esta fase, el especialista o coordinador del cambio planifica, comunica a las personas afectadas y ejecuta la implementación del cambio. Si el cambio es exitoso, el proceso continúa a la actividad "Cierre del Cambio" y luego a la actividad 9. Si el cambio no es exitoso, el proceso continúa a la actividad "Plan Rollback" y luego a la actividad 8.
8. Plan Rollback: Si el cambio implementado no es exitoso, se deberá volver el servicio al estado inicial.
9. Cierre del Cambio: Después de evaluar la implementación del cambio, se procede con el cierre del mismo, indicando el resultado de esta.
10. Enviar Notificación de Rechazo: Se enviará una notificación a través de correo electrónico al usuario solicitante en caso de que la solicitud de cambio sea rechazada.

PROCEDIMIENTO PARA EL RESPALDO PERIÓDICO DE INFORMACIÓN

Su base se establece en el dominio 12.3 del anexo A de la norma ISO 27001:2013

Objetivo: Implementar medidas de seguridad informática para prevenir y mitigar riesgos de ataques cibernéticos y proteger la confidencialidad, integridad y disponibilidad de la información crítica para la institución.

Contenido

1. Examinar la frecuencia con la que se realiza la copia de seguridad.
2. En caso de que se realice una copia de seguridad diaria, es importante verificar y validar el proceso automático de obtención de copias de seguridad y registrar los detalles relevantes en la bitácora de respaldos, incluyendo el tipo de copia de seguridad, la fecha de extracción, el nombre del archivo, observaciones pertinentes y la firma de la persona encargada de realizar la copia. Si no se realiza una copia diaria, se debe proceder a la actividad 3.

3. Realizar la obtención de la copia de seguridad y registrar los detalles en la bitácora de respaldos, incluyendo el tipo de copia de seguridad, la fecha de extracción, el nombre del archivo, observaciones pertinentes y la firma de la persona encargada de realizar la copia de seguridad.
4. Preparar el medio de respaldo para su envío al área de seguridad de la información, registrando la fecha de envío en la bitácora mediante un acta de entrega-recepción. Entregar el medio de respaldo al área de seguridad de la información y registrar la fecha de envío y entrega en la bitácora mediante acta.
5. El analista de seguridad debe recibir el medio de respaldo y responsabilizarse de su resguardo y custodia.
6. El analista de seguridad debe decidir la ubicación donde almacenará la copia de respaldo y registrarla en la bitácora.

Nota: Se debe tener en cuenta que, en caso de contener información sensible, las copias deben estar cifradas para garantizar su confidencialidad.

PROCEDIMIENTO DE ADMINISTRACIÓN DE REDES Y COMUNICACIONES

Su base se establece en el dominio 13.1 del anexo A de la norma ISO 27001:2013

Objetivo: Asegurar la accesibilidad y disponibilidad óptimas de la red a través de una gestión eficiente de los recursos tecnológicos de la institución. Este enfoque se centrará en permitir que los usuarios compartan información actualizada, veraz y confiable en línea.

Contenido

1. Supervisar las alertas de comunicación LAN y WAN y registrar cualquier cambio significativo en el registro de la red.
2. Realizar un seguimiento del ancho de banda disponible en el canal y registrar cualquier novedad relevante en el registro de la red.

3. Evaluar el rendimiento del servicio de correo electrónico y registrar cualquier problema o novedad relevante.
4. Realizar un seguimiento de la disponibilidad de la conexión a internet y registrar cualquier novedad en el registro de la red.
5. Monitorear los intentos de acceso no autorizado a la red y registrar cualquier actividad sospechosa en el registro de la red.
6. Evaluar la disponibilidad del sitio web de la institución y registrar cualquier problema o novedad relevante en el registro de la red.
7. Supervisar cualquier congestión del canal y registrar cualquier cambio significativo en el registro de la red.
8. Monitorear y verificar los controles de los puertos de la red y registrar cualquier actividad o novedad relevante.
9. Supervisar los servicios de comunicación unificada existentes y registrar cualquier cambio significativo en el registro de la red.
10. Analizar la bitácora y examinar la situación para identificar las causas que originaron las novedades.
11. ¿La novedad es un incidente?
12. Si la novedad es un incidente, verificar si la solución está registrada en la base de conocimiento y proceder a la actividad 15. Si no es un incidente, continuar con la actividad 18.
13. Si el incidente es interno, informar al jefe de tecnología sobre las novedades, analizar y determinar las acciones a tomar, y continuar con la actividad 15.
14. Si la novedad no es de origen interno, informar al jefe de tecnología sobre las novedades, analizar y definir las acciones en colaboración con el proveedor correspondiente, y continuar con la actividad 15.
15. Ejecutar las acciones definidas y evaluar si la novedad ha sido eliminada.

16. Si la novedad ha sido solucionada, notificar a los usuarios acerca de las soluciones tomadas (si corresponde), y registrar en la bitácora de administración de red las acciones realizadas.
17. Si la novedad no ha sido solucionada, analizar y determinar nuevas acciones para su eliminación, y regresar a la actividad 15.
18. Emitir una solicitud de cambio (RFC) para la configuración del firewall y justificar el cambio.
19. Evaluar el impacto del cambio solicitado y registrar en el RFC la viabilidad del cambio.
20. Si el cambio es viable, ejecutar la actividad del cambio, registrar en el RFC y notificar al solicitante acerca del cambio realizado. Posteriormente, firmar el RFC y enviarlo al solicitante.
21. Si el cambio no es viable, notificar al solicitante acerca del rechazo del cambio y documentar los motivos justificados en el RFC.

2.11.4. Diseño de métricas

Una vez que se hayan elegido e identificado los controles apropiados para cada activo crítico en el DDTI, en consonancia con las necesidades de seguridad de información de la institución, es importante establecer indicadores y métricas que permitan evaluar la eficacia de los controles seleccionados. Para tal fin, se ha elaborado la Tabla 23 que detalla tanto los controles como las métricas correspondientes.

Tabla 23

Controles y métricas

Dominio	Objetivo-control	Métricas
A.7 Seguridad relativa a los recursos humanos	**A.7.1 Antes del empleo** A.7.1.1 Investigaciones de antecedentes A.7.1.2 Términos y condiciones	Porcentaje de personal recién contratados que han pasado exitosamente todas las verificaciones (PRC) y cumplen con las políticas de la institución antes de comenzar a trabajar, fórmula %= $\frac{PRC}{PA*100}$

		donde PA es el total de personal recién contratado.
	A.7.2 Durante el empleo A.7.2.2 Concienciación, educación y formación en seguridad de la información	Evaluación (E) de la respuesta a las iniciativas de concientización en seguridad, medida por el número de correos electrónicos (#CE) y llamadas (#L) relacionadas con las campañas de concientización individuales, fórmula E= $\frac{\#CE}{\#L}$.
A.8 Gestión de activos	**A.8.1 Responsabilidad sobre los activos** A.8.1.1 Inventario de activos	Porcentaje de activos de información en cada etapa (#AIE) del proceso de clasificación (identificación, inventario, asignación de propietario, evaluación de riesgos, clasificación y aseguramiento), fórmula X= $\frac{\#AIE}{\#total\ activos*100}$. Porcentaje de activos de información críticos (#AIC) que cuentan con una estrategia global implementada para mitigar los riesgos de seguridad de la información, según sea necesario, y para mantener dichos riesgos en niveles aceptables, fórmula Y= $\frac{\#AIC}{\#total\ activos*100}$.
	A.8.2 Clasificación de la información A.8.2.1 Clasificación de la información	Porcentaje de activos de información en cada categoría de clasificación (#AICC), incluyendo aquellos que aún no han sido clasificados, fórmula A=$\frac{\#AICC}{total\ activos\ clasificados\ y\ no\ clasificados\ *100}$.
A.9 Control de acceso	**A.9.1 Requisitos comerciales de control de acceso** A.9.1.1 Política de control de acceso	El porcentaje de sistemas y aplicaciones empresariales en los que se han identificado adecuadamente los "propietarios" y han aceptado formalmente sus responsabilidades, así como llevado a cabo o encargado revisiones de accesos y seguridad de aplicaciones basadas en riesgos, y definido reglas de control de acceso basadas en roles.
	A.9.2 Gestión de acceso de usuario A.9.2.3 Gestión de privilegios de derechos de accesos	Se solicita la información relativa al tiempo medio entre la petición y la realización de cambios de acceso, así como el número de solicitudes de cambio de acceso presentadas durante el mes anterior. Se requiere un análisis de tendencias y comentarios adicionales sobre cualquier pico en el número de solicitudes
	A.11.1 Áreas seguras	

A.11 Seguridad física y del entorno	A.11.1.1 Perímetro de seguridad física A.11.1.4 Protección contra las amenazas externas y ambientales A.11.1.5 El trabajo en áreas seguras	Se solicita un informe periódico sobre las inspecciones de seguridad física realizadas en las instalaciones, que incluya una actualización regular sobre el estado de las medidas correctivas pendientes identificadas en inspecciones previas
	A.11.2 Seguridad de los equipos A.11.2.1 Emplazamiento y protección de equipos A.11.2.2 Instalaciones de suministro A.11.2.4 Mantenimiento de los equipos	Se requiere información sobre el número de controles realizados en el último mes, tanto para personas que salen de las instalaciones como para el stock de equipos o soportes informáticos. También se solicita el porcentaje de chequeos que revelaron movimientos no autorizados de equipos o soportes informáticos, así como otras cuestiones de seguridad. Se solicita un informe sobre las inspecciones periódicas realizadas a los equipos, incluyendo la revisión de su rendimiento, capacidad, eventos de seguridad y limpieza de los distintos componentes (como aplicaciones, almacenamiento, CPU, memoria y red).
A.12 Seguridad de las operaciones	**A.12.1 Procedimientos** operativos y responsabilidades A.12.1.1 Documentación de procedimientos operacionales A.12.1.2 Gestión de cambios A.12.1.2 Gestión de capacidades	Los indicadores de madurez de los procesos de Tecnologías de la Información relacionados con la seguridad incluyen el tiempo necesario para aplicar parches de seguridad a la mitad de los sistemas vulnerables, lo que evita la distorsión causada por la presencia de sistemas poco comunes que permanecen sin parchear por razones diversas como el hecho de que no se usan a diario o se encuentran normalmente fuera de la oficina.
	A.12.3 Copias de seguridad A.12.3.1 Copias de seguridad de la información	El porcentaje de éxito en las operaciones de copia de seguridad y en las pruebas de recuperación, fórmula $A=\frac{\#\ operaciones\ exitosas}{\#total\ de\ operaciones}*100$. También se puede medir el tiempo promedio que transcurre desde la recopilación de los medios de copia de seguridad de almacenamiento fuera de las instalaciones hasta la recuperación exitosa de los datos en todas las ubicaciones principales. Es importante medir el porcentaje de copias de seguridad y archivos que contienen datos sensibles o valiosos y que están cifrados para evaluar el nivel de seguridad en el manejo de dichos datos, fórmula

		$B = \frac{\#\ copias\ de\ datos\ sensibles}{\#total\ de\ copias\ *100}$.
	A.12.4 Registro de la actividad y supervisión A.12.4.1 Registro de eventos A.12.4.2 Protección de la información del registro A.12.4.3 Registro de administración y operación	El porcentaje de sistemas que tienen sus registros de seguridad correctamente configurados, transferidos de manera segura a un sistema de gestión centralizada de registros y monitoreados de manera regular y evaluados de manera efectiva, fórmula C= $\frac{\#\ sistemas\ seguros}{\#total\ de\ sistemas\ *100}$. La dirección del número de entradas registradas en los registros de seguridad que han sido analizadas y han llevado a actividades de seguimiento (D), fórmula D= $\frac{NRA*AR}{AS}$, donde NRA es número de entradas registradas, AR es proporción de entradas analizadas y AS es proporción de entradas que han llevado a actividades de seguimiento. .
	A.12.6 Gestión de la vulnerabilidad técnica A.12.6.1 Gestión de vulnerabilidades técnicas A.12.6.2 Restricciones en la instalación de software	Se solicita un informe periódico acerca de las vulnerabilidades técnicas y elaborar reglas que rijan la instalación de software por parte de los usuarios.
A.13 Seguridad de las comunicaciones	**A.13.1 Gestión de la seguridad en las redes** A.13.1.1 Controles de red A.13.1.2 Seguridad de los servicios de red	Las estadísticas de los cortafuegos incluyen la proporción de paquetes o sesiones salientes que han sido bloqueadas, como los intentos de acceso a sitios web prohibidos, así como el número de posibles ataques de piratería que han sido repelidos y se clasifican según su nivel de gravedad: insignificante, preocupante o crítico. El número de incidentes de seguridad de red que se han identificado en el mes anterior se divide por categorías según su nivel de gravedad, que puede ser leve, importante o grave. Se realiza un análisis de tendencias y se proporciona una descripción detallada de cada incidente serio y de cualquier tendencia adversa que se detecte.
	A.13.2 Intercambio de información con partes externas	El porcentaje de enlaces de terceros para los cuales se han definido y aplicado satisfactoriamente los requisitos de

	A.13.2.1 Políticas y procedimientos de transferencia de información A.13.2.3 Mensajería electrónica A.13.2.4 Acuerdos de confidencialidad o no revelación	seguridad de la información se ha medido para asegurar que se han implementado medidas adecuadas para proteger la información.
A.14 Adquisición desarrollo y mantenimiento de los sistemas de información	**A.14.1 Requisitos de seguridad de los sistemas de información** A.14.1.1 Análisis de requisitos y especificaciones de seguridad de la información A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas A.14.1.3 Protección de las transacciones de servicios de aplicaciones	El porcentaje de sistemas y aplicaciones utilizados por empresas para los cuales se han identificado adecuadamente los propietarios, han aceptado formalmente sus responsabilidades, han realizado revisiones de acceso y seguridad basadas en riesgos y han definido reglas de control de acceso basadas en roles se ha determinado. Un "estado de seguridad" se ha generado para informar el nivel general de confianza de la dirección de la empresa, basado en análisis de pruebas de penetración recientes, incidentes actuales o recientes, vulnerabilidades conocidas actuales, cambios planificados, entre otros factores.
	A.14.2 Seguridad en los procesos de desarrollo A.14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo A.14.2.8 Pruebas funcionales de seguridad de sistemas A.14.2.9 Pruebas de aceptación de sistemas	Generar un informe sobre el "estado de seguridad en sistemas en desarrollo" para evaluar el estado actual de la seguridad en los procesos de desarrollo de software, proporcionando comentarios sobre incidentes recientes o actuales, vulnerabilidades de seguridad conocidas y un pronóstico de cualquier riesgo creciente
A.16 Gestión de incidentes de la seguridad de la información	**A.16.1 Gestión de incidentes de seguridad de la información y mejoras** A.16.1.7 Recopilación de evidencias	Respecto al monitoreo de la seguridad de la información, se debe considerar la cantidad y la gravedad de los incidentes, así como el costo de analizar, detener y reparar los mismos y cualquier pérdida tangible o intangible que se haya producido como consecuencia de ellos. Es importante determinar el porcentaje de incidentes de seguridad que han ocasionado costos por encima de los umbrales aceptables definidos por la dirección, con el fin de evaluar el impacto económico y tomar medidas para prevenir futuros incidentes. Para realizar un análisis completo de la seguridad de la

		información, se recomienda examinar las estadísticas de helpdesk de TI, prestando especial atención al número y tipos de llamadas relacionadas con la seguridad de la información, incluyendo cambios de contraseña y preguntas sobre riesgos y controles de seguridad. A partir de estas estadísticas, se puede crear y publicar una tabla de clasificación de los departamentos, ajustada según el número de empleados, para determinar qué áreas están más concienciadas con la seguridad de la información y cuáles necesitan mejorar en este aspecto.
A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	**A.17.1 Continuidad de la seguridad de la información** A.17.1.1 Planificación de la continuidad de la seguridad de la información	Informes de las necesidades de seguridad de la información para gestionar la seguridad de la información en situaciones adversas.
A.18 Cumplimiento	**A.18.1 Cumplimiento de requisitos legales y contractuales** A.18.1.4 Protección y privacidad de la información de carácter personal	Cantidad de personal administrativo que poseen un conocimiento adecuado en cuanto al manejo de datos personales con la siguiente fórmula X= $\frac{PCA}{PA}$; en donde PCA es personal con conocimiento adecuado y PA es el total del personal. Cantidad de personal administrativo que han sido asignados a un nivel de acceso apropiado para la información, fórmula $Y = \frac{PAA}{PA}$; en donde PAA es personal de acceso apropiado y PA es el total del personal.
	A.18.2 Revisaciones de Seguridad de la información A.18.2.3 Comprobación del cumplimiento técnico	Número de cuestiones o recomendaciones relacionadas con la política interna y el cumplimiento normativo, que se han evaluado y clasificado según su estado (cerrado, abierto, nuevo, retrasado) y su nivel de riesgo (alto, medio, bajo). Porcentaje de revisiones de seguridad de la información que no han presentado incumplimientos significativos. Cantidad de cuestiones o recomendaciones de auditoría, clasificadas y evaluadas según su estado (cerrado, abierto, nuevo, retrasado) y su nivel de riesgo (alto, medio, bajo). Proporción de hallazgos de auditoría sobre seguridad de la información que han sido resueltos y cerrados, en relación con

	el total de hallazgos abiertos en el mismo periodo. Tiempo medio real de solución y cierre de recomendaciones, en comparación con los plazos reducidos por la dirección al final de las auditorías.

Nota: Elaboración propia

2.12. Capacitaciones y Sociabilización

Se aconseja realizar una capacitación de forma inmediata, lo que motivó la entrega de los recursos y directrices adecuados para que la empresa pueda difundir y promoverlos entre su personal en el futuro.

2.12.1. Objetivo

El propósito de esta medida es concientizar a todo el personal del DDTI acerca de la importancia que tiene la seguridad de la información que se maneja dentro de la institución. Para lograr este objetivo, se implementarán capacitaciones relevantes que se aplicarán en el desempeño diario de las actividades de los empleados.

2.12.2. Responsables

Existen varios actores que tienen responsabilidades específicas para garantizar que las capacitaciones y socializaciones sobre seguridad de la información se lleven a cabo efectivamente dentro de la institución:

- **Autoridades:** Es crucial que las autoridades de la institución estén familiarizadas con las leyes y las políticas de seguridad que sustentan el programa de seguridad, además de comprender su rol de liderazgo y la importancia de ser un ejemplo a seguir para el resto de los empleados.
- **Personal de seguridad**: Estos expertos en seguridad son responsables de estar debidamente capacitados en políticas de seguridad y buenas prácticas, con el objetivo de poder brindar asesoramiento y guía apropiada al resto del personal de la institución.

- **Propietarios de los sistemas (DDTI):** Es esencial que los propietarios de los sistemas estén al tanto de las políticas de seguridad y comprendan cómo se relacionan con los controles de seguridad que se aplican en los sistemas que manejan.
- **Administradores de sistemas y personal de soporte:** Estos empleados tienen la responsabilidad de estar altamente capacitados a nivel técnico en cuestiones de seguridad, a fin de poder brindar soporte adecuado para las operaciones críticas de la institución.
- **Usuarios finales:** Es importante que los usuarios finales estén altamente conscientes de la seguridad y conozcan las reglas de comportamiento adecuado con los sistemas a los que tienen acceso.

2.12.3. Necesidades de Capacitación

Es imprescindible proporcionar capacitación para:

- Promover la conciencia acerca de la seguridad de la información
- Fomentar la comprensión de las prácticas de seguridad adecuadas por parte del personal.
- Es necesario capacitar al personal que requiera habilidades específicas para cumplir con los requisitos de su trabajo.
- La capacitación puede ser organizada por el departamento de TIC para cumplir con los objetivos y las metas establecidas en la institución.
- Es común que los empleados tengan poca o ninguna información acerca de las políticas y los procedimientos de seguridad. Por lo tanto, es importante brindar capacitación para cubrir esas brechas.
- Es importante tener en cuenta las sugerencias del personal para identificar áreas en las que puedan necesitar capacitación adicional.

- La verificación de los comportamientos generales del personal, como la utilización de secciones abiertas y contraseñas visibles, puede ser un indicador de la necesidad de capacitación en seguridad de la información.
- Cualquier solicitud de capacitación para el personal debe ser presentada por escrito para asegurar una comunicación clara y efectiva entre los distintos departamentos y miembros de la institución.

2.12.4. Temas para tratar en cada sesión

- **Primera sesión:**

  Durante la primera sesión, se introducirán los conceptos fundamentales relacionados con la seguridad de la información. En la Tabla 24 se presentan de manera detallada los conceptos generales que se abordarán.

Tabla 24

Conceptos Generales

Conceptos Generales	
Seguridad Informática	Riesgo
Seguridad de la información	SGSI
Activo	Confidencialidad
Amenaza	Integridad
Vulnerabilidad	Disponibilidad

Nota: Elaboración propia

- **Segunda sesión:**

  Una vez que el personal haya adquirido conocimientos sobre los conceptos básicos, se procederá a explicar los diferentes métodos que los atacantes pueden emplear para obtener información. La Tabla 25 detalla los métodos que se discutirán durante esta sesión.

Tabla 25

Métodos de Obtención de Información

Métodos para obtener información	
Ingeniería Social	Phising
Spam	Malware
Dumpster diving	Shoulder surfing

Nota: Elaboración propia

- **Tercera sesión:**

  La tercera sesión tiene una gran relevancia, ya que se expondrán las leyes que tienen un impacto directo en la seguridad de la información. La Tabla 26 presenta las leyes que se abordarán en esta sesión.

Tabla 26

Leyes aplicables a la Seguridad de la Información

Leyes	
Les Orgánica de Protección de Datos de Carácter Personal	Ley de propiedad intelectual
Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos.	Ley de telecomunicaciones

Nota: Elaboración propia

- **Cuarta sesión:**

  En la cuarta sesión, se enfatizará en la importancia de aplicar buenas prácticas de seguridad de la información en el desempeño diario de los trabajadores de la institución. En la Tabla 27 se detallan las buenas prácticas que se discutirán durante esta sesión.

Tabla 27

Buenas Prácticas de la Seguridad de la Información

Buenas Prácticas	
Uso de correo electrónico e identificación de correos sospechosos	Gestión de contraseñas seguras
Uso apropiado de Internet	Seguridad en el puesto de trabajo
Escritorio Limpio	Uso apropiado de la Intranet

Uso de dispositivos de entidad fuera de las Instalaciones	Uso apropiado de credencial institucional

Nota: Elaboración propia

- **Quinta sesión:**

  En la quinta sesión, se abordarán los incidentes de seguridad que han ocurrido en el DDTI para que el personal esté informado y preparado para enfrentarlos en caso de que se presenten. La Tabla 28 presenta los temas relacionados con los incidentes que se tratarán en esta sesión.

Tabla 28

Tratamiento de incidentes

Incidentes	
Definición	Formas de reportar un incidente
Tipos	¿A quién debe reportar?
¿Qué puedo reportar?	Tiempo de respuesta

Nota: Elaboración propia

2.12.5. Tiempos estimados para cada sesión

Según lo señalado en la Tabla 29, se ha establecido el tiempo previsto para la realización de cada una de las secciones previamente mencionadas:

Tabla 29

Tiempos estimados por sesión

Sesión	Tiempo
Conceptos Generales	1hora
Métodos para obtener información	1hora
Leyes	1hora
Buenas Prácticas	1hora
Incidentes	1hora

Nota: Elaboración propia

2.12.6. Material

Se elaborarán presentaciones interactivas e infografías para cada una de las sesiones programadas previamente, las cuales contendrán información relevante sobre los temas expuestos. El Anexo 9 proporcionará detalles sobre este material. Este se enviará al personal mediante el correo institucional en forma de boletín. Asimismo, se identificarán lugares estratégicos donde se colocarán pósteres con mensajes y listas de verificación sobre lo que se debe y no se debe hacer.

2.12.7. Evaluación de actividades de sensibilización

La institución debe realizar evaluaciones o cuestionarios a través de plataformas digitales para verificar que las actividades de sensibilización se hayan llevado a cabo de manera efectiva y satisfactoria. Esto asegurará que no se excluya a personas que no hayan asistido a la evaluación. El Anexo 10 servirá como guía y proporcionará un formato que la institución podría utilizar.

2.12.8. Retroalimentaciones

Es importante que el personal reciba retroalimentación periódica sobre temas de seguridad de la información para crear conciencia y cultura en el DDTI en relación con la seguridad de la información manejada. Se sugiere realizar estas retroalimentaciones cada cuatro meses de forma regular.

2.13. Mejora Continua

Después de implementar el SGSI y analizar los resultados de los controles y métricas, es necesario fortalecer aquellos controles y políticas que son insuficientes para solucionar los incidentes presentados y reducir aún más el riesgo para los activos de información.

Es importante destacar que esta sección debe incluir acciones de mantenimiento y mejora del SGSI para garantizar que los procesos cumplan con las políticas y controles de seguridad, lo que permitirá brindar un servicio de calidad con un alto nivel de seguridad y reducir considerablemente la posibilidad de materialización del riesgo.

En la sección de mejora continua, la institución deberá abordar los siguientes elementos:

- Identificar y documentar las no conformidades en relación con las políticas de seguridad del Sistema de Gestión de Seguridad de la Información (SGSI).
- Definir y ejecutar las medidas correctivas necesarias para abordar las no conformidades identificadas.
- Evaluar la efectividad de las acciones correctivas implementadas.
- Recibir y tomar en cuenta la retroalimentación proporcionada por el personal de la institución en relación con el manejo de la seguridad de la información.
- Asignar los recursos necesarios para mejorar el SGSI en la institución.
- Monitorear y documentar todas las sugerencias de mejora en relación con el SGSI implementado.

2.13.1. Plan de Implementación

El proceso de implementación del SGSI en el DDTI implica una serie de pasos específicos.

Aplicar los controles establecidos en el Anexo A de la norma ISO 27001, de acuerdo con las políticas de seguridad que se hayan propuesto en el diseño.

Es fundamental aplicar las políticas y procedimientos dentro del alcance del SGSI en la propuesta de diseño del SGSI en el DDTI, ya sea de manera global o específica. Para evitar interrupciones en los procesos de la institución y garantizar un servicio adecuado a los pacientes, es necesario verificar que la política establecida en el diseño no interfiera con los procesos de la institución. Para ello, se recomienda utilizar una lista de chequeo antes de la implementación, así como apoyarse en el análisis de amenazas y vulnerabilidades, la valoración del riesgo, y las políticas y controles propuestos. Es importante comunicar adecuadamente las políticas, controles y procedimientos, impulsar su revisión y aplicación, y verificar su cumplimiento.

En este proceso de implementación se deben tener en cuenta aspectos como:

- El alcance del SGSI para el DDTI.
- Los resultados de la evaluación de riesgos.
- La política del SGSI.
- El plan de tratamiento de riesgos según los controles asignados.
- La participación del personal en el proceso a través de capacitaciones.
- La asignación de responsabilidades y la verificación del cumplimiento por parte del personal involucrado en el proceso.

Implementación de controles

Luego de identificar los activos de información, se procedió a determinar las amenazas que pueden afectarlos, para posteriormente realizar una valoración del riesgo. Como resultado, se han propuesto controles en el diseño del SGSI para el DDTI.

Para la implementación de esta propuesta, se recomienda una documentación detallada de cada uno de los controles, a fin de determinar los recursos necesarios para su desarrollo completo y óptimo, como, por ejemplo, los recursos económicos y técnicos, y planes de capacitación.

Además, es esencial garantizar la armonía y la cooperación entre las partes involucradas para enfrentar posibles incidentes relacionados con los activos de información. Con este fin, se sugiere la creación del área de Seguridad de la Información y del comité de Seguridad de la Información. Por último, es importante asignar responsabilidades y establecer cronogramas con fechas y procesos para la implementación de los controles propuestos en este diseño.

Implementación de un programa de gestión de incidentes

Es esencial que el área encargada de la seguridad de la información de la institución mantenga un registro detallado de todos los incidentes de seguridad que se produzcan. Esto

permitirá tomar medidas para mitigar y reducir la probabilidad de futuros incidentes. Asimismo, se recomienda que se realice un seguimiento constante tanto de los incidentes de seguridad como de las políticas establecidas. Es importante contar con un manual que establezca claramente las acciones a seguir en caso de incidente, lo cual incluye:

- Definir los procedimientos para reportar el incidente.
- Identificar a quién se debe reportar el incidente.
- Establecer las formas de escalonamiento.
- Contar con un plan de contingencia.
- Establecer acciones reparatorias.
- Priorizar los incidentes y las áreas afectadas.
- Recopilar evidencia de los incidentes.
- Comunicar los incidentes a los usuarios afectados en el menor tiempo posible.
- Presentar informes mensuales o trimestrales a la gerencia.
- Realizar un seguimiento estadístico de los incidentes.
- Llevar a cabo auditorías internas del Sistema de Gestión de Seguridad de la Información para verificar el cumplimiento de las políticas de seguridad y la efectividad de las medidas adoptadas para mitigar el riesgo.

Gestión de recursos para el SGSI

La administración de recursos para el Sistema de Gestión de Seguridad de la Información (SGSI) requiere la asignación adecuada de recursos económicos, tecnológicos y humanos. Para optimizar estos recursos, se debe realizar un análisis exhaustivo para determinar las prioridades de seguridad de la información en el DDTI y cómo se beneficiaría trabajando en ellas. Después de establecer las prioridades, se debe elaborar un plan de asignación de recursos que cumpla con las políticas de seguridad y garantice la aplicación prioritaria de los controles sugeridos para

cada activo de información. Cabe señalar que la gerencia debe autorizar la priorización de gastos en base a un informe elaborado por el departamento de TICs en función de esta propuesta.

Recepción, análisis y aprobación del diseño del SGSI por parte del DDTI

El Departamento de Desarrollo Tecnológico e Informático (DDTI) ha recibido la documentación generada por el diseño del SGSI. La institución verificó que el diseño cumple con los lineamientos planteados y no viola el acuerdo de confidencialidad establecido entre las partes. Finalmente, la institución aceptó formalmente el contenido y formato del trabajo. El certificado de recepción proporcionado por el DDTI se puede encontrar en el Anexo 13.

CAPÍTULO 3

Resultados

3.1. Evaluación del Diseño de Sistema de Gestión de Seguridad de la Información mediante el método Delphi

Después de finalizar la creación del Diseño del Sistema de Gestión de la Seguridad de la Información, resulta crucial verificar la efectividad del proceso de desarrollo. Con el propósito de validar este aspecto, se decidió llevar a cabo una Evaluación utilizando el método Delphi.

El Método Delphi es una técnica estructurada de comunicación y retroalimentación utilizada para explorar y alcanzar un consenso sobre un acontecimiento del futuro, por medio de sucesivas preguntas anónimas enfocadas un grupo de expertos, sin la necesidad de reunirse físicamente en una misma locación, lo que permite a los participantes reevaluar y modificar sus respuestas iniciales en función de la opinión del grupo. Por lo tanto, según (Astigarraga, 2018) “la capacidad de predicción de la Delphi se basa en la utilización sistemática de un juicio intuitivo emitido por un grupo de expertos”.

Figura 39

Elementos Método Delphi

Nota: Pasos a seguir del método Delphi, basado en Cicero Comunicaciones y FLAPP, 2022.

3.1.1. Identificación del Problema de Investigación

El primer paso en el método Delphi es identificar el problema u objetivo de investigación, que en este caso es evaluar la eficacia del Sistema de Gestión de Seguridad de la Información en el Departamento de Desarrollo Técnico e Informático de la Universidad Técnica del Norte, informe elaborado con la asistencia de MAGERIT versión 3 y en base a las consideraciones ISO 27001:2013 para el análisis y gestión de riesgos tecnológicos dentro de este departamento.

3.1.2. Elección panel de expertos

El panel de expertos es un componente fundamental del Método Delphi, y se refiere a un grupo de individuos que poseen conocimientos y experiencia en un tema específico y que son convocados para participar en el proceso de evaluación y consenso. Según (López, 2018), "conformar el panel de expertos implica llevar a cabo un proceso nominativo a partir de una propuesta formal a expertos reconocidos y relevantes en el tema de investigación".

A su vez, para definir el tamaño y la composición del panel de expertos se debe considerar la naturaleza de la investigación, posible alcance de objetivos y los recursos disponibles relacionados al investigador, sin embargo, para (Lopez, 2016) “El método Delphi no exige una muestra de expertos representativa de una población determinada, es decir, no hay normas específicas respecto al número de participantes”

En primer lugar, se contactó a una cantidad determinada de expertos de diversas organizaciones a través de correo electrónico. No obstante, únicamente se recibió respuesta de un número específico de ellos, el cual asciende a 4. La información pertinente de los expertos que participaron se encuentra disponible en la Tabla 30.

Tabla 30

Selección de expertos para la validación mediante el Método Delphi

N	Institución	Categoría de la Institución	Grado académico
E1	Universidad Técnica del Norte	Institución Pública de Educación Superior	Magister en Evaluación y Auditoria de Sistemas Tecnológicos
E2	Universidad Técnica del Norte	Institución Pública de Educación Superior	Magister en Evaluación y Auditoria de Sistemas Tecnológicos
E3	Universidad de las Fuerzas Armadas ESPE	Institución Pública de Educación Superior	Magister en Evaluación y Auditoria de Sistemas Tecnológicos
E4	Universidad Técnica del Norte	Institución Pública de Educación Superior	Magister en Evaluación y Auditoria de Sistemas Tecnológicos

Nota: La tabla indica una reseña de los expertos seleccionados. Elaboración propia

3.1.3. Elaboración y distribución del cuestionario inicial

Determinado el objetivo de la investigación , se creó una lista de verificación de 15 elementos que estarán enfocados en el objetivo de la investigación teniendo en cuenta los puntos más significativos del Sistema de Gestión de Seguridad de la Información ubicado en Anexo 11. Todo el proceso de recolección de datos se desarrolló de forma electrónica, la invitación para participar fue emitida por correo electrónico, se acordó que el tiempo esperado entre el envío de información y la recepción de respuestas sería de una semana; la información enviada incluyó el informe del Sistema de Gestión de Seguridad de la Información y un enlace para acceder al cuestionario en Google Forms.

Con excepción del ítem 15 (argumento personal), para la evaluación del resto de ítems se propuso la escala Likert de 5 puntos , como se muestra en la Tabla 31.

Tabla 31

Escala de Likert para la valoración de cuestionarios

Valor	Escala de Likert
1	Totalmente de acuerdo
2	De acuerdo
3	Indiferente o neutro
4	En desacuerdo
5	Totalmente en desacuerdo

Nota: Elaboración propia

3.1.4. Análisis de la información

El análisis de la información se desarrolló utilizando estrategias descriptivas, cuantitativas y cualitativas para evaluar los resultados obtenidos de los cuestionarios.

Para determinar el índice de validez de contenido reflejada por cada ítem, se aplica la siguiente fórmula:

$$CVI = \frac{\text{número de respuestas positivas}}{\text{número total de respuestas}}$$

$$CVITotal = \frac{\text{número de respuestas positivas}}{(\text{número de expertos x número de ítems})}$$

Existen tres maneras de calcular el CVITotal, para el caso de estudió se aplicará la primera forma detallada anteriormente, sin embargo, las tres formas de cálculo existente den dar el mismo valor como resultado. Por otro lado, para que un instrumento refleje el valor esperado su CVI general debe ser superior al 90%, y cada elemento debe tener un CVI superior al 75% (Silva & Montilha, 2021) .

Si se cumplen los valores, se considera que se ha llegado a un consenso. Si no se cumplen , es posible solicitar comentarios o sugerencias de mejora para modificarlos y / o eliminarlos .

Asimismo, se eligió emplear técnicas auxiliares como:

La estadística descriptiva: es una técnica que brinda diversos modos de mostrar y evaluar la información destacada de los datos encontrados mediante gráficos, tablas o medidas

resúmenes, ofreciendo un análisis exploratorio de datos como un todo y establecer cuáles son las características para considerar como sobresalientes de acuerdo con la variable que sea de interés ya sea categórica o numérica (Orellana, 2018). En vista de que se emplearon variables cuantitativas, específicamente la escala de Likert se consideró conveniente utilizar diferentes medidas de tendencia central para obtener información relevante acerca de los resultados obtenidos. Entre las medidas utilizadas se encuentran la media aritmética, la mediana, la desviación típica, así como el porcentaje de acuerdo y desacuerdo en cada uno de los ítems presentes en el cuestionario.

El alfa de Cronbach: es la metodología más utilizada por los investigadores para determinar la fiabilidad de pruebas, test, cuestionarios o escalas puesto a que requiere únicamente una administración de la prueba, además posee una facilidad de cálculo, son utilizados por casi todos los programas estadísticos y en relación con varios índices refleja un análisis de confiabilidad (Muñoz, 2019).

Para la interpretación del coeficiente se considera el valor esperado máximo de 0.90, sobre este valor se estima que la información pose duplicación o incluso redundancia, por lo tanto, existirán ítems que deberán ser eliminados, a su vez, el valor aceptable mínimo de 0.70, las cifras debajo del marcador serán de consistencia interna baja, por lo tanto, es de preferencia tener valores entre 0.80 y 0.90. (Orellana, 2018)

A continuación, en la Tabla 32 se indican los resultados obtenidos por parte de los expertos.

Tabla 32

Resultados del primer cuestionario suministrado a expertos

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15
E1	1	2	2	3	2	1	2	2	1	2	3	2	1	1	No
E2	2	2	2	1	3	1	3	2	1	3	1	1	1	2	No modificaría el plan de acción, pero sería conveniente que se realice un monitoreo continuo para que no solo quede en papel la información.
E3	1	1	2	1	2	1	2	1	1	1	2	1	1	1	No
E4	1	2	1	1	1	2	1	1	1	1	1	2	1	1	No

Nota: La tabla indica los datos obtenidos, donde E son los expertos y P las interrogaciones. Elaboración propia

Para calcular los índices de validez del contenido, se requiere una tabla de respuestas por pregunta y valor en la escala Likert. Esta matriz se puede encontrar en la Tabla 33 y gráficamente en la Figura 40.

Tabla 33

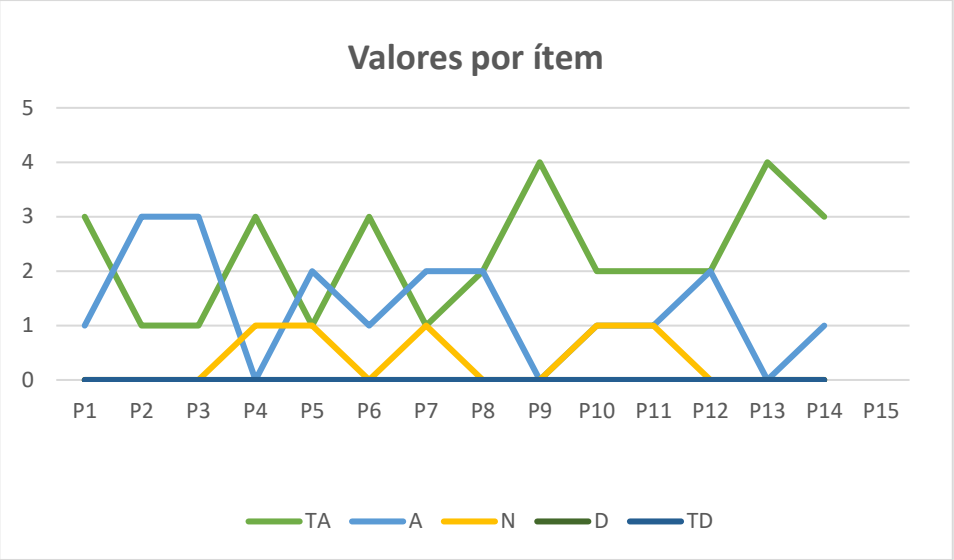
Tabulación de respuestas del primer cuestionario realizado a expertos por pregunta y valor mediante la escala de Likert

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15
TA	3	1	1	3	1	3	1	2	4	2	2	2	4	3	-
A	1	3	3	0	2	1	2	2	0	1	1	2	0	1	-
N	0	0	0	1	1	0	1	0	0	1	1	0	0	0	
D	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
TD	0	0	0	0	0	0	0	0	0	0	0	0	0	0	

Nota: P: interrogantes del cuestionario, TD: Totalmente desacuerdo, D: Desacuerdo, N: Indiferente, A: De acuerdo, TA: Totalmente de acuerdo. Elaboración propia

Figura 40

Respuestas por ítem del primer cuestionario a expertos



Nota: P: interrogantes del cuestionario, TD: Totalmente desacuerdo, D: Desacuerdo, N: Indiferente, A: De acuerdo, TA: Totalmente de acuerdo. Elaboración propia

Siguiente a que las respuestas han sido tabuladas, los cálculos del índice de Validez de Contenido se pueden realizar utilizando las fórmulas mencionadas anteriormente. La información está disponible en la Tabla 34.

Tabla 34

Índice de Validez de Contenido (CVI) del primer cuestionario a expertos

Pregunta	TD	D	N	A	TA	IVC ÍTEM
1.-¿Cree usted que es indispensable que se implemente un Diseño de Sistema de Gestión de Seguridad de la Información para el DDTI-UTN?	-	-	-	25%	75%	100%
2.-¿Estaría de acuerdo en que el informe sobre el Diseño del Sistema de Gestión de la Seguridad de la Información para el DDTI-UTN se escribió de manera clara y comprensible?	-	-	-	75%	25%	100%
3.-¿Está de acuerdo en que el Diseño de un Sistema de Gestión de la Seguridad de la Información para el DDTI-UTN cuenta con los datos esenciales?	-	-	-	75%	25%	100%
4.-¿Considera que se da cumplimiento a los objetivos principales del Diseño del Sistema de Gestión de la Seguridad de la Información para el DDTI-UTN?	-	-	25%	-	75%	75%
5.-¿Considera que los procedimientos implementados durante la creación de un Sistema	-	-	25%	50%	25%	75%

de Gestión de la Seguridad de la Información para el DDTI-UTN fueron adecuados y suficientes?						
6.-¿Considera esencial que se realice evaluaciones sobre las capacitaciones del Sistema de Gestión de la Seguridad de la Información para el DDTI-UTN?	-	-	-	25%	75%	100%
7.-¿En su opinión, las tareas propuestas a manera de controles para la mitigación de riesgos en el Diseño de un Sistema de Gestión de la Seguridad de la Información para el DDTI-UTN fueron las idóneas?	-	-	25%	50%	25%	75%
8.-¿Considera que las tareas asignadas como controles para reducir riesgos en la implementación de un Sistema de Gestión de la Seguridad de la Información en el DDTI-UTN fueron apropiadas según su criterio?	-	-	-	50%	50%	100%
9.-¿Cree usted que el Sistema de Gestión de la Seguridad de la Información creado específicamente para el DDTI-UTN podría ser utilizado con éxito en otras instituciones de educación superior?	-	-	-	-	100%	100%
10.-¿Cree usted que las políticas de seguridad implementadas para la creación de un Sistema de Gestión de Seguridad de la Información del DDTI-UTN fueron idóneas?	-	-	25%	25%	50%	75%
11.-¿Considera que mediante el plan de tratamiento de riesgos implementado se garantiza la confidencialidad, integridad y disponibilidad de la información en el Sistema de Gestión de la Seguridad de la Información del DDTI-UTN?	-	-	25%	25%	50%	75%
12.-¿Cree usted que mediante las acciones de los directivos y los controles establecidos se puede garantizar el cumplimiento de las normas y regulaciones de un Sistema de Gestión de Seguridad de la Información del DDTI-UTN?	-	-	-	50%	50%	100%
13.-¿ Considera usted que se puede garantizar que un Sistema de Gestión de Seguridad de la Información del DDTI-UTN sea escalable y adaptable a los cambios en el entorno tecnológico y empresarial mediante la evaluación continua, una adecuada capacitación y la integración de estándares?	-	-	-	-	100%	100%
14.-¿En su opinión, está de acuerdo que mediante el Diseño de un Sistema de Gestión de Seguridad de la Información del DDTI-UTN se puede minimizar los impactos que podrían resultar si se produce una violación de seguridad ?	-	-	-	25%	75%	100%
15.-¿Modificaría algún componente del plan de acción diseñado para el Sistema de Gestión de la Seguridad de la Información del DDTI-UTN? En	-	-	-	-	-	-

caso afirmativo, ¿cuál sería el elemento que se propondría cambiar?	
IVC TOTAL	91.07%

Nota: IVC: Índice de validez de contenido, TD: Totalmente desacuerdo, D: Desacuerdo, N: Indiferente, A: De acuerdo, TA: Totalmente de acuerdo. Elaboración propia.

Se obtuvo un índice de Validez de Contenido (IVC) total de 91.07% en la primera ronda de cuestionarios, lo que, según la literatura, es un buen puntaje para permitir que el cuestionario sea válido. Cada pregunta tiene un IVC de ítem superior o igual al 75%, por lo que se considera que existe un consenso en los resultados y no es necesario cambiar o eliminar ítems.

Para verificar la validez del cuestionario, se aplicó la técnica de estadística alfa de Cronbach a todo el cuestionario; la fórmula alfa de Cronbach es la siguiente:

$$\alpha = \frac{k}{k-1} \times \left[1 - \frac{\sum v_i}{v_t}\right]$$

En donde,

$\alpha = Alfa\ de\ Cronbach$

$k = N\acute{u}mero\ de\ \acute{i}tems$

$Vi = Varianza\ de\ cada\ \acute{i}tem$

$Vt = Varianza\ total$

Los resultados obtenidos de la varianza se observan en la Tabla 35, mientras que valores del alfa de Cronbach en la Tabla 36.

Tabla 35

Varianza de ítems del primer cuestionario suministrado a expertos

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	Sumatoria
E1	1	2	2	3	2	1	2	2	1	2	3	2	1	1	25
E2	2	2	2	1	3	1	3	2	1	3	1	1	1	2	25
E3	1	1	2	1	2	1	2	1	1	1	2	1	1	1	18
E4	1	2	1	1	1	2	1	1	1	1	1	2	1	1	17
Varianza	0.19	0.19	0.19	0.75	0.5	0.19	0.5	0.25	0	0.69	0.69	0.25	0	0.19	85

Nota: P: interrogantes del cuestionario, E: Número de expertos. Elaboración propia

Tabla 36

Alfa de Cronbach del primer cuestionario suministrado a expertos

K	14
Suma de Varianzas (Vi)	4.56
Varianza Total (Vt)	14.19
Cronbach	**0.731**

Nota: Elaboración propia

La puntuación del Alfa de Cronbach es de 0,731, lo que está en un rango aceptable para la validez interna del cuestionario puesto que la literatura nos dice que en una categoría de 0.72 a 0.99 su confiabilidad es excelente.

Sin embargo, el ítem 15 incluye una pregunta argumentativa sobre la opción de modificar o mejorar el Plan de Acción del Sistema de Gestión de la Seguridad de la Información. Estas recomendaciones se utilizarán para modificar el informe y las preguntas de la segunda ronda del método Delphi.

3.1.5. Elaboración y administración del segundo cuestionario

Primero es necesario considerar las respuestas obtenidas en el ítem número 15 del primer cuestionario en relación con la decisión de modificar el informe actual del Plan de Acción del Sistema de Gestión de la Seguridad de la Información.

La síntesis de las respuestas se muestra en la Tabla 37.

Tabla 37

Síntesis de respuestas del ítem 15 del primer cuestionario suministrado a expertos

P15.-¿Modificaría algún componente del plan de acción diseñado para el Sistema de Gestión de la Seguridad de la Información del DDTI-UTN? En caso afirmativo, ¿cuál sería el elemento que se propondría cambiar?	
Expertos	**Respuesta**
E1	No
E2	No modificaría el plan de acción, pero sería conveniente que se realice un monitoreo continuo para que no solo quede en papel la información.
E3	No
E4	No

Nota: E: Número de Experto.
Elaboración propia

Solamente el experto 2 brinda retroalimentación que podría ayudar a aumentar la efectividad del Sistema de Gestión de la Seguridad de la Información.

Para aplicar adecuadamente a este comentario, se desarrolla la siguiente acción:

1. **Monitoreo Continuo**

   Las políticas de monitoreo continuo están expuestas en el Plan de Sistema Gestión de la Seguridad de la Información, estás fueron generadas a partir del dominio 17 del anexo A de la norma ISO/IEC 27001:2013, esta vez se incluyó una mejor explicación de este enunciado, tomando en cuenta objetivos y alcance del monitoreo, establecimiento de métricas así como umbrales de referencia, selección de herramientas de monitoreo, configuración de alertas y notificaciones además de la realización de un análisis y seguimiento.

Se elaboró el segundo cuestionario para el método de validación Delphi una vez establecida la adecuación en el Informe. Las preguntas tendrán el mismo estilo y constará de 5 elementos que están directamente relacionados con los cambios como respuesta del primer cuestionario, mismo se encuentran en el Anexo 12.

3.1.6. Observación final de la información

Luego de haber obtenido las respuestas de los expertos podemos evidenciar los resultados obtenidos mismos que se muestran en la Tabla 38.

Tabla 38

Resultados del segundo cuestionario suministrado a expertos

	P1	P2	P3	P4	P5
E1	1	2	1	1	1
E2	2	2	2	1	2
E3	1	1	1	1	1
E4	1	2	1	1	1

Nota: La tabla indica los datos obtenidos, donde E son los expertos y P las interrogaciones. Elaboración propia

Para calcular los índices de validez del contenido, se requiere una tabla de respuestas por pregunta y valor en la escala Likert. Esta matriz se puede encontrar en la Tabla 39 y gráficamente en la Figura 41.

Tabla 39

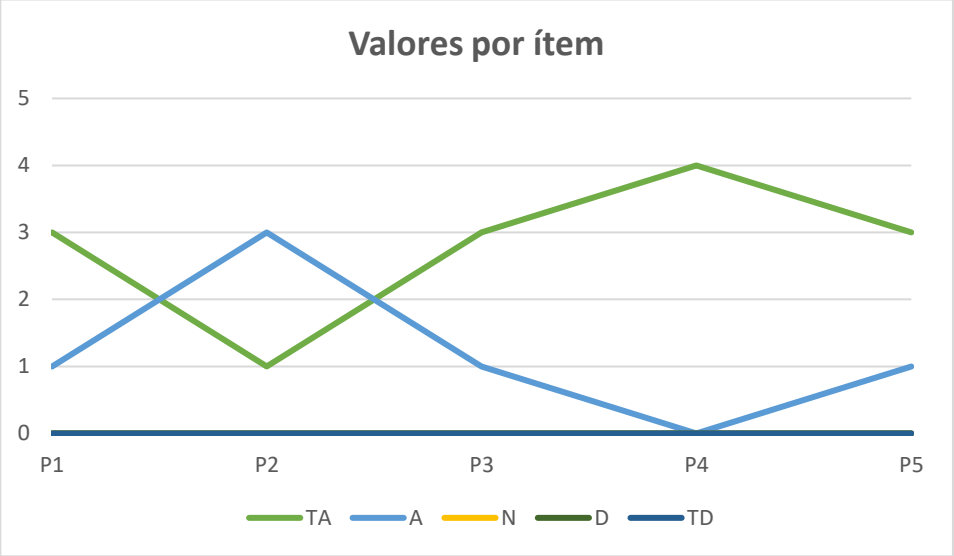
Tabulación de respuestas del primer cuestionario realizado a expertos por pregunta y valor mediante la escala de Likert

	P1	P2	P3	P4	P5
TA	3	1	3	4	3
A	1	3	1	0	1
N	0	0	0	0	0
D	0	0	0	0	0
TD	0	0	0	0	0

Nota: P: interrogantes del cuestionario, TD: Totalmente desacuerdo, D: Desacuerdo, N: Indiferente, A: De acuerdo, TA: Totalmente de acuerdo. Elaboración propia

Figura 41

Respuestas por ítem del cuestionario final a expertos



Nota: P: interrogantes del cuestionario, TD: Totalmente desacuerdo, D: Desacuerdo, N: Indiferente, A: De acuerdo, TA: Totalmente de acuerdo. Elaboración propia-.

Siguiente a que las respuestas han sido tabuladas, los cálculos del índice de Validez de Contenido se pueden realizar utilizando las fórmulas mencionadas anteriormente. La información está disponible en la Tabla 40.

Tabla 40

Índice de Validez de Contenido (CVI) del cuestionario final a expertos

Pregunta	TD	D	N	A	TA	IVC ÍTEM
1.-¿Considera que las políticas de Mejora Continua que se han establecido en el Diseño del Sistema de Gestión de la Seguridad de la Información están acordes con el DDTI-UTN?	-	-	-	25%	75%	100%
2.-¿Estaría de acuerdo en que el uso la norma ISO/IEC 27001:2013 fue acertada para el Diseño de un Sistema de Gestión de la Seguridad de la Información para el DDTI-UTN?	-	-	-	75%	25%	100%
3.-¿Está de acuerdo en que el Monitoreo Continuo es fundamental para mejorar el Sistema de Gestión	-	-	-	25%	75%	100%

de la Seguridad de la Información para el DDTI-UTN?						
4.-¿Considera usted que, en respuesta al enfoque de Mejora Continua, sea acertado plantear un seguimiento por lo menos una vez al año en el Departamento de Desarrollo Tecnológico e Informático de la UTN?	-	-	-	-	100%	100%
5.-¿Considera que los cambios en el Informe del Sistema de Gestión de la Seguridad de la Información desarrollados para el Departamento de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte fue adecuado y suficientes a fin de mejorar la calidad de este, tomando en cuenta las consideraciones extraídas del análisis del primer cuestionario?	-	-	-	25%	75%	100%
IVC TOTAL	100.00%					

Nota: IVC: Índice de validez de contenido, TD: Totalmente desacuerdo, D: Desacuerdo, N: Indiferente, A: De acuerdo, TA: Totalmente de acuerdo. Elaboración propia.

En la segunda ronda de cuestionarios, se obtuvo un 100% de IVC Total, indicando que todas las respuestas recogidas habían sido verificadas y se consideraron adecuadas para el cuestionario. Además, todas las preguntas han alcanzado un IVC de valor del 100%, indicando unanimidad sobre la relevancia de cada una de ellas. Esto conduce a la conclusión de que los resultados reflejan un consenso significativo y que no se requieren cambios o exclusión de temas del cuestionario.

Se decidió una vez más utilizar la técnica estadística Alfa de Cronbach en todas las preguntas para confirmar la validez del cuestionario.

La Tabla 41 contiene los valores de varianza, mientras que la Tabla 42 tiene los cálculos alfa de Cronbach.

Tabla 41

Varianza de ítems del cuestionario final suministrado a expertos

	P1	P2	P3	P4	P5	Sumatoria
E1	1	2	1	1	1	6
E2	2	2	2	1	2	9
E3	1	1	1	1	1	5
E4	1	2	1	1	1	6
Varianza	0.19	0.19	0.19	0.00	0.19	26

Nota: P: interrogantes del cuestionario, E: Número de expertos. Elaboración propia

Tabla 42

Alfa de Cronbach del segundo cuestionario suministrado a expertos

K	5
Suma de Varianzas (Vi)	0.75
Varianza Total (Vt)	2.25
Cronbach	**0.833**

Nota: Elaboración propia

El cálculo Alfa de Cronbach muestra una puntuación de 0.833, esto indica que está en un rango de excelente fiabilidad.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Tras una evaluación preliminar de la conformidad con los controles estipulados en el Anexo A de la norma ISO/IEC 27001, se ha determinado que el Departamento de Desarrollo Tecnológico e Informático en cuestión se encuentra en un nivel de madurez repetible. Esto se debe a que no existe una política o conjunto de políticas que aborden adecuadamente los asuntos de seguridad de la información en dicho departamento, y hay dominios donde los controles no están debidamente documentados ni conocidos por toda la institución. Como resultado, el departamento está expuesto a numerosas amenazas que podrían ser aprovechadas en cualquier momento.
- Luego de realizar un análisis exhaustivo, se puede afirmar que un riesgo se define como un evento incierto que, de suceder, tendría consecuencias negativas para la institución. La identificación del riesgo se basa en la probabilidad de que ocurra y en el impacto que tendría en caso de que se materializara. En consecuencia, el proceso de identificación de los riesgos incluye una serie de actividades, tales como el reconocimiento de los activos, amenazas, vulnerabilidades y controles implementados, cuyo objetivo es proteger los activos de información de la empresa. Es crucial gestionar adecuadamente los riesgos para aplicar medidas preventivas que aseguren la confidencialidad, integridad y disponibilidad de la información, lo que a su vez garantiza la continuidad del negocio.
- Con el avance constante de la tecnología, las organizaciones están cada vez más preocupadas por proteger su información de cualquier amenaza potencial. Por esta razón, es muy útil diseñar e implementar un sistema de gestión de seguridad de la información (SGSI), cuya principal función es administrar la seguridad de la

información en una institución al establecer políticas, métodos y técnicas para proteger la información. En resumen, la adopción de un SGSI conduce a una mejora continua al permitir un análisis constante de la situación actual y la detección oportuna de posibles incidentes de seguridad.

- Se determina que mantener un registro actualizado de los activos puede ayudar a clasificarlos según su nivel de riesgo, lo que resulta en una mejor protección para los mismos. Para valorar los activos se consideran los criterios de disponibilidad, integridad y confidencialidad asignándoles una importancia relativa. En el caso específico del DDTI de la UTN, se identificaron 15 activos críticos que se tuvieron en cuenta en la elaboración del SGSI.
- Magerit v3 es una metodología diseñada para gestionar los riesgos de seguridad de la información en las organizaciones, que se alinea con la norma ISO/IEC 27001 y el Sistema de Gestión de Seguridad de la Información (SGSI). Esta metodología propone diversas actividades para el análisis de riesgos, incluyendo la evaluación, tratamiento, aceptación, comunicación y revisión. En consecuencia, se recomienda establecer un plan de tratamiento de riesgos para mitigar las amenazas y reducir los riesgos a un nivel aceptable tanto para el Departamento de Desarrollo Tecnológico e Informático como para la institución en general.
- Se puede deducir que el propósito principal de contar con un conjunto de políticas de seguridad de la información es crear conciencia entre los empleados sobre los peligros de seguridad, al mismo tiempo que se les proporciona las herramientas necesarias para manejar adecuadamente la información.

Recomendaciones

- Las empresas utilizan una serie de directrices para evaluar el rendimiento, como el logro de objetivos organizacionales, la identificación rápida de problemas y la mejora constante, con la ayuda de la alta gerencia liderando los proyectos de

seguridad de la información y la cooperación de todas las áreas de la institución. Por lo tanto, se sugiere la implementación del sistema de gestión de seguridad de la información presentado en este proyecto en el DDTI de la UTN, además de un análisis de riesgos a todo el departamento.

- Se sugiere que, en el marco de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) propuesto en este proyecto, se establezca un comité de seguridad de la información. Este comité sería responsable de definir los roles y responsabilidades relacionados con la ejecución de las actividades necesarias para proteger la información. Se recomienda que el comité se reúna cada dos o tres meses, o en caso de que las circunstancias lo requieran, para coordinar todas las actividades relacionadas con la seguridad de la información.
- Se aconseja llevar a cabo regularmente programas de formación para el personal del DDTI y los proveedores con el fin de difundir los conocimientos sobre seguridad de la información. El objetivo de estas capacitaciones es fomentar una cultura de prevención y minimizar los posibles riesgos que puedan surgir.
- Se sugiere que se realice una mejora en las medidas de seguridad tanto físicas como electrónicas en el Departamento de Desarrollo Tecnológico e Informático. Además, se propone planificar y llevar a cabo tanto mantenimientos preventivos como correctivos de forma regular en todos los equipos pertenecientes a dicho departamento, con el fin de prevenir posibles fallos y asegurar la continuidad del negocio.
- Es crucial para asegurar la continuidad de una institución establecer un plan de respuesta a incidentes y reducir los riesgos asociados. Dado que el personal del DDTI puede provocar incidentes de seguridad, tanto intencional como involuntariamente, se aconseja que se establezcan procedimientos para determinar las responsabilidades y criterios de respuesta a los incidentes de

seguridad de la información. Estos procedimientos permitirán solucionar de forma rápida y efectiva cualquier eventualidad negativa que pueda surgir.

REFERENCIAS Y BIBLIOGRAFÍA

Bibliografía

Altamirano, D. L. M. (2019). Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. Avances, ISSN-e 1562-3297, Vol. 21, Nº. 2, 2019, págs. 248-263, 21(2), 248-263. https://dialnet.unirioja.es/servlet/articulo?codigo=6989568&info=resumen&idioma=ENG

CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, 449 Registro Oficial (2021). www.lexis.com.ec

Astigarraga, E. (2018). El método Delphi. San Sebastián: Universidad de Deusto. https://www.academia.edu/1778723/El_método_delphi

Borrero, P. (2019). IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN, RIESGOS Y CONTROLES ASOCIADOS PARA LA EMPRESA ESTRATEGIAS EMPRESARIALES DE COLOMBIA BAJO LA NORMA ISO 27001 E ISO 31000.

Buitrago, D., & Alvarado, E. (2018). Sistema de gestión de seguridad de la infromación aplicada al área de operaciones.

Cano, J. J. (2004). Inseguridad Informática: un concepto dual en seguridad informática. 19, 40-44. https://doi.org/10.16924/RIUA.V0I19.437

Castillo, M., & Molina, J. (2020). Análisis de riesgos al proceso de fiscalización de proyectos de ingeniería para una empresa que brinda servicios de ingeniería bajo la norma ISO/IEC 27005. ESPOL. FIEC.

Centro Criptológico Nacional. (2023). CNN. https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/9572-pilar-herramienta-de-analisis-y-gestion-de-riesgos.html

Cheng, J., Goto, Y., Morimoto, S., & Horie, D. (2008). A security engineering environment based on ISO/IEC standards: Providing standard, formal, and consistent supports for design,

development, operation, and maintenance of secure information systems. Proceedings of the 2nd International Conference on Information Security and Assurance, ISA 2008, 350-354. https://doi.org/10.1109/ISA.2008.106

Plan Nacional de Desarrollo 2017-2021- Toda una Vida, 1 (2017) (testimony of Consejo Nacional de Planificación: REPÚBLICA DEL ECUADOR (CNP) & Lenín Moreno). https://www.mendeley.com/catalogue/d2c0c0ae-b214-3f93-ad9f-26e467bd225a/?utm_source=desktop&utm_medium=1.19.8&utm_campaign=open_catalog&userDocumentId=%7Baece4158-d674-47db-817a-0be983434d3f%7D

LEY ORGANICA DE TRANSPARENCIA Y ACCESO A LA INFORMACION PUBLICA, (2004). www.lexis.com.ec

CONTRALORÍA GENERAL DEL ESTADO. (2014, diciembre 16). NORMAS DE CONTROL INTERNO DE LA CONTRALORIA GENERAL DEL ESTADO. www.gob.ec

De la Rosa, M. (2021). Automatización de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001. Universidad y Sociedad, 13(5), 495-506. https://rus.ucf.edu.cu/index.php/rus/article/view/2260

Dhillon, G., Smith, K., & Dissanayaka, I. (2021). Information systems security research agenda: Exploring the gap between research and practice. The Journal of Strategic Information Systems, 30(4), 101693. https://doi.org/10.1016/J.JSIS.2021.101693

Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II : Catálogo de elementos, (testimony of Dirección General de Modernización Administrativa & Procedimientos e Impulso de la Administración Electrónica). Recuperado 27 de mayo de 2023, de http://administracionelectronica.gob.es/

Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método, (2012) (testimony of Dirección General de Modernización Administrativa & Procedimientos Impulso de la Administración Electrónica). http://administracionelectronica.gob.es/

Fernández, G. (2021). Análisis y diseño de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001, orientando a la disminución de riesgos en la unidad de informatica del GAD municipal del cantón Pujilí. 7(2), 196.

Fondo de Población de las Naciones Unidad- UNFPA. (2017). Objetivos y metas de desarrollo sostenible - Desarrollo Sostenible. Web Page. https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

Gallego Ramos, J. R. (2018). Building the theoretical framework of a research study. Cadernos de Pesquisa, 48(169), 830-854. https://doi.org/10.1590/198053145177

Guano, M., & Jaramillo, M. (2020). Diseño de un SGSI bajo norma ISO/IEC 27001:2013.

Hermoso-Orzáez, M. J., & Garzón-Moreno, J. (2022). Risk management methodology in the supply chain: a case study applied. Annals of Operations Research, 313(2), 1051-1075. https://doi.org/10.1007/S10479-021-04220-Y/TABLES/14

Hohan, A. I., Olaru, M., & Pirnea, I. C. (2015). Assessment and Continuous Improvement of Information Security Based on TQM and Business Excellence Principles. Procedia Economics and Finance, 32, 352-359. https://doi.org/10.1016/S2212-5671(15)01404-5

Imbaquingo, D., San Pedro, L., Diaz, J., Saltos, T., & Arciniega, S. (2021). Let's talk about Computer Audit Quality: A systematic literature review. 2021 International Conference on Maintenance and Intelligent Asset Management, ICMIAM 2021. https://doi.org/10.1109/ICMIAM54662.2021.9715192

Imbaquingo, E. D. E., Diaz, F. J., Egas, R. M. B., Sinchiguano, C. F. A., & Misacango, L. R. A. (2020). Evaluation model of computer audit methodologies based on inherent risk. Iberian Conference on Information Systems and Technologies, CISTI, 2020-June. https://doi.org/10.23919/CISTI49556.2020.9140877

Imbaquingo, E. D. E., Diaz, F. J., Saltos, E. T. K., Hidrobo, S. R. A., Leon, V. D. A., & Ordonez, A. R. (2020). Information security issues in educational institutions. Iberian Conference on

Information Systems and Technologies, CISTI, 2020-June. https://doi.org/10.23919/CISTI49556.2020.9141014

Imbaquingo, E. D. E., Jácome, L. J. G., & Pusdá, C. M. R. (2017). Fundamentos de Auditoría Informática basada en riesgos. En F. Mafla (Ed.), Fundamentos de Auditoria basada en riesgos. Imprenta Universitaria - Universidad Técnica del Norte. http://repositorio.utn.edu.ec/handle/123456789/6794

Imbaquingo, E. D. E., & Pusda, C. M. R. (2015). EVALUACIÓN DE AMENAZAS Y VULNERABILIDADES DEL MÓDULO DE GESTIÓN ACADÉMICA - SISTEMA INFORMÁTICO INTEGRADO UNIVERSITARIO DE LA UNIVERSIDAD TÉCNICA DEL NORTE, APLICANDO ISO 27000 [Universidad de las Fuerzas Armadas ESPE]. http://repositorio.espe.edu.ec/handle/21000/12355

ISO. (2018, febrero). ISO - ISO/IEC 27000:2018 - Information technology — Security techniques — Information security management systems — Overview and vocabulary. https://www.iso.org/standard/73906.html

ISO/IEC. (2018, febrero). ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary. ISO.org [Online]. http://standards.iso.org/ittf/PubliclyAvailableStandards/c066435_ISO_IEC_27000_2016(E).zip

Kisan, S., & Rao, C. (2020). INFORMATION SECURITY LECTURE NOTES (Subject Code: BIT 301) for Bachelor of Technology in Information Technology [Veer Surendra Sai University of Technology]. moz-extension://3ca42106-e67d-42d4-b6ab-784d47c949e6/enhanced-reader.html?openApp&pdf=https%3A%2F%2Fwww.vssut.ac.in%2Flecture_notes%2Flecture1423183198.pdf

López, E. (2018). El método delphi en la investigación actual en educación: Una revisión teórica y metodológica. Educacion XX1, 21(1), 17-40. https://doi.org/10.5944/educXX1.15536

Lopez, R. (2016). Metodologías para el análisis de riesgo de la seguridad de la información. 0-3.

López Rubio, C. P. (2014). Tecnología de la Información y la Comunicación Tecnología de la Información y la Comunicación. Editorial Planeta Alvi. https://books.google.com/books?id=JEJRCgAAQBAJ&pgis=1

Mahfouz Alhassan, M., & Adjei-Quaye, A. (2017). Information Security in an Organization. International Journal of Computer. http://ijcjournal.org/

Michilena, J., & Díaz, P. (2018). Sistema de Gestión de Seguridad de la Información (SGSI) en el Comando Provincial de Policía «Imbabura No. 12».

Mieres, J. (2009). Ataques informáticos.

MINTIC. (2016). Guía para la Gestión y Clasificación de Activos de Información. Ministerio de Tecnologías de la Información y Comunicaciones, 5, 18.

Molina, M. (2015). Propuesta de un Plan de Gestión de Riesgos de Tecnología aplicado en la Escuela Superior Politécnica del Litoral. moz-extension://3ca42106-e67d-42d4-b6ab-784d47c949e6/enhanced-reader.html?openApp&pdf=http%3A%2F%2Fwww.dit.upm.es%2F~posgrado%2Fdoc%2FTFM%2FTFMs2014-2015%2FTFM_Maria_Fernanda_Molina_Miranda_2015.pdf

Mujica. (2015). Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos. https://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf

Muñoz, R. (2019). Análisis De La Situación Actual De La Metodología Para Proyectos De Servicios Tecnológicos. Caso Ciateq Ac. 111.

NIST. (2018). LA SEGURIDAD CIBERNÉTICA. https://www.nist.gov/cybersecurity

Novoa, H. (2015). Metodología para la implementación de un SGSI en la Fundación Universitaria Juan de Castellanos bajo la norma ISO 27001:2005. 95.

Orellana, L. (2018). Estadística Desctiptiva. Estadistica descriptiva, 1-64.

Recalde, J. (2019). Plan de implementación de un SGSI y aplicación de controles críticos en el centro de operaciones de seguridad en la empresa GMS. Quito, 2019.

Registro Oficial. (2020, enero 10). Esquema Gubernamental de Seguridad de la Información. Ecuador. Edicion Especial No. 228. https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/ediciones-especiales/item/12413-edicion-especial-no-228

Restrepo Ortiz, G. E., & Zabala Mendoza, D. E. (2016). Indicadores de gestión para proyectos de investigación y extensión en instituciones de Educación Superior. Revista Ciencias Estratégicas, 24(36), 451-461. https://doi.org/10.18566/rces.v24n36.a13

Romero, M., Figueroa, G., & Vera, D. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. En Aplicaciones Criptográficas.

Satán, D. (2017). Planteamiento de almacenamiento y gestión de LOGS para fortalecer la seguaridad informática de una emprsa telefónica. Universidad de Guayaquil Facultad de Ciencias Administrativas.

Silva, M. R. da, & Montilha, R. de C. I. (2021). Contribuições da técnica Delphi para a validação de uma avaliação de terapia ocupacional em deficiência visual. Cadernos Brasileiros de Terapia Ocupacional, 29, e2863. https://doi.org/10.1590/2526-8910.CTOAO2163

Suarez, R. (2015). ANALISIS DE ACTIVOS DE INFORMACION PARA UN SISTEMA MISIONAL BASADOS EN LA METODOLOGIA MAGERIT V3 Y LA NORMA ISO 27001:2013. Rafael. Dk, 53(9), 1689-1699.

Trujillo, D., & Rozo, J. (2018). Gestión del riesgo en seguridad de la información : caso de estudio en el repositorio institucional Unisalle - Rius colección tegra y propuesta metodológica a partir de la comparación de normas y estándares internacionales ISO 27005 , ISO 31000 y Octave. Gestión del riesgo en seguridad de la información : caso de estudio en el repositorio institucional Unisalle - Rius colección tegra y propuesta metodológica a partir de la comparación de normas y estándares internacionales ISO 27005, ISO 31000 y Octave, 2014-10-02, 1-89.

Viguri Cordero, J. A. (2021). Las normas ISO/IEC como mecanismos de responsabilidad proactiva en el Reglamento General de Protección de Datos. IDP. Revista de Internet Derecho y Política. https://doi.org/10.7238/idp.v0i33.376366

Villacís, M. (2016). Diseño de un sistema de Gestión de la seguridad de la Información (SGSI) basado en la Norma ISO 27001:2013 para la red corporativa de la empresa Ecuatronix. En Tesis. http://dspace.ups.edu.ec/handle/123456789/12406%0Ahttp://dspace.ups.edu.ec/bitstream/123456789/5081/1/UPS-CYT00109.pdf

Wang, C.-H., & Tsai, D.-R. (2009). Integrated installing ISO 9000 and ISO 27000 management systems on an organization. 43rd Annual 2009 International Carnahan Conference on Security Technology, 265-267. https://doi.org/10.1109/CCST.2009.533552710.1109/CCST.2009.5335527

Anexos

Anexo 1: Encuesta sobre la valoración de los activos del DDTI-UTN

UNIVERSIDAD TÉCNICA DEL NORTE

UNIVERSIDAD ACREDITADA RESOLUCIÓN 002-CONEA-2010-129-DC
Resolución No 001-073 CEAACES – 2013 – 13

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

Encuesta sobre la Conciencia en la Gestión de Riesgos

La presente encuesta tiene como finalidad realizar una valoración de los activos de la información - con la finalidad de conocer el nivel de riesgos existentes para los activos de la información del DDTI, solicita a usted de la manera más comedida, brinde la información respectiva, descrita en las siguientes preguntas. Su información será estrictamente confidencial.

A continuación, usted encontrará una serie de preguntas como guía para la correcta calificación de los riesgos de los activos.

• Confidencialidad : ¿ Cómo afectaría al DDTI que la información sea conocida por personas ajenas no autorizadas?

• Integridad : ¿Qué perjuicio causaría para el DDTI que estuviera dañado o corrupto?

• Disponibilidad :¿Cómo afectaría al DDTI no poder utilizar un activo?

En cada numeral usted debe calificar el riesgo del activo con base en los siguientes criterios:

10: Extremo
9: Muy alto
6-8: Alto
3-5: Medio
1-2. Bajo
0. Despreciable

CÓDIGO ACTIVO	NOMBRE DE ACTIVO	C	I	D
IN-01	Base de datos			
IN-02	Archivos de datos			
IN-03	Documentación interna			
IN-04	Material impreso			
IN-05	Carpetas compartidas			
SW-01	Motor de base de datos			
SW-02	Repositorio de aplicaciones desarrolladas			
SW-03	Antivirus			
SW-04	Firewall			
SW-05	Licencias			
SW-06	Navegadores			

SW-07	Sistemas Operativos
HW-01	Dispositivos de almacenamiento
HW-02	Computadoras
HW-03	Teléfonos IP
HW-04	Servidores
HW-05	Equipos para funcionamiento de red (switchs /Access point / transceivers)
HW-06	Equipo multifuncional (impresora/Scanner)
HW-07	Dispositivos de grabación y fotografía
HW-08	Radios de comunicación
AUX-01	UPS
AUX-02	Generador Eléctrico
AUX-03	Equipos de climatización
AUX-04	Mobiliario
SR-01	Telefonía
SR-02	Internet
SR-03	Electricidad
SR-04	Correo institucional
SR-05	Soporte a la red
SR-06	Soporte a los servicios informáticos
SR-07	Mantenimiento a los equipos
IF-01	Instalación de red de datos
IF-02	Instalación de red eléctrica
IF-03	UPS del centro cableado
IF-04	Espacio Físico del DDTI
PR-01	Personal Administrativo
PR-02	Personal de desarrollo
RD-01	Ethernet
RD-02	Red Inalámbrica
RD-03	Red LAN
RD-04	Red Telefónica

Nota: Elaboración propia

Anexo 2: Entrevista al Sub - director del DDTI-UTN

UNIVERSIDAD TÉCNICA DEL NORTE

UNIVERSIDAD ACREDITADA RESOLUCIÓN 002-CONEA-2010-129-DC
Resolución No 001-073 CEAACES – 2013 – 13
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

Trabajo de Titulación
Entrevista sobre la situación actual del DDTI-UTN

La presente entrevista tiene como finalidad recolectar información necesaria acerca de la situación actual del DDTI-UTN.
Para esta entrevista se tomó en consideración al Sub – director del DDTI-UTN, Ingeniero Juan Carlos García. La transcripción de la entrevista es la siguiente.

Entrevista dirigida por: Santiago Guzmán (Auditor 1)	**Fecha de la reunión:** 01/02/2023 **Hora inicio:** 08:00 am **Hora fin:** 08:15 am	**Lugar:** DDTI

Tema: Instrumentos de Evaluación - Entrevista

Dirigida a: Ing. Juan Carlos García

INFORMACIÓN GENERAL

1. Presentación del o de los entrevistadores
2. Definición del tema y objetivos de la evaluación técnica
3. Solicitar permisos para grabar la entrevista
4. Aclarar términos de confidencialidad de la entrevista

NRO.	PREGUNTA	RESUMEN
1	¿La dirección general y ejecutiva ha considerado la importancia que tiene establecer un SGSI?	
2	¿Se tiene políticas de seguridad de los sistemas de información?	
3	¿Existe un responsable encargado de la seguridad de la información?	
4	¿Se realiza una clasificación de activos según la criticidad de estos?	
5	¿El personal tiene una capacitación adecuada de seguridad y tratamiento de activos?	
6	¿Qué seguridad física existe dentro del departamento ?	

7	¿Se tiene planes de contingencia en caso de que exista vulnerabilidades detectadas?	
8	¿Existe un control de acceso a los servicios de red?	
9	¿Cada que intervalo de tiempo se realiza revisiones de la política de seguridad?	
10	¿Se tienen políticas o medidas para proteger la confidencialidad e integridad de la información que se maneja dentro del departamento?	
11	¿Cuáles son las brechas internas como externas que existe en el departamento?	
12	¿ Actualmente la institución cuenta con procesos y políticas definidas, documentadas? Si es el caso quien las aprueba	
13	¿Cuáles son los procesos críticos del departamento? Aportan valor y que tienen especial relación con el enfoque estratégico de la institución(base de datos redes)	
14	¿Quiénes son los responsables de las distintas áreas del departamento ?	
15	¿Existen controles existentes en el departamento y cuáles son ?	

Nota: Elaboración propia

Anexo 3: Identificación de Amenazas en el DDTI-UTN

ACTIVO	AMENAZA
INFORMACIÓN	
BASE DE DATOS	
Base de datos	[E.15] Alteración de la información
Base de datos	[E.18] Destrucción de la información
Base de datos	[E.19] Fugas de información
Base de datos	[A.5] Suplantación de la identidad
Base de datos	[A.6] Abuso de privilegios de acceso
Base de datos	[A.11] Acceso no autorizado
ARCHIVO DE DATOS	
Archivo de datos	[E.15] Alteración de la información
Archivo de datos	[E.18] Destrucción de la información
Archivo de datos	[E.19] Fugas de información
Archivo de datos	[A.5] Suplantación de la identidad
Archivo de datos	[A.6] Abuso de privilegios de acceso
Archivo de datos	[A.11] Acceso no autorizado

DOCUMENTACIÓN INTERNA	
Documentación interna	[E.15] Alteración de la información
Documentación interna	[E.18] Destrucción de la información
Documentación interna	[E.19] Fugas de información
Documentación interna	[A.5] Suplantación de la identidad
Documentación interna	[A.6] Abuso de privilegios de acceso
Documentación interna	[A.11] Acceso no autorizado
MATERIAL IMPRESO	
Material impreso	[N.1] Fuego
Material impreso	[N.2] Daños por agua
Material impreso	[N.*] Desastres naturales
Material impreso	[I.1] Fuego
Material impreso	[I.2] Daños por agua
Material impreso	[I.*] Desastres industriales
Material impreso	[I.3] Contaminación medioambiental
Material impreso	[I.7] Condiciones inadecuadas de temperatura o humedad
Material impreso	[E.1] Errores de los usuarios
Material impreso	[E.15] Alteración de la información
Material impreso	[E.18] Destrucción de la información
Material impreso	[E.19] Fugas de información
Material impreso	[A.7] Uso no previsto
Material impreso	[A.11] Acceso no autorizado
Material impreso	[A.15] Modificación de la información
Material impreso	[A.18] Destrucción de la información
Material impreso	[A.26] Ataques destructivos
CARPETAS COMPARTIDAS	
Carpetas compartidas	[E.15] Alteración de la información
Carpetas compartidas	[E.18] Destrucción de la información
Carpetas compartidas	[E.19] Fugas de información
Carpetas compartidas	[A.5] Suplantación de la identidad
Carpetas compartidas	[A.6] Abuso de privilegios de acceso
Carpetas compartidas	[A.11] Acceso no autorizado
APLICACIONES	
MOTOR DE BASE DE DATOS	
Motor de base de datos	[I.5.1] Avería de origen lógico
Motor de base de datos	[E.8] Difusión de software dañino
Motor de base de datos	[E.20]Vulnerabilidades de los programas (software)

Motor de base de datos	[E.21] Errores de mantenimiento/actualización de programas (software)
Motor de base de datos	[A.8] Difusión de software dañino
Motor de base de datos	[A.22] Manipulación de programas

REPOSITORIO DE APLICACIONES DESARROLLADAS

Repositorio de aplicación desarrolladas	[I.5.1] Avería de origen lógico
Repositorio de aplicación desarrolladas	[E.8] Difusión de software dañino
Repositorio de aplicación desarrolladas	[E.20]Vulnerabilidades de los programas (software)
Repositorio de aplicación desarrolladas	[E.21] Errores de mantenimiento/actualización de programas (software)
Repositorio de aplicación desarrolladas	[A.8] Difusión de software dañino
Repositorio de aplicación desarrolladas	[A.22] Manipulación de programas
ANTIVIRUS	
Antivirus	[I.5.1] Avería de origen lógico
Antivirus	[E.8] Difusión de software dañino
Antivirus	[E.20]Vulnerabilidades de los programas (software)
Antivirus	[E.21] Errores de mantenimiento/actualización de programas (software)
Antivirus	[A.8] Difusión de software dañino
Antivirus	[A.22] Manipulación de programas
FIREWALL	
Firewall	[I.5.1] Avería de origen lógico
Firewall	[E.4] Errores de configuración
Firewall	[E.8] Difusión de software dañino
Firewall	[E.18] Destrucción de la información
Firewall	[E.20]Vulnerabilidades de los programas (software)
Firewall	[E.21] Errores de mantenimiento/actualización de programas (software)
Firewall	[A.4] Manipulación de los ficheros de configuración
Firewall	[A.5] Suplantación de la identidad

Firewall	[A.8] Difusión de software dañino
Firewall	[A.22] Manipulación de programas
LICENCIAS	
Licencias	[I.5.1] Avería de origen lógico
Licencias	[E.8] Difusión de software dañino
Licencias	[E.20]Vulnerabilidades de los programas (software)
Licencias	[E.21] Errores de mantenimiento/actualización de programas (software)
Licencias	[A.8] Difusión de software dañino
Licencias	[A.22] Manipulación de programas
NAVEGADORES	
Navegadores	[I.5.1] Avería de origen lógico
Navegadores	[E.8] Difusión de software dañino
Navegadores	[E.20]Vulnerabilidades de los programas (software)
Navegadores	[E.21] Errores de mantenimiento/actualización de programas (software)
Navegadores	[A.8] Difusión de software dañino
Navegadores	[A.22] Manipulación de programas
SISTEMAS OPERATIVOS	
Sistemas operativos	[I.5.1] Avería de origen lógico
Sistemas operativos	[E.8] Difusión de software dañino
Sistemas operativos	[E.20]Vulnerabilidades de los programas (software)
Sistemas operativos	[E.21] Errores de mantenimiento/actualización de programas (software)
Sistemas operativos	[A.8] Difusión de software dañino
Sistemas operativos	[A.22] Manipulación de programas
EQUIPOS	
DISPOSITIVOS DE ALMACENAMIENTO	
Dispositivos de almacenamiento	[N.1] Fuego
Dispositivos de almacenamiento	[N.2] Daños por agua
Dispositivos de almacenamiento	[N.*] Desastres naturales
Dispositivos de almacenamiento	[I.1] Fuego

Dispositivos de almacenamiento	[I.2] Daños por agua
Dispositivos de almacenamiento	[I.*] Desastres industriales
Dispositivos de almacenamiento	[I.3] Contaminación medioambiental
Dispositivos de almacenamiento	[I.4] Contaminación electromagnética
Dispositivos de almacenamiento	[I.5.2] Avería de origen físico
Dispositivos de almacenamiento	[I.6] Corte del suministro eléctrico
Dispositivos de almacenamiento	[I.7] Condiciones inadecuadas de temperatura o humedad
Dispositivos de almacenamiento	[I.11] Emanaciones electromagnéticas (TEMPEST)
Dispositivos de almacenamiento	[E.23] Errores de mantenimiento/actualización de equipos (hardware)
Dispositivos de almacenamiento	[E.24] Caída del sistema por agotamiento de recursos
Dispositivos de almacenamiento	[E.25] Pérdida de equipos
Dispositivos de almacenamiento	[A.11] Acceso no autorizado
Dispositivos de almacenamiento	[A.23] Manipulación de hardware
Dispositivos de almacenamiento	[A.24] Denegación de servicio
Dispositivos de almacenamiento	[A.25] Robo de equipos
Dispositivos de almacenamiento	[A.26] Ataques destructivos
	COMPUTADORAS
Computadoras	[N.1] Fuego
Computadoras	[N.2] Daños por agua
Computadoras	[N.*] Desastres naturales
Computadoras	[I.1] Fuego
Computadoras	[I.2] Daños por agua
Computadoras	[I.*] Desastres industriales
Computadoras	[I.3] Contaminación medioambiental
Computadoras	[I.4] Contaminación electromagnética
Computadoras	[I.5.2] Avería de origen físico
Computadoras	[I.6] Corte del suministro eléctrico

Computadoras	[I.7] Condiciones inadecuadas de temperatura o humedad
Computadoras	[I.11] Emanaciones electromagnéticas (TEMPEST)
Computadoras	[E.23] Errores de mantenimiento/actualización de equipos (hardware)
Computadoras	[E.24] Caída del sistema por agotamiento de recursos
Computadoras	[E.25] Pérdida de equipos
Computadoras	[A.11] Acceso no autorizado
Computadoras	[A.23] Manipulación de hardware
Computadoras	[A.24] Denegación de servicio
Computadoras	[A.25] Robo de equipos
Computadoras	[A.26] Ataques destructivos
TELÉFONOS IP	
Teléfonos IP	[N.1] Fuego
Teléfonos IP	[N.2] Daños por agua
Teléfonos IP	[N.*] Desastres naturales
Teléfonos IP	[I.1] Fuego
Teléfonos IP	[I.2] Daños por agua
Teléfonos IP	[I.*] Desastres industriales
Teléfonos IP	[I.3] Contaminación medioambiental
Teléfonos IP	[I.4] Contaminación electromagnética
Teléfonos IP	[I.5.2] Avería de origen físico
Teléfonos IP	[I.6] Corte del suministro eléctrico
Teléfonos IP	[I.7] Condiciones inadecuadas de temperatura o humedad
Teléfonos IP	[I.11] Emanaciones electromagnéticas (TEMPEST)
Teléfonos IP	[E.23] Errores de mantenimiento/actualización de equipos (hardware)
Teléfonos IP	[E.24] Caída del sistema por agotamiento de recursos
Teléfonos IP	[E.25] Pérdida de equipos
Teléfonos IP	[A.11] Acceso no autorizado
Teléfonos IP	[A.23] Manipulación de hardware
Teléfonos IP	[A.24] Denegación de servicio
Teléfonos IP	[A.25] Robo de equipos
Teléfonos IP	[A.26] Ataques destructivos
SERVIDORES	
Servidores	[N.1] Fuego

Servidores	[N.2] Daños por agua
Servidores	[N.*] Desastres naturales
Servidores	[I.1] Fuego
Servidores	[I.2] Daños por agua
Servidores	[I.*] Desastres industriales
Servidores	[I.3] Contaminación medioambiental
Servidores	[I.4] Contaminación electromagnética
Servidores	[I.5.2] Avería de origen físico
Servidores	[I.6] Corte del suministro eléctrico
Servidores	[I.7] Condiciones inadecuadas de temperatura o humedad
Servidores	[I.11] Emanaciones electromagnéticas (TEMPEST)
Servidores	[E.23] Errores de mantenimiento/actualización de equipos (hardware)
Servidores	[E.24] Caída del sistema por agotamiento de recursos
Servidores	[E.25] Pérdida de equipos
Servidores	[A.11] Acceso no autorizado
Servidores	[A.23] Manipulación de hardware
Servidores	[A.24] Denegación de servicio
Servidores	[A.25] Robo de equipos
Servidores	[A.26] Ataques destructivos

EQUIPO PARA EL FUNCIONAMIENTO DE RED

Equipo para el funcionamiento de red	[N.1] Fuego
Equipo para el funcionamiento de red	[N.2] Daños por agua
Equipo para el funcionamiento de red	[N.*] Desastres naturales
Equipo para el funcionamiento de red	[I.1] Fuego
Equipo para el funcionamiento de red	[I.2] Daños por agua
Equipo para el funcionamiento de red	[I.*] Desastres industriales
Equipo para el funcionamiento de red	[I.3] Contaminación medioambiental
Equipo para el funcionamiento de red	[I.4] Contaminación electromagnética

Equipo para el funcionamiento de red	[I.5.2] Avería de origen físico
Equipo para el funcionamiento de red	[I.6] Corte del suministro eléctrico
Equipo para el funcionamiento de red	[I.7] Condiciones inadecuadas de temperatura o humedad
Equipo para el funcionamiento de red	[I.11] Emanaciones electromagnéticas (TEMPEST)
Equipo para el funcionamiento de red	[E.23] Errores de mantenimiento/actualización de equipos (hardware)
Equipo para el funcionamiento de red	[E.24] Caída del sistema por agotamiento de recursos
Equipo para el funcionamiento de red	[E.25] Pérdida de equipos
Equipo para el funcionamiento de red	[A.11] Acceso no autorizado
Equipo para el funcionamiento de red	[A.23] Manipulación de hardware
Equipo para el funcionamiento de red	[A.24] Denegación de servicio
Equipo para el funcionamiento de red	[A.25] Robo de equipos
Equipo para el funcionamiento de red	[A.26] Ataques destructivos
	EQUIPO MULTIFUNCIONAL
Equipo multifuncional	[N.1] Fuego
Equipo multifuncional	[N.2] Daños por agua
Equipo multifuncional	[N.*] Desastres naturales
Equipo multifuncional	[I.1] Fuego
Equipo multifuncional	[I.2] Daños por agua
Equipo multifuncional	[I.*] Desastres industriales
Equipo multifuncional	[I.3] Contaminación medioambiental
Equipo multifuncional	[I.4] Contaminación electromagnética
Equipo multifuncional	[I.5.2] Avería de origen físico
Equipo multifuncional	[I.6] Corte del suministro eléctrico
Equipo multifuncional	[I.7] Condiciones inadecuadas de temperatura o humedad
Equipo multifuncional	[I.11] Emanaciones electromagnéticas (TEMPEST)
Equipo multifuncional	[E.23] Errores de mantenimiento/actualización de equipos (hardware)

Equipo multifuncional	[E.24] Caída del sistema por agotamiento de recursos
Equipo multifuncional	[E.25] Pérdida de equipos
Equipo multifuncional	[A.11] Acceso no autorizado
Equipo multifuncional	[A.23] Manipulación de hardware
Equipo multifuncional	[A.24] Denegación de servicio
Equipo multifuncional	[A.25] Robo de equipos
Equipo multifuncional	[A.26] Ataques destructivos

DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA

Dispositivo de grabación y fotografía	[N.1] Fuego
Dispositivo de grabación y fotografía	[N.2] Daños por agua
Dispositivo de grabación y fotografía	[N.*] Desastres naturales
Dispositivo de grabación y fotografía	[I.1] Fuego
Dispositivo de grabación y fotografía	[I.2] Daños por agua
Dispositivo de grabación y fotografía	[I.*] Desastres industriales
Dispositivo de grabación y fotografía	[I.3] Contaminación medioambiental
Dispositivo de grabación y fotografía	[I.4] Contaminación electromagnética
Dispositivo de grabación y fotografía	[I.5.2] Avería de origen físico
Dispositivo de grabación y fotografía	[I.6] Corte del suministro eléctrico
Dispositivo de grabación y fotografía	[I.7] Condiciones inadecuadas de temperatura o humedad
Dispositivo de grabación y fotografía	[I.11] Emanaciones electromagnéticas (TEMPEST)
Dispositivo de grabación y fotografía	[E.23] Errores de mantenimiento/actualización de equipos (hardware)
Dispositivo de grabación y fotografía	[E.24] Caída del sistema por agotamiento de recursos
Dispositivo de grabación y fotografía	[E.25] Pérdida de equipos
Dispositivo de grabación y fotografía	[A.11] Acceso no autorizado

Dispositivo de grabación y fotografía	[A.23] Manipulación de hardware
Dispositivo de grabación y fotografía	[A.24] Denegación de servicio
Dispositivo de grabación y fotografía	[A.25] Robo de equipos
Dispositivo de grabación y fotografía	[A.26] Ataques destructivos
RADIOS DE COMUNICACIÓN	
Radios de comunicación	[N.1] Fuego
Radios de comunicación	[N.2] Daños por agua
Radios de comunicación	[N.*] Desastres naturales
Radios de comunicación	[I.1] Fuego
Radios de comunicación	[I.2] Daños por agua
Radios de comunicación	[I.*] Desastres industriales
Radios de comunicación	[I.3] Contaminación medioambiental
Radios de comunicación	[I.4] Contaminación electromagnética
Radios de comunicación	[I.5.2] Avería de origen físico
Radios de comunicación	[I.6] Corte del suministro eléctrico
Radios de comunicación	[I.7] Condiciones inadecuadas de temperatura o humedad
Radios de comunicación	[I.11] Emanaciones electromagnéticas (TEMPEST)
Radios de comunicación	[E.23] Errores de mantenimiento/actualización de equipos (hardware)
Radios de comunicación	[E.24] Caída del sistema por agotamiento de recursos
Radios de comunicación	[E.25] Pérdida de equipos
Radios de comunicación	[A.11] Acceso no autorizado
Radios de comunicación	[A.23] Manipulación de hardware
Radios de comunicación	[A.24] Denegación de servicio
Radios de comunicación	[A.25] Robo de equipos
Radios de comunicación	[A.26] Ataques destructivos
COMUNICACIÓN	
ETHERNET	
Ethernet	[I.8] Fallo de servicios de comunicación
Ethernet	[E.2] Errores del administrador del sistema
Ethernet	[E.9] Errores de [re-]encaminamiento
Ethernet	[E.10] Errores de secuencia
Ethernet	[E.15] Alteración de la información
Ethernet	[E.19] Fugas de información
Ethernet	[E.24] Caída del sistema por agotamiento de recursos
Ethernet	[A.5] Suplantación de la identidad

Ethernet	[A.7] Uso no previsto
Ethernet	[A.9] [Re-]encaminamiento de mensajes
Ethernet	[A.10] Alteración de secuencia
Ethernet	[A.11] Acceso no autorizado
Ethernet	[A.12] Análisis de tráfico
Ethernet	[A.14] Interceptación de información (escucha)
Ethernet	[A.15] Modificación de la información
Ethernet	[A.18] Destrucción de la información
Ethernet	[A.24] Denegación de servicio
	RED INALAMBRICA
Red inalámbrica	[I.8] Fallo de servicios de comunicación
Red inalámbrica	[E.2] Errores del administrador del sistema
Red inalámbrica	[E.9] Errores de [re-]encaminamiento
Red inalámbrica	[E.10] Errores de secuencia
Red inalámbrica	[E.15] Alteración de la información
Red inalámbrica	[E.19] Fugas de información
Red inalámbrica	[E.24] Caída del sistema por agotamiento de recursos
Red inalámbrica	[A.5] Suplantación de la identidad
Red inalámbrica	[A.7] Uso no previsto
Red inalámbrica	[A.9] [Re-]encaminamiento de mensajes
Red inalámbrica	[A.10] Alteración de secuencia
Red inalámbrica	[A.11] Acceso no autorizado
Red inalámbrica	[A.12] Análisis de tráfico
Red inalámbrica	[A.14] Interceptación de información (escucha)
Red inalámbrica	[A.15] Modificación de la información
Red inalámbrica	[A.18] Destrucción de la información
Red inalámbrica	[A.24] Denegación de servicio
	RED LAN
Red LAN	[I.8] Fallo de servicios de comunicación
Red LAN	[E.2] Errores del administrador del sistema
Red LAN	[E.9] Errores de [re-]encaminamiento
Red LAN	[E.10] Errores de secuencia
Red LAN	[E.15] Alteración de la información
Red LAN	[E.19] Fugas de información
Red LAN	[E.24] Caída del sistema por agotamiento de recursos
Red LAN	[A.5] Suplantación de la identidad
Red LAN	[A.7] Uso no previsto
Red LAN	[A.9] [Re-]encaminamiento de mensajes
Red LAN	[A.10] Alteración de secuencia
Red LAN	[A.11] Acceso no autorizado
Red LAN	[A.12] Análisis de tráfico

Red LAN	[A.14] Interceptación de información (escucha)
Red LAN	[A.15] Modificación de la información
Red LAN	[A.18] Destrucción de la información
Red LAN	[A.24] Denegación de servicio
	RED TELEFÓNICA
Red telefónica	[I.8] Fallo de servicios de comunicación
Red telefónica	[E.2] Errores del administrador del sistema
Red telefónica	[E.9] Errores de [re-]encaminamiento
Red telefónica	[E.10] Errores de secuencia
Red telefónica	[E.15] Alteración de la información
Red telefónica	[E.19] Fugas de información
Red telefónica	[E.24] Caída del sistema por agotamiento de recursos
Red telefónica	[A.5] Suplantación de la identidad
Red telefónica	[A.7] Uso no previsto
Red telefónica	[A.9] [Re-]encaminamiento de mensajes
Red telefónica	[A.10] Alteración de secuencia
Red telefónica	[A.11] Acceso no autorizado
Red telefónica	[A.12] Análisis de tráfico
Red telefónica	[A.14] Interceptación de información (escucha)
Red telefónica	[A.15] Modificación de la información
Red telefónica	[A.18] Destrucción de la información
Red telefónica	[A.24] Denegación de servicio
	ELEMENTOS AUXILIARES
	UPS
UPS	[N.1] Fuego
UPS	[N.2] Daños por agua
UPS	[N.*] Desastres naturales
UPS	[I.1] Fuego
UPS	[I.2] Daños por agua
UPS	[I.*] Desastres industriales
UPS	[I.3] Contaminación medioambiental
UPS	[E.23] Errores de mantenimiento/actualización de equipos (hardware)
UPS	[A.7] Uso no previsto
UPS	[A.23] Manipulación de hardware
UPS	[A.25] Robo de equipos
UPS	[A.26] Ataques destructivos
	GENERADOR ELÉCTRICO
Generador eléctrico	[N.1] Fuego

Generador eléctrico	[N.2] Daños por agua
Generador eléctrico	[N.*] Desastres naturales
Generador eléctrico	[I.1] Fuego
Generador eléctrico	[I.2] Daños por agua
Generador eléctrico	[I.*] Desastres industriales
Generador eléctrico	[I.3] Contaminación medioambiental
Generador eléctrico	[E.23] Errores de mantenimiento/actualización de equipos (hardware)
Generador eléctrico	[A.7] Uso no previsto
Generador eléctrico	[A.23] Manipulación de hardware
Generador eléctrico	[A.25] Robo de equipos
Generador eléctrico	[A.26] Ataques destructivos
EQUIPOS DE CLIMATIZACIÓN	
Equipos de climatización	[N.1] Fuego
Equipos de climatización	[N.2] Daños por agua
Equipos de climatización	[N.*] Desastres naturales
Equipos de climatización	[I.1] Fuego
Equipos de climatización	[I.2] Daños por agua
Equipos de climatización	[I.*] Desastres industriales
Equipos de climatización	[I.3] Contaminación medioambiental
Equipos de climatización	[E.23] Errores de mantenimiento/actualización de equipos (hardware)
Equipos de climatización	[A.7] Uso no previsto
Equipos de climatización	[A.23] Manipulación de hardware
Equipos de climatización	[A.25] Robo de equipos
Equipos de climatización	[A.26] Ataques destructivos
MOBILIARIO	
Mobiliario	[N.1] Fuego
Mobiliario	[N.2] Daños por agua
Mobiliario	[N.*] Desastres naturales
Mobiliario	[I.1] Fuego
Mobiliario	[I.2] Daños por agua
Mobiliario	[I.*] Desastres industriales
Mobiliario	[I.3] Contaminación medioambiental
Mobiliario	[E.23] Errores de mantenimiento/actualización de equipos (hardware)
Mobiliario	[A.7] Uso no previsto
Mobiliario	[A.23] Manipulación de hardware
Mobiliario	[A.25] Robo de equipos
Mobiliario	[A.26] Ataques destructivos

SERVICIOS	
TELEFONÍA	
Telefonía	[E.15] Alteración de la información
Telefonía	[E.18] Destrucción de la información
Telefonía	[E.19] Fugas de información
Telefonía	[A.15] Modificación de la información
Telefonía	[A.18] Destrucción de la información
Telefonía	[A.24] Denegación de servicio
INTERNET	
Internet	[E.15] Alteración de la información
Internet	[E.18] Destrucción de la información
Internet	[E.19] Fugas de información
Internet	[A.5] Suplantación de la identidad
Internet	[A.15] Modificación de la información
Internet	[A.18] Destrucción de la información
Internet	[A.24] Denegación de servicio
ELECTRICIDAD	
Electricidad	[I.9] Interrupción de otros servicios o suministros esenciales
Electricidad	[E.15] Alteración de la información
Electricidad	[E.18] Destrucción de la información
CORREO INSTITUCIONAL	
Correo institucional	[E.1] Errores de los usuarios
Correo institucional	[E.2] Errores del administrador del sistema
Correo institucional	[E.15] Alteración de la información
Correo institucional	[E.18] Destrucción de la información
Correo institucional	[E.19] Fugas de información
Correo institucional	[E.24] Caída del sistema por agotamiento de recursos
Correo institucional	[A.5] Suplantación de la identidad
Correo institucional	[A.6] Abuso de privilegios de acceso
Correo institucional	[A.7] Uso no previsto
Correo institucional	[A.11] Acceso no autorizado
Correo institucional	[A.15] Modificación de la información
Correo institucional	[A.18] Destrucción de la información
Correo institucional	[A.24] Denegación de servicio
SOPORTE DE RED	
Soporte de red	[E.1] Errores de los usuarios
Soporte de red	[E.15] Alteración de la información
Soporte de red	[E.18] Destrucción de la información

Soporte de red	[E.19] Fugas de información
Soporte de red	[A.7] Uso no previsto
Soporte de red	[A.11] Acceso no autorizado
Soporte de red	[A.15] Modificación de la información
Soporte de red	[A.18] Destrucción de la información

SOPORTE A LOS SERVICIOS INFORMÁTICOS

Soporte a los servicios informáticos	[E.1] Errores de los usuarios
Soporte a los servicios informáticos	[E.2] Errores del administrador del sistema
Soporte a los servicios informáticos	[E.15] Alteración de la información
Soporte a los servicios informáticos	[E.18] Destrucción de la información
Soporte a los servicios informáticos	[E.19] Fugas de información
Soporte a los servicios informáticos	[E.24] Caída del sistema por agotamiento de recursos
Soporte a los servicios informáticos	[A.5] Suplantación de la identidad
Soporte a los servicios informáticos	[A.6] Abuso de privilegios de acceso
Soporte a los servicios informáticos	[A.7] Uso no previsto
Soporte a los servicios informáticos	[A.11] Acceso no autorizado
Soporte a los servicios informáticos	[A.15] Modificación de la información
Soporte a los servicios informáticos	[A.18] Destrucción de la información
Soporte a los servicios informáticos	[A.24] Denegación de servicio

MANTENIMIENTO DE EQUIPOS

Mantenimiento de equipos	[E.1] Errores de los usuarios
Mantenimiento de equipos	[E.2] Errores del administrador del sistema
Mantenimiento de equipos	[E.15] Alteración de la información
Mantenimiento de equipos	[E.18] Destrucción de la información
Mantenimiento de equipos	[E.19] Fugas de información
Mantenimiento de equipos	[E.24] Caída del sistema por agotamiento de recursos

Mantenimiento de equipos	[A.5] Suplantación de la identidad
Mantenimiento de equipos	[A.6] Abuso de privilegios de acceso
Mantenimiento de equipos	[A.7] Uso no previsto
Mantenimiento de equipos	[A.11] Acceso no autorizado
Mantenimiento de equipos	[A.15] Modificación de la información
Mantenimiento de equipos	[A.18] Destrucción de la información
Mantenimiento de equipos	[A.24] Denegación de servicio
INFRAESTRUCTURA	
INSTALACIÓN DE RED DE DATOS	
Instalación de red de datos	[N.1] Fuego
Instalación de red de datos	[N.2] Daños por agua
Instalación de red de datos	[N.*] Desastres naturales
Instalación de red de datos	[I.1] Fuego
Instalación de red de datos	[I.2] Daños por agua
Instalación de red de datos	[I.*] Desastres industriales
Instalación de red de datos	[I.3] Contaminación medioambiental
Instalación de red de datos	[I.4] Contaminación electromagnética
Instalación de red de datos	[E.25] Pérdida de equipos
Instalación de red de datos	[A.6] Abuso de privilegios de acceso
Instalación de red de datos	[A.7] Uso no previsto
Instalación de red de datos	[A.25] Robo de equipos
Instalación de red de datos	[A.26] Ataques destructivos
Instalación de red de datos	[A.27] Ocupación enemiga
INSTALACIÓN DE RED ELÉCTRICA	
Instalación de red eléctrica	[N.1] Fuego
Instalación de red eléctrica	[N.2] Daños por agua
Instalación de red eléctrica	[N.*] Desastres naturales
Instalación de red eléctrica	[I.1] Fuego
Instalación de red eléctrica	[I.2] Daños por agua
Instalación de red eléctrica	[I.*] Desastres industriales
Instalación de red eléctrica	[I.3] Contaminación medioambiental
Instalación de red eléctrica	[I.4] Contaminación electromagnética
Instalación de red eléctrica	[E.25] Pérdida de equipos
Instalación de red eléctrica	[A.6] Abuso de privilegios de acceso
Instalación de red eléctrica	[A.7] Uso no previsto
Instalación de red eléctrica	[A.25] Robo de equipos
Instalación de red eléctrica	[A.26] Ataques destructivos
Instalación de red eléctrica	[A.27] Ocupación enemiga
UPS DEL CENTRO CABLEADO	

UPS del centro cableado	[N.1] Fuego
UPS del centro cableado	[N.2] Daños por agua
UPS del centro cableado	[N.*] Desastres naturales
UPS del centro cableado	[I.1] Fuego
UPS del centro cableado	[I.2] Daños por agua
UPS del centro cableado	[I.*] Desastres industriales
UPS del centro cableado	[I.3] Contaminación medioambiental
UPS del centro cableado	[I.4] Contaminación electromagnética
UPS del centro cableado	[E.25] Pérdida de equipos
UPS del centro cableado	[A.6] Abuso de privilegios de acceso
UPS del centro cableado	[A.7] Uso no previsto
UPS del centro cableado	[A.25] Robo de equipos
UPS del centro cableado	[A.26] Ataques destructivos
UPS del centro cableado	[A.27] Ocupación enemiga
ESPACIO FÍSICO DDTI	
Espacio físico DDTI	[N.1] Fuego
Espacio físico DDTI	[N.2] Daños por agua
Espacio físico DDTI	[N.*] Desastres naturales
Espacio físico DDTI	[I.1] Fuego
Espacio físico DDTI	[I.2] Daños por agua
Espacio físico DDTI	[I.*] Desastres industriales
Espacio físico DDTI	[I.3] Contaminación medioambiental
Espacio físico DDTI	[I.4] Contaminación electromagnética
Espacio físico DDTI	[E.25] Pérdida de equipos
Espacio físico DDTI	[A.6] Abuso de privilegios de acceso
Espacio físico DDTI	[A.7] Uso no previsto
Espacio físico DDTI	[A.25] Robo de equipos
Espacio físico DDTI	[A.26] Ataques destructivos
Espacio físico DDTI	[A.27] Ocupación enemiga
PERSONAL	
PERSONAL ADMINISTRATIVO	
Personal Administrativo	[E.15] Alteración de la información
Personal Administrativo	[E.18] Destrucción de la información
Personal Administrativo	[E.19] Fugas de información
Personal Administrativo	[A.15] Modificación de la información
Personal Administrativo	[A.18] Destrucción de la información
Personal Administrativo	[A.19] Revelación de información
Personal Administrativo	[A.28] Indisponibilidad del personal
Personal Administrativo	[A.29] Extorsión
Personal Administrativo	[A.30] Ingeniería social (picaresca)

PERSONAL DE DESARROLLO	
Personal de desarrollo	[E.15] Alteración de la información
Personal de desarrollo	[E.18] Destrucción de la información
Personal de desarrollo	[E.19] Fugas de información
Personal de desarrollo	[A.15] Modificación de la información
Personal de desarrollo	[A.18] Destrucción de la información
Personal de desarrollo	[A.19] Revelación de información
Personal de desarrollo	[A.28] Indisponibilidad del personal
Personal de desarrollo	[A.29] Extorsión
Personal de desarrollo	[A.30] Ingeniería social (picaresca)

Nota: Elaboración propia

Anexo 4: Valoración de Amenazas en el DDTI-UTN

ACTIVO	AMENAZA	FRECUENCIA	D	I	C
INFORMACIÓN					
BASE DE DATOS					
Base de datos	[E.15] Alteración de la información	1		1%	
Base de datos	[E.18] Destrucción de la información	1	1%		
Base de datos	[E.19] Fugas de información	1			10%
Base de datos	[A.5] Suplantación de la identidad	10		10%	50%
Base de datos	[A.6] Abuso de privilegios de acceso	10	1%	10%	50%
Base de datos	[A.11] Acceso no autorizado	100		10%	50%
ARCHIVO DE DATOS					
Archivo de datos	[E.15] Alteración de la información	1		1%	
Archivo de datos	[E.18] Destrucción de la información	1	1%		
Archivo de datos	[E.19] Fugas de información	1			10%
Archivo de datos	[A.5] Suplantación de la identidad	10		10%	50%
Archivo de datos	[A.6] Abuso de privilegios de acceso	10	1%	10%	50%
Archivo de datos	[A.11] Acceso no autorizado	100		10%	50%
DOCUMENTACIÓN INTERNA					
Documentación interna	[E.15] Alteración de la información	1		1%	
Documentación interna	[E.18] Destrucción de la información	1	1%		
Documentación interna	[E.19] Fugas de información	1			10%

Documentación interna	[A.5] Suplantación de la identidad	10		10%	50%
Documentación interna	[A.6] Abuso de privilegios de acceso	10	1%	10%	50%
Documentación interna	[A.11] Acceso no autorizado	100		10%	50%
	MATERIAL IMPRESO				
Material impreso	[N.1] Fuego	0,10	100 %		
Material impreso	[N.2] Daños por agua	0,10	50%		
Material impreso	[N.*] Desastres naturales	0,10	100 %		
Material impreso	[I.1] Fuego	1	100 %		
Material impreso	[I.2] Daños por agua	1	50%		
Material impreso	[I.*] Desastres industriales	1	100 %		
Material impreso	[I.3] Contaminación medioambiental	1	50%		
Material impreso	[I.7] Condiciones inadecuadas de temperatura o humedad	1	100 %		
Material impreso	[E.1] Errores de los usuarios	1	1%	5%	10%
Material impreso	[E.15] Alteración de la información	1		1%	
Material impreso	[E.18] Destrucción de la información	1	100 %		
Material impreso	[E.19] Fugas de información	1			10%
Material impreso	[A.7] Uso no previsto	1	1%		1%
Material impreso	[A.11] Acceso no autorizado	1		1%	50%
Material impreso	[A.15] Modificación de la información	10		100 %	
Material impreso	[A.18] Destrucción de la información	1	100 %		
Material impreso	[A.26] Ataques destructivos	1	10%		
	CARPETAS COMPARTIDAS				
Carpetas compartidas	[E.15] Alteración de la información	1		1%	
Carpetas compartidas	[E.18] Destrucción de la información	1	1%		
Carpetas compartidas	[E.19] Fugas de información	1			10%

Carpetas compartidas	[A.5] Suplantación de la identidad	10		10%	50%
Carpetas compartidas	[A.6] Abuso de privilegios de acceso	10	1%	10%	50%
Carpetas compartidas	[A.11] Acceso no autorizado	100		10%	50%
APLICACIONES					
MOTOR DE BASE DE DATOS					
Motor de base de datos	[I.5.1] Avería de origen lógico	1	50%		
Motor de base de datos	[E.8] Difusión de software dañino	1	10%	10%	10%
Motor de base de datos	[E.20]Vulnerabilidades de los programas (software)	1	1%	20%	20%
Motor de base de datos	[E.21] Errores de mantenimiento/actualización de programas (software)	10	1%	10%	50%
Motor de base de datos	[A.8] Difusión de software dañino	1	100 %	100 %	100 %
Motor de base de datos	[A.22] Manipulación de programas	1	50%	100 %	100 %
REPOSITORIO DE APLICACIONES DESARROLLADAS					
Repositorio de aplicación desarrolladas	[I.5.1] Avería de origen lógico	1	50%		
Repositorio de aplicación desarrolladas	[E.8] Difusión de software dañino	1	10%	10%	10%
Repositorio de aplicación desarrolladas	[E.20]Vulnerabilidades de los programas (software)	1	1%	20%	20%
Repositorio de aplicación desarrolladas	[E.21] Errores de mantenimiento/actualización de programas (software)	10	1%	10%	50%
Repositorio de aplicación desarrolladas	[A.8] Difusión de software dañino	1	100 %	100 %	100 %
Repositorio de aplicación desarrolladas	[A.22] Manipulación de programas	1	50%	100 %	100 %
ANTIVIRUS					
Antivirus	[I.5.1] Avería de origen lógico	1	50%		
Antivirus	[E.8] Difusión de software dañino	1	10%	10%	10%
Antivirus	[E.20]Vulnerabilidades de los programas (software)	1	1%	20%	20%
Antivirus	[E.21] Errores de mantenimiento/actualización de programas (software)	10	1%	10%	50%

Antivirus	[A.8] Difusión de software dañino	1	100 %	100 %	100 %
Antivirus	[A.22] Manipulación de programas	1	50%	100 %	100 %
	FIREWALL				
Firewall	[I.5.1] Avería de origen lógico	1	50%		
Firewall	[E.4] Errores de configuración	1		1%	
Firewall	[E.8] Difusión de software dañino	1	10%	10%	10%
Firewall	[E.18] Destrucción de la información	1	1%		
Firewall	[E.20]Vulnerabilidades de los programas (software)	1	1%	20%	20%
Firewall	[E.21] Errores de mantenimiento/actualización de programas (software)	10	1%	10%	50%
Firewall	[A.4] Manipulación de los ficheros de configuración	10	10%	10%	10%
Firewall	[A.5] Suplantación de la identidad	10		10%	50%
Firewall	[A.8] Difusión de software dañino	1	100 %	100 %	100 %
Firewall	[A.22] Manipulación de programas	1	50%	100 %	100 %
	LICENCIAS				
Licencias	[I.5.1] Avería de origen lógico	1	50%		
Licencias	[E.8] Difusión de software dañino	1	10%	10%	10%
Licencias	[E.20]Vulnerabilidades de los programas (software)	1	1%	20%	20%
Licencias	[E.21] Errores de mantenimiento/actualización de programas (software)	10	1%	10%	50%
Licencias	[A.8] Difusión de software dañino	1	100 %	100 %	100 %
Licencias	[A.22] Manipulación de programas	1	50%	100 %	100 %
	NAVEGADORES				
Navegadores	[I.5.1] Avería de origen lógico	1	50%		
Navegadores	[E.8] Difusión de software dañino	1	10%	10%	10%
Navegadores	[E.20]Vulnerabilidades de los programas (software)	1	1%	20%	20%
Navegadores	[E.21] Errores de mantenimiento/actualización de programas (software)	10	1%	10%	50%
Navegadores	[A.8] Difusión de software dañino	1	100 %	100 %	100 %
Navegadores	[A.22] Manipulación de programas	1	50%	100 %	100 %
	SISTEMAS OPERATIVOS				

Sistemas operativos	[I.5.1] Avería de origen lógico	1	50%		
Sistemas operativos	[E.8] Difusión de software dañino	1	10%	10%	10%
Sistemas operativos	[E.20]Vulnerabilidades de los programas (software)	1	1%	20%	20%
Sistemas operativos	[E.21] Errores de mantenimiento/actualización de programas (software)	10	1%	10%	50%
Sistemas operativos	[A.8] Difusión de software dañino	1	100 %	100 %	100 %
Sistemas operativos	[A.22] Manipulación de programas	1	50%	100 %	100 %
EQUIPOS					
DISPOSITIVOS DE ALMACENAMIENTO					
Dispositivos de almacenamiento	[N.1] Fuego	0,10	100 %		
Dispositivos de almacenamiento	[N.2] Daños por agua	0,10	50%		
Dispositivos de almacenamiento	[N.*] Desastres naturales	0,10	100 %		
Dispositivos de almacenamiento	[I.1] Fuego	1	100 %		
Dispositivos de almacenamiento	[I.2] Daños por agua	1	50%		
Dispositivos de almacenamiento	[I.*] Desastres industriales	1	100 %		
Dispositivos de almacenamiento	[I.3] Contaminación medioambiental	0,10	50%		
Dispositivos de almacenamiento	[I.4] Contaminación electromagnética	M	10%		
Dispositivos de almacenamiento	[I.5.2] Avería de origen físico	M	50%		
Dispositivos de almacenamiento	[I.6] Corte del suministro eléctrico	M	100 %		
Dispositivos de almacenamiento	[I.7] Condiciones inadecuadas de temperatura o humedad	M	100 %		

Dispositivos de almacenamiento	[I.11] Emanaciones electromagnéticas (TEMPEST)	M			1%
Dispositivos de almacenamiento	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	M	10%		
Dispositivos de almacenamiento	[E.24] Caída del sistema por agotamiento de recursos	A	50%		
Dispositivos de almacenamiento	[E.25] Pérdida de equipos	M	100 %		50%
Dispositivos de almacenamiento	[A.11] Acceso no autorizado	M	10%	10%	50%
Dispositivos de almacenamiento	[A.23] Manipulación de hardware	M	50%		50%
Dispositivos de almacenamiento	[A.24] Denegación de servicio	M	100 %		
Dispositivos de almacenamiento	[A.25] Robo de equipos	M	100 %		50%
Dispositivos de almacenamiento	[A.26] Ataques destructivos	M	100 %		
	COMPUTADORAS				
Computadoras	[N.1] Fuego	0,10	100 %		
Computadoras	[N.2] Daños por agua	0,10	50%		
Computadoras	[N.*] Desastres naturales	0,10	100 %		
Computadoras	[I.1] Fuego	1	100 %		
Computadoras	[I.2] Daños por agua	1	50%		
Computadoras	[I.*] Desastres industriales	1	100 %		
Computadoras	[I.3] Contaminación medioambiental	0,10	50%		
Computadoras	[I.4] Contaminación electromagnética	1	10%		
Computadoras	[I.5.2] Avería de origen físico	1	50%		
Computadoras	[I.6] Corte del suministro eléctrico	1	100 %		
Computadoras	[I.7] Condiciones inadecuadas de temperatura o humedad	1	100 %		
Computadoras	[I.11] Emanaciones electromagnéticas (TEMPEST)	1			1%

Computadoras	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	1	10%		
Computadoras	[E.24] Caída del sistema por agotamiento de recursos	10	50%		
Computadoras	[E.25] Pérdida de equipos	1	100 %		50%
Computadoras	[A.11] Acceso no autorizado	1	10%	10%	50%
Computadoras	[A.23] Manipulación de hardware	1	50%		50%
Computadoras	[A.24] Denegación de servicio	1	100 %		
Computadoras	[A.25] Robo de equipos	1	100 %		50%
Computadoras	[A.26] Ataques destructivos	1	100 %		
	TELÉFONOS IP				
Teléfonos IP	[N.1] Fuego	0,10	100 %		
Teléfonos IP	[N.2] Daños por agua	0,10	50%		
Teléfonos IP	[N.*] Desastres naturales	0,10	100 %		
Teléfonos IP	[I.1] Fuego	1	100 %		
Teléfonos IP	[I.2] Daños por agua	1	50%		
Teléfonos IP	[I.*] Desastres industriales	1	100 %		
Teléfonos IP	[I.3] Contaminación medioambiental	0,10	50%		
Teléfonos IP	[I.4] Contaminación electromagnética	1	10%		
Teléfonos IP	[I.5.2] Avería de origen físico	1	50%		
Teléfonos IP	[I.6] Corte del suministro eléctrico	1	100 %		
Teléfonos IP	[I.7] Condiciones inadecuadas de temperatura o humedad	1	100 %		
Teléfonos IP	[I.11] Emanaciones electromagnéticas (TEMPEST)	1			1%
Teléfonos IP	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	1	10%		
Teléfonos IP	[E.24] Caída del sistema por agotamiento de recursos	10	50%		
Teléfonos IP	[E.25] Pérdida de equipos	1	100 %		50%
Teléfonos IP	[A.11] Acceso no autorizado	1	10%	10%	50%
Teléfonos IP	[A.23] Manipulación de hardware	1	50%		50%
Teléfonos IP	[A.24] Denegación de servicio	1	100 %		
Teléfonos IP	[A.25] Robo de equipos	1	100 %		50%

Teléfonos IP	[A.26] Ataques destructivos	1	100 %		
SERVIDORES					
Servidores	[N.1] Fuego	0,10	100 %		
Servidores	[N.2] Daños por agua	0,10	50%		
Servidores	[N.*] Desastres naturales	0,10	100 %		
Servidores	[I.1] Fuego	1	100 %		
Servidores	[I.2] Daños por agua	1	50%		
Servidores	[I.*] Desastres industriales	1	100 %		
Servidores	[I.3] Contaminación medioambiental	0,10	50%		
Servidores	[I.4] Contaminación electromagnética	1	10%		
Servidores	[I.5.2] Avería de origen físico	1	50%		
Servidores	[I.6] Corte del suministro eléctrico	1	100 %		
Servidores	[I.7] Condiciones inadecuadas de temperatura o humedad	1	100 %		
Servidores	[I.11] Emanaciones electromagnéticas (TEMPEST)	1			1%
Servidores	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	1	10%		
Servidores	[E.24] Caída del sistema por agotamiento de recursos	10	50%		
Servidores	[E.25] Pérdida de equipos	1	100 %		50%
Servidores	[A.11] Acceso no autorizado	1	10%	10%	50%
Servidores	[A.23] Manipulación de hardware	1	50%		50%
Servidores	[A.24] Denegación de servicio	1	100 %		
Servidores	[A.25] Robo de equipos	1	100 %		50%
Servidores	[A.26] Ataques destructivos	1	100 %		
EQUIPO PARA EL FUNCIONAMIENTO DE RED					
Equipo para el funcionamiento de red	[N.1] Fuego	0,10	100 %		
Equipo para el funcionamiento de red	[N.2] Daños por agua	0,10	50%		
Equipo para el funcionamiento de red	[N.*] Desastres naturales	0,10	100 %		

Equipo para el funcionamiento de red	[I.1] Fuego	1	100 %		
Equipo para el funcionamiento de red	[I.2] Daños por agua	1	50%		
Equipo para el funcionamiento de red	[I.*] Desastres industriales	1	100 %		
Equipo para el funcionamiento de red	[I.3] Contaminación medioambiental	0,10	50%		
Equipo para el funcionamiento de red	[I.4] Contaminación electromagnética	1	10%		
Equipo para el funcionamiento de red	[I.5.2] Avería de origen físico	1	50%		
Equipo para el funcionamiento de red	[I.6] Corte del suministro eléctrico	1	100 %		
Equipo para el funcionamiento de red	[I.7] Condiciones inadecuadas de temperatura o humedad	1	100 %		
Equipo para el funcionamiento de red	[I.11] Emanaciones electromagnéticas (TEMPEST)	1			1%
Equipo para el funcionamiento de red	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	1	10%		
Equipo para el funcionamiento de red	[E.24] Caída del sistema por agotamiento de recursos	10	50%		
Equipo para el funcionamiento de red	[E.25] Pérdida de equipos	1	100 %		50%
Equipo para el funcionamiento de red	[A.11] Acceso no autorizado	1	10%	10%	50%
Equipo para el funcionamiento de red	[A.23] Manipulación de hardware	1	50%		50%
Equipo para el funcionamiento de red	[A.24] Denegación de servicio	1	100 %		
Equipo para el funcionamiento de red	[A.25] Robo de equipos	1	100 %		50%

Equipo para el funcionamiento de red	[A.26] Ataques destructivos	1	100 %		
EQUIPO MULTIFUNCIONAL					
Equipo multifuncional	[N.1] Fuego	0,10	100 %		
Equipo multifuncional	[N.2] Daños por agua	0,10	50%		
Equipo multifuncional	[N.*] Desastres naturales	0,10	100 %		
Equipo multifuncional	[I.1] Fuego	1	100 %		
Equipo multifuncional	[I.2] Daños por agua	1	50%		
Equipo multifuncional	[I.*] Desastres industriales	1	100 %		
Equipo multifuncional	[I.3] Contaminación medioambiental	0,10	50%		
Equipo multifuncional	[I.4] Contaminación electromagnética	1	10%		
Equipo multifuncional	[I.5.2] Avería de origen físico	1	50%		
Equipo multifuncional	[I.6] Corte del suministro eléctrico	1	100 %		
Equipo multifuncional	[I.7] Condiciones inadecuadas de temperatura o humedad	1	100 %		
Equipo multifuncional	[I.11] Emanaciones electromagnéticas (TEMPEST)	1			1%
Equipo multifuncional	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	1	10%		
Equipo multifuncional	[E.24] Caída del sistema por agotamiento de recursos	10	50%		
Equipo multifuncional	[E.25] Pérdida de equipos	1	100 %		50%
Equipo multifuncional	[A.11] Acceso no autorizado	1	10%	10%	50%
Equipo multifuncional	[A.23] Manipulación de hardware	1	50%		50%
Equipo multifuncional	[A.24] Denegación de servicio	1	100 %		
Equipo multifuncional	[A.25] Robo de equipos	1	100 %		50%
Equipo multifuncional	[A.26] Ataques destructivos	1	100 %		
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA					
Dispositivo de grabación y fotografía	[N.1] Fuego	0,10	100 %		

Dispositivo de grabación y fotografía	[N.2] Daños por agua	0,10	50%		
Dispositivo de grabación y fotografía	[N.*] Desastres naturales	0,10	100 %		
Dispositivo de grabación y fotografía	[I.1] Fuego	1	100 %		
Dispositivo de grabación y fotografía	[I.2] Daños por agua	1	50%		
Dispositivo de grabación y fotografía	[I.*] Desastres industriales	1	100 %		
Dispositivo de grabación y fotografía	[I.3] Contaminación medioambiental	0,10	50%		
Dispositivo de grabación y fotografía	[I.4] Contaminación electromagnética	1	10%		
Dispositivo de grabación y fotografía	[I.5.2] Avería de origen físico	1	50%		
Dispositivo de grabación y fotografía	[I.6] Corte del suministro eléctrico	1	100 %		
Dispositivo de grabación y fotografía	[I.7] Condiciones inadecuadas de temperatura o humedad	1	100 %		
Dispositivo de grabación y fotografía	[I.11] Emanaciones electromagnéticas (TEMPEST)	1			1%
Dispositivo de grabación y fotografía	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	1	10%		
Dispositivo de grabación y fotografía	[E.24] Caída del sistema por agotamiento de recursos	10	50%		
Dispositivo de grabación y fotografía	[E.25] Pérdida de equipos	1	100 %		50%
Dispositivo de grabación y fotografía	[A.11] Acceso no autorizado	1	10%	10%	50%
Dispositivo de grabación y fotografía	[A.23] Manipulación de hardware	1	50%		50%

Dispositivo de grabación y fotografía	[A.24] Denegación de servicio	1	100 %		
Dispositivo de grabación y fotografía	[A.25] Robo de equipos	1	100 %		50%
Dispositivo de grabación y fotografía	[A.26] Ataques destructivos	1	100 %		
RADIOS DE COMUNICACIÓN					
Radios de comunicación	[N.1] Fuego	0,10	100 %		
Radios de comunicación	[N.2] Daños por agua	0,10	50%		
Radios de comunicación	[N.*] Desastres naturales	0,10	100 %		
Radios de comunicación	[I.1] Fuego	1	100 %		
Radios de comunicación	[I.2] Daños por agua	1	50%		
Radios de comunicación	[I.*] Desastres industriales	1	100 %		
Radios de comunicación	[I.3] Contaminación medioambiental	0,10	50%		
Radios de comunicación	[I.4] Contaminación electromagnética	1	10%		
Radios de comunicación	[I.5.2] Avería de origen físico	1	50%		
Radios de comunicación	[I.6] Corte del suministro eléctrico	1	100 %		
Radios de comunicación	[I.7] Condiciones inadecuadas de temperatura o humedad	1	100 %		
Radios de comunicación	[I.11] Emanaciones electromagnéticas (TEMPEST)	1			1%
Radios de comunicación	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	1	10%		
Radios de comunicación	[E.24] Caída del sistema por agotamiento de recursos	10	50%		
Radios de comunicación	[E.25] Pérdida de equipos	1	100 %		50%
Radios de comunicación	[A.11] Acceso no autorizado	1	10%	10%	50%
Radios de comunicación	[A.23] Manipulación de hardware	1	50%		50%
Radios de comunicación	[A.24] Denegación de servicio	1	100 %		
Radios de comunicación	[A.25] Robo de equipos	1	100 %		50%

Radios de comunicación	[A.26] Ataques destructivos	1	100 %		
COMUNICACIÓN					
ETHERNET					
Ethernet	[I.8] Fallo de servicios de comunicación	1	50%		
Ethernet	[E.2] Errores del administrador del sistema	1	20%	20%	20%
Ethernet	[E.9] Errores de [re-]encaminamiento	1			10%
Ethernet	[E.10] Errores de secuencia	1		10%	
Ethernet	[E.15] Alteración de la información	1		1%	
Ethernet	[E.19] Fugas de información	1			10%
Ethernet	[E.24] Caída del sistema por agotamiento de recursos	1	50%		
Ethernet	[A.5] Suplantación de la identidad	1		10%	50%
Ethernet	[A.7] Uso no previsto	1	10%	10%	10%
Ethernet	[A.9] [Re-]encaminamiento de mensajes	1			10%
Ethernet	[A.10] Alteración de secuencia	1		10%	
Ethernet	[A.11] Acceso no autorizado	1		10%	50%
Ethernet	[A.12] Análisis de tráfico	1			2%
Ethernet	[A.14] Interceptación de información (escucha)	1			10%
Ethernet	[A.15] Modificación de la información	1		10%	
Ethernet	[A.18] Destrucción de la información	1	50%		
Ethernet	[A.24] Denegación de servicio	10	50%		
RED INALAMBRICA					
Red inalámbrica	[I.8] Fallo de servicios de comunicación	1	50%		
Red inalámbrica	[E.2] Errores del administrador del sistema	1	20%	20%	20%
Red inalámbrica	[E.9] Errores de [re-]encaminamiento	1			10%
Red inalámbrica	[E.10] Errores de secuencia	1		10%	
Red inalámbrica	[E.15] Alteración de la información	1		1%	
Red inalámbrica	[E.19] Fugas de información	1			10%
Red inalámbrica	[E.24] Caída del sistema por agotamiento de recursos	1	50%		
Red inalámbrica	[A.5] Suplantación de la identidad	1		10%	50%
Red inalámbrica	[A.7] Uso no previsto	1	10%	10%	10%
Red inalámbrica	[A.9] [Re-]encaminamiento de mensajes	1			10%
Red inalámbrica	[A.10] Alteración de secuencia	1		10%	
Red inalámbrica	[A.11] Acceso no autorizado	1		10%	50%
Red inalámbrica	[A.12] Análisis de tráfico	1			2%

Red inalámbrica	[A.14] Interceptación de información (escucha)	1			10%
Red inalámbrica	[A.15] Modificación de la información	1		10%	
Red inalámbrica	[A.18] Destrucción de la información	1	50%		
Red inalámbrica	[A.24] Denegación de servicio	10	50%		
	RED LAN				
Red LAN	[I.8] Fallo de servicios de comunicación	1	50%		
Red LAN	[E.2] Errores del administrador del sistema	1	20%	20%	20%
Red LAN	[E.9] Errores de [re-]encaminamiento	1			10%
Red LAN	[E.10] Errores de secuencia	1		10%	
Red LAN	[E.15] Alteración de la información	1		1%	
Red LAN	[E.19] Fugas de información	1			10%
Red LAN	[E.24] Caída del sistema por agotamiento de recursos	1	50%		
Red LAN	[A.5] Suplantación de la identidad	1		10%	50%
Red LAN	[A.7] Uso no previsto	1	10%	10%	10%
Red LAN	[A.9] [Re-]encaminamiento de mensajes	1			10%
Red LAN	[A.10] Alteración de secuencia	1		10%	
Red LAN	[A.11] Acceso no autorizado	1		10%	50%
Red LAN	[A.12] Análisis de tráfico	1			2%
Red LAN	[A.14] Interceptación de información (escucha)	1			10%
Red LAN	[A.15] Modificación de la información	1		10%	
Red LAN	[A.18] Destrucción de la información	1	50%		
Red LAN	[A.24] Denegación de servicio	10	50%		
	RED TELEFÓNICA				
Red telefónica	[I.8] Fallo de servicios de comunicación	1	50%		
Red telefónica	[E.2] Errores del administrador del sistema	1	20%	20%	20%
Red telefónica	[E.9] Errores de [re-]encaminamiento	1			10%
Red telefónica	[E.10] Errores de secuencia	1		10%	
Red telefónica	[E.15] Alteración de la información	1		1%	
Red telefónica	[E.19] Fugas de información	1			10%
Red telefónica	[E.24] Caída del sistema por agotamiento de recursos	1	50%		
Red telefónica	[A.5] Suplantación de la identidad	1		10%	50%
Red telefónica	[A.7] Uso no previsto	1	10%	10%	10%
Red telefónica	[A.9] [Re-]encaminamiento de mensajes	1			10%
Red telefónica	[A.10] Alteración de secuencia	1		10%	
Red telefónica	[A.11] Acceso no autorizado	1		10%	50%

Red telefónica	[A.12] Análisis de tráfico	1			2%
Red telefónica	[A.14] Interceptación de información (escucha)	1			10%
Red telefónica	[A.15] Modificación de la información	1		10%	
Red telefónica	[A.18] Destrucción de la información	1	50%		
Red telefónica	[A.24] Denegación de servicio	10	50%		
	ELEMENTOS AUXILIARES				
	UPS				
UPS	[N.1] Fuego	0,10	100 %		
UPS	[N.2] Daños por agua	0,10	50%		
UPS	[N.*] Desastres naturales	0,10	100 %		
UPS	[I.1] Fuego	1	100 %		
UPS	[I.2] Daños por agua	1	50%		
UPS	[I.*] Desastres industriales	1	100 %		
UPS	[I.3] Contaminación medioambiental	0,10	50%		
UPS	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	1	10%		
UPS	[A.7] Uso no previsto	1	50%	1%	1%
UPS	[A.23] Manipulación de hardware	1	50%		50%
UPS	[A.25] Robo de equipos	1	10%		
UPS	[A.26] Ataques destructivos	1	10%		
	GENERADOR ELÉCTRICO				
Generador eléctrico	[N.1] Fuego	0,10	100 %		
Generador eléctrico	[N.2] Daños por agua	0,10	50%		
Generador eléctrico	[N.*] Desastres naturales	0,10	100 %		
Generador eléctrico	[I.1] Fuego	1	100 %		
Generador eléctrico	[I.2] Daños por agua	1	50%		
Generador eléctrico	[I.*] Desastres industriales	1	100 %		
Generador eléctrico	[I.3] Contaminación medioambiental	0,10	50%		
Generador eléctrico	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	1	10%		
Generador eléctrico	[A.7] Uso no previsto	1	50%	1%	1%

Generador eléctrico	[A.23] Manipulación de hardware	1	50%		50%
Generador eléctrico	[A.25] Robo de equipos	1	10%		
Generador eléctrico	[A.26] Ataques destructivos	1	10%		
EQUIPOS DE CLIMATIZACIÓN					
Equipos de climatización	[N.1] Fuego	0,10	100 %		
Equipos de climatización	[N.2] Daños por agua	0,10	50%		
Equipos de climatización	[N.*] Desastres naturales	0,10	100 %		
Equipos de climatización	[I.1] Fuego	1	100 %		
Equipos de climatización	[I.2] Daños por agua	1	50%		
Equipos de climatización	[I.*] Desastres industriales	1	100 %		
Equipos de climatización	[I.3] Contaminación medioambiental	0,10	50%		
Equipos de climatización	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	1	10%		
Equipos de climatización	[A.7] Uso no previsto	1	50%	1%	1%
Equipos de climatización	[A.23] Manipulación de hardware	1	50%		50%
Equipos de climatización	[A.25] Robo de equipos	1	10%		
Equipos de climatización	[A.26] Ataques destructivos	1	10%		
MOBILIARIO					
Mobiliario	[N.1] Fuego	0,10	100 %		
Mobiliario	[N.2] Daños por agua	0,10	50%		
Mobiliario	[N.*] Desastres naturales	0,10	100 %		
Mobiliario	[I.1] Fuego	1	100 %		
Mobiliario	[I.2] Daños por agua	1	50%		
Mobiliario	[I.*] Desastres industriales	1	100 %		
Mobiliario	[I.3] Contaminación medioambiental	0,10	50%		
Mobiliario	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	1	10%		
Mobiliario	[A.7] Uso no previsto	1	50%	1%	1%

Mobiliario	[A.23] Manipulación de hardware	1	50%		50%
Mobiliario	[A.25] Robo de equipos	1	10%		
Mobiliario	[A.26] Ataques destructivos	1	10%		
	SERVICIOS				
	TELEFONÍA				
Telefonía	[E.15] Alteración de la información	1		10%	
Telefonía	[E.18] Destrucción de la información	1	10%		
Telefonía	[E.19] Fugas de información	1			10%
Telefonía	[A.15] Modificación de la información	1		50%	
Telefonía	[A.18] Destrucción de la información	1	50%		
Telefonía	[A.24] Denegación de servicio	1	50%		
	INTERNET				
Internet	[E.15] Alteración de la información	1		10%	
Internet	[E.18] Destrucción de la información	1	10%		
Internet	[E.19] Fugas de información	1			10%
Internet	[A.5] Suplantación de la identidad	0,1		100 %	100 %
Internet	[A.15] Modificación de la información	1		50%	
Internet	[A.18] Destrucción de la información	1	50%		
Internet	[A.24] Denegación de servicio	1	50%		
	ELECTRICIDAD				
Electricidad	[I.9] Interrupción de otros servicios o suministros esenciales	1	50%		
Electricidad	[E.15] Alteración de la información	1		10%	
Electricidad	[E.18] Destrucción de la información	1	10%		
	CORREO INSTITUCIONAL				
Correo institucional	[E.1] Errores de los usuarios	1	10%	10%	10%
Correo institucional	[E.2] Errores del administrador del sistema	1	20%	20%	20%
Correo institucional	[E.15] Alteración de la información	1		1%	
Correo institucional	[E.18] Destrucción de la información	1	10%		
Correo institucional	[E.19] Fugas de información	1			10%
Correo institucional	[E.24] Caída del sistema por agotamiento de recursos	10	50%		
Correo institucional	[A.5] Suplantación de la identidad	1		50%	50%
Correo institucional	[A.6] Abuso de privilegios de acceso	1	1%	10%	10%
Correo institucional	[A.7] Uso no previsto	1	1%	10%	10%
Correo institucional	[A.11] Acceso no autorizado	1		10%	50%

Correo institucional	[A.15] Modificación de la información	10		50%	
Correo institucional	[A.18] Destrucción de la información	1	50%		
Correo institucional	[A.24] Denegación de servicio	10	50%		
SOPORTE DE RED					
Soporte de red	[E.1] Errores de los usuarios	1	1%	5%	10%
Soporte de red	[E.15] Alteración de la información	1		1%	
Soporte de red	[E.18] Destrucción de la información	1	100 %		
Soporte de red	[E.19] Fugas de información	1			10%
Soporte de red	[A.7] Uso no previsto	1	1%		1%
Soporte de red	[A.11] Acceso no autorizado	1		1%	50%
Soporte de red	[A.15] Modificación de la información	10		100 %	
Soporte de red	[A.18] Destrucción de la información	1	100 %		
SOPORTE A LOS SERVICIOS INFORMÁTICOS					
Soporte a los servicios informáticos	[E.1] Errores de los usuarios	1	10%	10%	10%
Soporte a los servicios informáticos	[E.2] Errores del administrador del sistema	1	20%	20%	20%
Soporte a los servicios informáticos	[E.15] Alteración de la información	1		1%	
Soporte a los servicios informáticos	[E.18] Destrucción de la información	1	10%		
Soporte a los servicios informáticos	[E.19] Fugas de información	1			10%
Soporte a los servicios informáticos	[E.24] Caída del sistema por agotamiento de recursos	10	50%		
Soporte a los servicios informáticos	[A.5] Suplantación de la identidad	1		50%	50%
Soporte a los servicios informáticos	[A.6] Abuso de privilegios de acceso	1	1%	10%	10%
Soporte a los servicios informáticos	[A.7] Uso no previsto	1	1%	10%	10%
Soporte a los servicios informáticos	[A.11] Acceso no autorizado	1		10%	50%

Soporte a los servicios informáticos	[A.15] Modificación de la información	10		50%	
Soporte a los servicios informáticos	[A.18] Destrucción de la información	1	50%		
Soporte a los servicios informáticos	[A.24] Denegación de servicio	10	50%		
MANTENIMIENTO DE EQUIPOS					
Mantenimiento de equipos	[I.9] Interrupción de otros servicios o suministros esenciales	1	50%		
Mantenimiento de equipos	[E.15] Alteración de la información	1		10%	
Mantenimiento de equipos	[E.18] Destrucción de la información	1	10%		
Mantenimiento de equipos	[E.19] Fugas de información	1			10%
Mantenimiento de equipos	[A.5] Suplantación de la identidad	0,1		100 %	100 %
Mantenimiento de equipos	[A.15] Modificación de la información	1		50%	
Mantenimiento de equipos	[A.18] Destrucción de la información	1	50%		
Mantenimiento de equipos	[A.19] Revelación de información	1			50%
Mantenimiento de equipos	[A.24] Denegación de servicio	1	50%		
INFRAESTRUCTURA					
INSTALACIÓN DE RED DE DATOS					
Instalación de red de datos	[N.1] Fuego	1	100 %		
Instalación de red de datos	[N.2] Daños por agua	1	100 %		
Instalación de red de datos	[N.*] Desastres naturales	1	100 %		
Instalación de red de datos	[I.1] Fuego	1	100 %		
Instalación de red de datos	[I.2] Daños por agua	1	100 %		
Instalación de red de datos	[I.*] Desastres industriales	1	100 %		
Instalación de red de datos	[I.3] Contaminación medioambiental	1	10%		
Instalación de red de datos	[I.4] Contaminación electromagnética	0,10	10%		
Instalación de red de datos	[E.25] Pérdida de equipos	10			10%

Instalación de red de datos	[A.6] Abuso de privilegios de acceso	1	10%	
Instalación de red de datos	[A.7] Uso no previsto	1	10%	
Instalación de red de datos	[A.25] Robo de equipos	10		100 %
Instalación de red de datos	[A.26] Ataques destructivos	0,10	100 %	
Instalación de red de datos	[A.27] Ocupación enemiga	1	100 %	
INSTALACIÓN DE RED ELÉCTRICA				
Instalación de red eléctrica	[N.1] Fuego	1	100 %	
Instalación de red eléctrica	[N.2] Daños por agua	1	100 %	
Instalación de red eléctrica	[N.*] Desastres naturales	1	100 %	
Instalación de red eléctrica	[I.1] Fuego	1	100 %	
Instalación de red eléctrica	[I.2] Daños por agua	1	100 %	
Instalación de red eléctrica	[I.*] Desastres industriales	1	100 %	
Instalación de red eléctrica	[I.3] Contaminación medioambiental	1	10%	
Instalación de red eléctrica	[I.4] Contaminación electromagnética	0,10	10%	
Instalación de red eléctrica	[E.25] Pérdida de equipos	10		10%
Instalación de red eléctrica	[A.6] Abuso de privilegios de acceso	1	10%	
Instalación de red eléctrica	[A.7] Uso no previsto	1	10%	
Instalación de red eléctrica	[A.25] Robo de equipos	10		100 %
Instalación de red eléctrica	[A.26] Ataques destructivos	0,10	100 %	
Instalación de red eléctrica	[A.27] Ocupación enemiga	1	100 %	
UPS DEL CENTRO CABLEADO				
UPS del centro cableado	[N.1] Fuego	1	100 %	
UPS del centro cableado	[N.2] Daños por agua	1	100 %	
UPS del centro cableado	[N.*] Desastres naturales	1	100 %	
UPS del centro cableado	[I.1] Fuego	1	100 %	

UPS del centro cableado	[I.2] Daños por agua	1	100 %	
UPS del centro cableado	[I.*] Desastres industriales	1	100 %	
UPS del centro cableado	[I.3] Contaminación medioambiental	1	10%	
UPS del centro cableado	[I.4] Contaminación electromagnética	0,10	10%	
UPS del centro cableado	[E.25] Pérdida de equipos	10		10%
UPS del centro cableado	[A.6] Abuso de privilegios de acceso	1	10%	
UPS del centro cableado	[A.7] Uso no previsto	1	10%	
UPS del centro cableado	[A.25] Robo de equipos	10		100 %
UPS del centro cableado	[A.26] Ataques destructivos	0,10	100 %	
UPS del centro cableado	[A.27] Ocupación enemiga	1	100 %	
	ESPACIO FÍSICO DDTI			
Espacio físico DDTI	[N.1] Fuego	1	100 %	
Espacio físico DDTI	[N.2] Daños por agua	1	100 %	
Espacio físico DDTI	[N.*] Desastres naturales	1	100 %	
Espacio físico DDTI	[I.1] Fuego	1	100 %	
Espacio físico DDTI	[I.2] Daños por agua	1	100 %	
Espacio físico DDTI	[I.*] Desastres industriales	1	100 %	
Espacio físico DDTI	[I.3] Contaminación medioambiental	1	10%	
Espacio físico DDTI	[I.4] Contaminación electromagnética	0,10	10%	
Espacio físico DDTI	[E.25] Pérdida de equipos	10		10%
Espacio físico DDTI	[A.6] Abuso de privilegios de acceso	1	10%	
Espacio físico DDTI	[A.7] Uso no previsto	1	10%	
Espacio físico DDTI	[A.25] Robo de equipos	10		100 %
Espacio físico DDTI	[A.26] Ataques destructivos	0,10	100 %	
Espacio físico DDTI	[A.27] Ocupación enemiga	1	100 %	

PERSONAL					
PERSONAL ADMINISTRATIVO					
Personal Administrativo	[E.15] Alteración de la información	1		10%	
Personal Administrativo	[E.18] Destrucción de la información	1	1%		
Personal Administrativo	[E.19] Fugas de información	1			10%
Personal Administrativo	[A.15] Modificación de la información	1		50%	
Personal Administrativo	[A.18] Destrucción de la información	1	1%		
Personal Administrativo	[A.19] Revelación de información	1			50%
Personal Administrativo	[A.28] Indisponibilidad del personal	1	10%		
Personal Administrativo	[A.29] Extorsión	1	10%	10%	50%
Personal Administrativo	[A.30] Ingeniería social (picaresca)	1	10%	10%	50%
PERSONAL DE DESARROLLO					
Personal de desarrollo	[E.15] Alteración de la información	1		10%	
Personal de desarrollo	[E.18] Destrucción de la información	1	1%		
Personal de desarrollo	[E.19] Fugas de información	1			10%
Personal de desarrollo	[A.15] Modificación de la información	1		50%	
Personal de desarrollo	[A.18] Destrucción de la información	1	1%		
Personal de desarrollo	[A.19] Revelación de información	1			50%
Personal de desarrollo	[A.28] Indisponibilidad del personal	1	10%		
Personal de desarrollo	[A.29] Extorsión	1	10%	10%	50%
Personal de desarrollo	[A.30] Ingeniería social (picaresca)	1	10%	10%	50%

Nota: Elaboración propia

Anexo 5: Impacto potencial acumulado de afectación de activos del DDTI-UTN

	IMPACTO POTENCIAL ACUMULADO			PESO PONDERADO
ACTIVO	**D**	**I**	**C**	
INFORMACIÓN	10	10	9	
BASE DE DATOS	4	7	9	
[E.15] Alteración de la información		4		4
[E.18] Destrucción de la información	4			4
[E.19] Fugas de información			7	7
[A.5] Suplantación de la identidad		7	9	8
[A.6] Abuso de privilegios de acceso	4	7	9	6,7
[A.11] Acceso no autorizado		7	9	8
ARCHIVO DE DATOS	4	7	9	6,7
[E.15] Alteración de la información		4		4
[E.18] Destrucción de la información	4			4
[E.19] Fugas de información			7	7
[A.5] Suplantación de la identidad		7	9	8
[A.6] Abuso de privilegios de acceso	4	7	9	6,7
[A.11] Acceso no autorizado		7	9	8,0
DOCUMENTACIÓN INTERNA	4	7	9	6,7
[E.15] Alteración de la información		4		4
[E.18] Destrucción de la información	4			4
[E.19] Fugas de información			7	7
[A.5] Suplantación de la identidad		7	9	8
[A.6] Abuso de privilegios de acceso	4	7	9	6,7
[A.11] Acceso no autorizado		7	9	8
MATERIAL IMPRESO	10	10	9	9,7
[N.1] Fuego	10			10
[N.2] Daños por agua	9			9
[N.*] Desastres naturales	10			10
[I.1] Fuego	10			10
[I.2] Daños por agua	9			9
[I.*] Desastres industriales	10			10
[I.3] Contaminación medioambiental	9			9
[I.7] Condiciones inadecuadas de temperatura o humedad	10			10
[E.1] Errores de los usuarios	4	6	7	5,7
[E.15] Alteración de la información		4		4
[E.18] Destrucción de la información	10			10
[E.19] Fugas de información			7	7
[A.7] Uso no previsto	4		4	4

[A.11] Acceso no autorizado		4	9	6,5
[A.15] Modificación de la información		10		10
[A.18] Destrucción de la información	10			10
[A.26] Ataques destructivos	7			7
CARPETAS COMPARTIDAS	4	7	9	6,7
[E.15] Alteración de la información		4		4
[E.18] Destrucción de la información	4			4
[E.19] Fugas de información			7	7
[A.5] Suplantación de la identidad		7	9	8
[A.6] Abuso de privilegios de acceso	4	7	9	6,7
[A.11] Acceso no autorizado		7	9	8
APLICACIONES	10	10	10	10
MOTOR DE BASE DE DATOS	10	10	10	10
[I.5.1] Avería de origen lógico	9			9
[E.8] Difusión de software dañino	7	7	7	7
[E.20]Vulnerabilidades de los programas (software)	4	8	8	6,7
[E.21] Errores de mantenimiento/actualización de programas (software)	4	7	9	6,7
[A.8] Difusión de software dañino	10	10	10	10
[A.22] Manipulación de programas	9	10	10	9,7
REPOSITORIO DE APLICACIONES DESARROLLADAS	10	10	10	10
[I.5.1] Avería de origen lógico	9			9
[E.8] Difusión de software dañino	7	7	7	7
[E.20]Vulnerabilidades de los programas (software)	4	8	8	6,7
[E.21] Errores de mantenimiento/actualización de programas (software)	4	7	9	6,7
[A.8] Difusión de software dañino	10	10	10	10
[A.22] Manipulación de programas	9	10	10	9,7
ANTIVIRUS	10	10	10	10
[I.5.1] Avería de origen lógico	9			9
[E.8] Difusión de software dañino	7	7	7	7
[E.20]Vulnerabilidades de los programas (software)	4	8	8	6,7
[E.21] Errores de mantenimiento/actualización de programas (software)	4	7	9	6,7
[A.8] Difusión de software dañino	10	10	10	10
[A.22] Manipulación de programas	9	10	10	9,7
FIREWALL	10	10	10	10
[I.5.1] Avería de origen lógico	9			9

[E.4] Errores de configuración		4		4
[E.8] Difusión de software dañino	7	7	7	7
[E.18] Destrucción de la información	4			4
[E.20]Vulnerabilidades de los programas (software)	4	8	8	6,7
[E.21] Errores de mantenimiento/actualización de programas (software)	4	7	9	6,7
[A.4] Manipulación de los ficheros de configuración	7	7	7	7
[A.5] Suplantación de la identidad		7	9	8
[A.8] Difusión de software dañino	10	10	10	10
[A.22] Manipulación de programas	9	10	10	9,7
LICENCIAS	10	10	10	10
[I.5.1] Avería de origen lógico	9			9
[E.8] Difusión de software dañino	7	7	7	7
[E.20]Vulnerabilidades de los programas (software)	4	8	8	6,7
[E.21] Errores de mantenimiento/actualización de programas (software)	4	7	9	6,7
[A.8] Difusión de software dañino	10	10	10	10
[A.22] Manipulación de programas	9	10	10	9,7
NAVEGADORES	10	10	10	10
[I.5.1] Avería de origen lógico	9			9
[E.8] Difusión de software dañino	7	7	7	7
[E.20]Vulnerabilidades de los programas (software)	4	8	8	6,7
[E.21] Errores de mantenimiento/actualización de programas (software)	4	7	9	6,7
[A.8] Difusión de software dañino	10	10	10	10
[A.22] Manipulación de programas	9	10	10	9,7
SISTEMAS OPERATIVOS	10	10	10	10
[I.5.1] Avería de origen lógico	9			9
[E.8] Difusión de software dañino	7	7	7	7
[E.20]Vulnerabilidades de los programas (software)	4	8	8	6,7
[E.21] Errores de mantenimiento/actualización de programas (software)	4	7	9	6,7
[A.8] Difusión de software dañino	10	10	10	10
[A.22] Manipulación de programas	9	10	10	9,7
EQUIPOS	10	7	9	8,7
DISPOSITIVOS DE ALMACENAMIENTO	10	7	9	8,7

[N.1] Fuego	10			10
[N.2] Daños por agua	9			9
[N.*] Desastres naturales	10			10
[I.1] Fuego	10			10
[I.2] Daños por agua	9			9
[I.*] Desastres industriales	10			10
[I.3] Contaminación medioambiental	9			9
[I.4] Contaminación electromagnética	7			7
[I.5.2] Avería de origen físico	9			9
[I.6] Corte del suministro eléctrico	10			10
[I.7] Condiciones inadecuadas de temperatura o humedad	10			10
[I.11] Emanaciones electromagnéticas (TEMPEST)			4	4
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	7			7
[E.24] Caída del sistema por agotamiento de recursos	9			9
[E.25] Pérdida de equipos	10		9	9,5
[A.11] Acceso no autorizado	7	7	9	7,7
[A.23] Manipulación de hardware	9		9	9
[A.24] Denegación de servicio	10			10
[A.25] Robo de equipos	10		9	9,5
[A.26] Ataques destructivos	10			10
COMPUTADORAS	10	7	9	8,7
[N.1] Fuego	10			10
[N.2] Daños por agua	9			9
[N.*] Desastres naturales	10			10
[I.1] Fuego	10			10
[I.2] Daños por agua	9			9
[I.*] Desastres industriales	10			10
[I.3] Contaminación medioambiental	9			9
[I.4] Contaminación electromagnética	7			7
[I.5.2] Avería de origen físico	9			9
[I.6] Corte del suministro eléctrico	10			10
[I.7] Condiciones inadecuadas de temperatura o humedad	10			10
[I.11] Emanaciones electromagnéticas (TEMPEST)			4	4
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	7			7
[E.24] Caída del sistema por agotamiento de recursos	9			9

[E.25] Pérdida de equipos	10		9	9,5
[A.11] Acceso no autorizado	7	7	9	7,7
[A.23] Manipulación de hardware	9		9	9
[A.24] Denegación de servicio	10			10
[A.25] Robo de equipos	10		9	9,5
[A.26] Ataques destructivos	10			10
TELÉFONOS IP	10	7	9	8,7
[N.1] Fuego	10			10
[N.2] Daños por agua	9			9
[N.*] Desastres naturales	10			10
[I.1] Fuego	10			10
[I.2] Daños por agua	9			9
[I.*] Desastres industriales	10			10
[I.3] Contaminación medioambiental	9			9
[I.4] Contaminación electromagnética	7			7
[I.5.2] Avería de origen físico	9			9
[I.6] Corte del suministro eléctrico	10			10
[I.7] Condiciones inadecuadas de temperatura o humedad	10			10
[I.11] Emanaciones electromagnéticas (TEMPEST)			4	4
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	7			7
[E.24] Caída del sistema por agotamiento de recursos	9			9
[E.25] Pérdida de equipos	10		9	9,5
[A.11] Acceso no autorizado	7	7	9	7,7
[A.23] Manipulación de hardware	9		9	9
[A.24] Denegación de servicio	10			10
[A.25] Robo de equipos	10		9	9,5
[A.26] Ataques destructivos	10			10
SERVIDORES	10	7	9	8,7
[N.1] Fuego	10			10
[N.2] Daños por agua	9			9
[N.*] Desastres naturales	10			10
[I.1] Fuego	10			10
[I.2] Daños por agua	9			9
[I.*] Desastres industriales	10			10
[I.3] Contaminación medioambiental	9			9
[I.4] Contaminación electromagnética	7			7
[I.5.2] Avería de origen físico	9			9
[I.6] Corte del suministro eléctrico	10			10

[I.7] Condiciones inadecuadas de temperatura o humedad	10			10
[I.11] Emanaciones electromagnéticas (TEMPEST)			4	4
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	7			7
[E.24] Caída del sistema por agotamiento de recursos	9			9
[E.25] Pérdida de equipos	10		9	9,5
[A.11] Acceso no autorizado	7	7	9	7,7
[A.23] Manipulación de hardware	9		9	9
[A.24] Denegación de servicio	10			10
[A.25] Robo de equipos	10		9	9,5
[A.26] Ataques destructivos	10			10
EQUIPO PARA EL FUNCIONAMIENTO DE RED	10	7	9	8,7
[N.1] Fuego	10			10
[N.2] Daños por agua	9			9
[N.*] Desastres naturales	10			10
[I.1] Fuego	10			10
[I.2] Daños por agua	9			9
[I.*] Desastres industriales	10			10
[I.3] Contaminación medioambiental	9			9
[I.4] Contaminación electromagnética	7			7
[I.5.2] Avería de origen físico	9			9
[I.6] Corte del suministro eléctrico	10			10
[I.7] Condiciones inadecuadas de temperatura o humedad	10			10
[I.11] Emanaciones electromagnéticas (TEMPEST)			4	4
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	7			7
[E.24] Caída del sistema por agotamiento de recursos	9			9
[E.25] Pérdida de equipos	10		9	9,5
[A.11] Acceso no autorizado	7	7	9	7,7
[A.23] Manipulación de hardware	9		9	9
[A.24] Denegación de servicio	10			10
[A.25] Robo de equipos	10		9	9,5
[A.26] Ataques destructivos	10			10
EQUIPO MULTIFUNCIONAL	10	7	9	8,7
[N.1] Fuego	10			10
[N.2] Daños por agua	9			9

[N.*] Desastres naturales	10			10
[I.1] Fuego	10			10
[I.2] Daños por agua	9			9
[I.*] Desastres industriales	10			10
[I.3] Contaminación medioambiental	9			9
[I.4] Contaminación electromagnética	7			7
[I.5.2] Avería de origen físico	9			9
[I.6] Corte del suministro eléctrico	10			10
[I.7] Condiciones inadecuadas de temperatura o humedad	10			10
[I.11] Emanaciones electromagnéticas (TEMPEST)			4	4
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	7			7
[E.24] Caída del sistema por agotamiento de recursos	9			9
[E.25] Pérdida de equipos	10		9	9,5
[A.11] Acceso no autorizado	7	7	9	7,7
[A.23] Manipulación de hardware	9		9	9
[A.24] Denegación de servicio	10			10
[A.25] Robo de equipos	10		9	9,5
[A.26] Ataques destructivos	10			10
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	10	7	9	8,7
[N.1] Fuego	10			10
[N.2] Daños por agua	9			9
[N.*] Desastres naturales	10			10
[I.1] Fuego	10			10
[I.2] Daños por agua	9			9
[I.*] Desastres industriales	10			10
[I.3] Contaminación medioambiental	9			9
[I.4] Contaminación electromagnética	7			7
[I.5.2] Avería de origen físico	9			9
[I.6] Corte del suministro eléctrico	10			10
[I.7] Condiciones inadecuadas de temperatura o humedad	10			10
[I.11] Emanaciones electromagnéticas (TEMPEST)			4	4
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	7			7
[E.24] Caída del sistema por agotamiento de recursos	9			9
[E.25] Pérdida de equipos	10		9	9,5

[A.11] Acceso no autorizado	7	7	9	7,7
[A.23] Manipulación de hardware	9		9	9
[A.24] Denegación de servicio	10			10
[A.25] Robo de equipos	10		9	9,5
[A.26] Ataques destructivos	10			10
RADIOS DE COMUNICACIÓN	10	7	9	8,7
[N.1] Fuego	10			10
[N.2] Daños por agua	9			9
[N.*] Desastres naturales	10			10
[I.1] Fuego	10			10
[I.2] Daños por agua	9			9
[I.*] Desastres industriales	10			10
[I.3] Contaminación medioambiental	9			9
[I.4] Contaminación electromagnética	7			7
[I.5.2] Avería de origen físico	9			9
[I.6] Corte del suministro eléctrico	10			10
[I.7] Condiciones inadecuadas de temperatura o humedad	10			10
[I.11] Emanaciones electromagnéticas (TEMPEST)			4	4
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	7			7
[E.24] Caída del sistema por agotamiento de recursos	9			9
[E.25] Pérdida de equipos	10		9	9,5
[A.11] Acceso no autorizado	7	7	9	7,7
[A.23] Manipulación de hardware	9		9	9
[A.24] Denegación de servicio	10			10
[A.25] Robo de equipos	10		9	9,5
[A.26] Ataques destructivos	10			10
COMUNICACIÓN	9	8	9	8,7
ETHERNET	9	8	9	8,7
[I.8] Fallo de servicios de comunicación	9			9
[E.2] Errores del administrador del sistema	8	8	8	8
[E.9] Errores de [re-]encaminamiento			7	7
[E.10] Errores de secuencia		7		7
[E.15] Alteración de la información		4		4
[E.19] Fugas de información			7	7
[E.24] Caída del sistema por agotamiento de recursos	9			9
[A.5] Suplantación de la identidad		7	9	8
[A.7] Uso no previsto	7	7	7	7

[A.9] [Re-]encaminamiento de mensajes			7	7
[A.10] Alteración de secuencia		7		7
[A.11] Acceso no autorizado		7	9	8
[A.12] Análisis de tráfico			5	5
[A.14] Interceptación de información (escucha)			7	7
[A.15] Modificación de la información		7		7
[A.18] Destrucción de la información	9			9
[A.24] Denegación de servicio	9			9
RED INALAMBRICA	9	8	9	8,7
[I.8] Fallo de servicios de comunicación	9			9
[E.2] Errores del administrador del sistema	8	8	8	8
[E.9] Errores de [re-]encaminamiento			7	7
[E.10] Errores de secuencia		7		7
[E.15] Alteración de la información		4		4
[E.19] Fugas de información			7	7
[E.24] Caída del sistema por agotamiento de recursos	9			9
[A.5] Suplantación de la identidad		7	9	8
[A.7] Uso no previsto	7	7	7	7
[A.9] [Re-]encaminamiento de mensajes			7	7
[A.10] Alteración de secuencia		7		7
[A.11] Acceso no autorizado		7	9	8
[A.12] Análisis de tráfico			5	5
[A.14] Interceptación de información (escucha)			7	7
[A.15] Modificación de la información		7		7
[A.18] Destrucción de la información	9			9
[A.24] Denegación de servicio	9			9
RED LAN	9	8	9	8,7
[I.8] Fallo de servicios de comunicación	9			9
[E.2] Errores del administrador del sistema	8	8	8	8
[E.9] Errores de [re-]encaminamiento			7	7
[E.10] Errores de secuencia		7		7
[E.15] Alteración de la información		4		4
[E.19] Fugas de información			7	7
[E.24] Caída del sistema por agotamiento de recursos	9			9
[A.5] Suplantación de la identidad		7	9	8
[A.7] Uso no previsto	7	7	7	7
[A.9] [Re-]encaminamiento de mensajes			7	7
[A.10] Alteración de secuencia		7		7

[A.11] Acceso no autorizado		7	9	8
[A.12] Análisis de tráfico			5	5
[A.14] Interceptación de información (escucha)			7	7
[A.15] Modificación de la información		7		7
[A.18] Destrucción de la información	9			9
[A.24] Denegación de servicio	9			9
RED TELEFÓNICA	9	8	9	8,7
[I.8] Fallo de servicios de comunicación	9			9
[E.2] Errores del administrador del sistema	8	8	8	8
[E.9] Errores de [re-]encaminamiento			7	7
[E.10] Errores de secuencia		7		7
[E.15] Alteración de la información		4		4
[E.19] Fugas de información			7	7
[E.24] Caída del sistema por agotamiento de recursos	9			9
[A.5] Suplantación de la identidad		7	9	8
[A.7] Uso no previsto	7	7	7	7
[A.9] [Re-]encaminamiento de mensajes			7	7
[A.10] Alteración de secuencia		7		7
[A.11] Acceso no autorizado		7	9	8
[A.12] Análisis de tráfico			5	5
[A.14] Interceptación de información (escucha)			7	7
[A.15] Modificación de la información		7		7
[A.18] Destrucción de la información	9			9
[A.24] Denegación de servicio	9			9
ELEMENTOS AUXILIARES	10	4	9	7,7
UPS	10	4	9	7,7
[N.1] Fuego	10			10
[N.2] Daños por agua	9			9
[N.*] Desastres naturales	10			10
[I.1] Fuego	10			10
[I.2] Daños por agua	9			9
[I.*] Desastres industriales	10			10
[I.3] Contaminación medioambiental	9			9
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	7			7
[A.7] Uso no previsto	9	4	4	5,7
[A.23] Manipulación de hardware	9		9	9
[A.25] Robo de equipos	7			7
[A.26] Ataques destructivos	7			7

GENERADOR ELÉCTRICO	10	4	9	7,7
[N.1] Fuego	10			10
[N.2] Daños por agua	9			9
[N.*] Desastres naturales	10			10
[I.1] Fuego	10			10
[I.2] Daños por agua	9			9
[I.*] Desastres industriales	10			10
[I.3] Contaminación medioambiental	9			9
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	7			7
[A.7] Uso no previsto	9	4	4	5,7
[A.23] Manipulación de hardware	9		9	9
[A.25] Robo de equipos	7			7
[A.26] Ataques destructivos	7			7
EQUIPOS DE CLIMATIZACIÓN	10	4	9	7,7
[N.1] Fuego	10			10
[N.2] Daños por agua	9			9
[N.*] Desastres naturales	10			10
[I.1] Fuego	10			10
[I.2] Daños por agua	9			9
[I.*] Desastres industriales	10			10
[I.3] Contaminación medioambiental	9			9
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	7			7
[A.7] Uso no previsto	9	4	4	5,7
[A.23] Manipulación de hardware	9		9	9
[A.25] Robo de equipos	7			7
[A.26] Ataques destructivos	7			7
MOBILIARIO	10	4	9	7,7
[N.1] Fuego	10			10
[N.2] Daños por agua	9			9
[N.*] Desastres naturales	10			10
[I.1] Fuego	10			10
[I.2] Daños por agua	9			9
[I.*] Desastres industriales	10			10
[I.3] Contaminación medioambiental	9			9
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	7			7
[A.7] Uso no previsto	9	4	4	5,7
[A.23] Manipulación de hardware	9		9	9
[A.25] Robo de equipos	7			7

[A.26] Ataques destructivos	7			7
SERVICIOS	10	10	10	10
TELEFONÍA	9	9	7	8,3
[E.15] Alteración de la información		7		7
[E.18] Destrucción de la información	7			7
[E.19] Fugas de información			7	7
[A.15] Modificación de la información		9		9
[A.18] Destrucción de la información	9			9
[A.24] Denegación de servicio	9			9
INTERNET	9	10	10	9,7
[E.15] Alteración de la información		7		7
[E.18] Destrucción de la información	7			7
[E.19] Fugas de información			7	7
[A.5] Suplantación de la identidad		10	10	10
[A.15] Modificación de la información		9		9
[A.18] Destrucción de la información	9			9
[A.24] Denegación de servicio	9			9
ELECTRICIDAD	9	9	9	9
[I.9] Interrupción de otros servicios o suministros esenciales	9			9
[E.15] Alteración de la información		7		7
[E.18] Destrucción de la información	7			7
CORREO INSTITUCIONAL	9	9	9	9
[E.1] Errores de los usuarios	7	7	7	7
[E.2] Errores del administrador del sistema	8	8	8	8
[E.15] Alteración de la información		4		4
[E.18] Destrucción de la información	7			7
[E.19] Fugas de información			7	7
[E.24] Caída del sistema por agotamiento de recursos	9			9
[A.5] Suplantación de la identidad		9	9	9
[A.6] Abuso de privilegios de acceso	4	7	7	6
[A.7] Uso no previsto	4	7	7	6
[A.11] Acceso no autorizado		7	9	8
[A.15] Modificación de la información		9		9
[A.18] Destrucción de la información	9			9
[A.24] Denegación de servicio	9			9
SOPORTE DE RED	10	10	9	9,7
[E.1] Errores de los usuarios	4	6	7	5,7
[E.15] Alteración de la información		4		4
[E.18] Destrucción de la información	10			10
[E.19] Fugas de información			7	7
[A.7] Uso no previsto	4		4	4

[A.11] Acceso no autorizado		4	9	6,5
[A.15] Modificación de la información		10		10
[A.18] Destrucción de la información	10			10
SOPORTE A LOS SERVICIOS INFORMÁTICOS	9	9	7	8,3
[E.1] Errores de los usuarios	7	7	5	6,3
[E.2] Errores del administrador del sistema	8	8	6	7,3
[E.15] Alteración de la información		4		4
[E.18] Destrucción de la información	7			7
[E.19] Fugas de información			5	5
[E.24] Caída del sistema por agotamiento de recursos	9			9
[A.5] Suplantación de la identidad		9	7	8
[A.6] Abuso de privilegios de acceso	4	7	5	5,3
[A.7] Uso no previsto	4	7	5	5,3
[A.11] Acceso no autorizado		7	7	7
[A.15] Modificación de la información		9		9
[A.18] Destrucción de la información	9			9
[A.24] Denegación de servicio	9			9
MANTENIMIENTO DE EQUIPOS	9	10	10	9,7
[I.9] Interrupción de otros servicios o suministros esenciales	9			9
[E.15] Alteración de la información		7		7
[E.18] Destrucción de la información	7			7
[E.19] Fugas de información			7	7
[A.5] Suplantación de la identidad		10	10	10
[A.15] Modificación de la información		9		9
[A.18] Destrucción de la información	9			9
[A.19] Revelación de información			9	9
[A.24] Denegación de servicio	9			9
INFRAESTRUCTURA	10		10	10
INSTALACIÓN DE RED DE DATOS	10		10	10
[N.1] Fuego	10			10
[N.2] Daños por agua	10			10
[N.*] Desastres naturales	10			10
[I.1] Fuego	10			10
[I.2] Daños por agua	10			10
[I.*] Desastres industriales	10			10
[I.3] Contaminación medioambiental	7			7
[I.4] Contaminación electromagnética	7			7
[E.25] Pérdida de equipos			7	7
[A.6] Abuso de privilegios de acceso	7			7
[A.7] Uso no previsto	7			7

[A.25] Robo de equipos		10	10
[A.26] Ataques destructivos	10		10
[A.27] Ocupación enemiga	10		10
INSTALACIÓN DE RED ELÉCTRICA	10	10	10
[N.1] Fuego	10		10
[N.2] Daños por agua	10		10
[N.*] Desastres naturales	10		10
[I.1] Fuego	10		10
[I.2] Daños por agua	10		10
[I.*] Desastres industriales	10		10
[I.3] Contaminación medioambiental	7		7
[I.4] Contaminación electromagnética	7		7
[E.25] Pérdida de equipos		7	7
[A.6] Abuso de privilegios de acceso	7		7
[A.7] Uso no previsto	7		7
[A.25] Robo de equipos		10	10
[A.26] Ataques destructivos	10		10
[A.27] Ocupación enemiga	10		10
UPS DEL CENTRO CABLEADO	10	10	10
[N.1] Fuego	10		10
[N.2] Daños por agua	10		10
[N.*] Desastres naturales	10		10
[I.1] Fuego	10		10
[I.2] Daños por agua	10		10
[I.*] Desastres industriales	10		10
[I.3] Contaminación medioambiental	7		7
[I.4] Contaminación electromagnética	7		7
[E.25] Pérdida de equipos		7	7
[A.6] Abuso de privilegios de acceso	7		7
[A.7] Uso no previsto	7		7
[A.25] Robo de equipos		10	10
[A.26] Ataques destructivos	10		10
[A.27] Ocupación enemiga	10		10
ESPACIO FÍSICO DDTI	10	10	10
[N.1] Fuego	10		10
[N.2] Daños por agua	10		10
[N.*] Desastres naturales	10		10
[I.1] Fuego	10		10
[I.2] Daños por agua	10		10
[I.*] Desastres industriales	10		10
[I.3] Contaminación medioambiental	7		7
[I.4] Contaminación electromagnética	7		7
[E.25] Pérdida de equipos		7	7

[A.6] Abuso de privilegios de acceso	7			7
[A.7] Uso no previsto	7			7
[A.25] Robo de equipos			10	10
[A.26] Ataques destructivos	10			10
[A.27] Ocupación enemiga	10			10
PERSONAL	7	9	9	8,3
PERSONAL ADMINISTRATIVO	7	9	9	8,3
[E.15] Alteración de la información		7		7
[E.18] Destrucción de la información	4			4
[E.19] Fugas de información			7	7
[A.15] Modificación de la información		9		9
[A.18] Destrucción de la información	7			7
[A.19] Revelación de información			9	9
[A.28] Indisponibilidad del personal	7			7
[A.29] Extorsión	7	7	9	7,7
[A.30] Ingeniería social (picaresca)	7	7	9	7,7
PERSONAL DE DESARROLLO	7	9	9	8,3
[E.15] Alteración de la información		7		7
[E.18] Destrucción de la información	4			4
[E.19] Fugas de información			7	7
[A.15] Modificación de la información		9		9
[A.18] Destrucción de la información	7			7
[A.19] Revelación de información			9	9
[A.28] Indisponibilidad del personal	7			7
[A.29] Extorsión	7	7	9	7,7
[A.30] Ingeniería social (picaresca)	7	7	9	7,7

Nota: Elaboración propia

Anexo 6: Riesgo potencial acumulado de Amenazas del DDTI-UTN

	RIESGO POTENCIAL ACUMULADO			**PESO PONDERADO**
ACTIVOS	**D**	**I**	**C**	
INFORMACIÓN	6,9	7,5	8,2	7,5
BASE DE DATOS	4,4	6,9	8,2	6,5
[E.15] Alteración de la información		3,4		3,4
[E.18] Destrucción de la información	3,4			3,4
[E.19] Fugas de información			5,1	5,1
[A.5] Suplantación de la identidad		6	7,3	6,7
[A.6] Abuso de privilegios de acceso	4,4	6,1	7,4	6
[A.11] Acceso no autorizado		6,9	8,2	7,6

ARCHIVO DE DATOS	4,4	6,9	8,2	6,5
[E.15] Alteración de la información		3,4		3,4
[E.18] Destrucción de la información	3,4			3,4
[E.19] Fugas de información			5,1	5,1
[A.5] Suplantación de la identidad		6	7,3	6,7
[A.6] Abuso de privilegios de acceso	4,4	6,1	7,4	6,0
[A.11] Acceso no autorizado		6,9	8,2	7,6
DOCUMENTACIÓN INTERNA	4,4	6,9	8,2	6,5
[E.15] Alteración de la información		3,4		3,4
[E.18] Destrucción de la información	3,4			3,4
[E.19] Fugas de información			5,1	5,1
[A.5] Suplantación de la identidad		6	7,3	6,7
[A.6] Abuso de privilegios de acceso	4,4	6,1	7,4	6
[A.11] Acceso no autorizado		6,9	8,2	7,6
MATERIAL IMPRESO	6,9	7,5	6,4	6,9
[N.1] Fuego	6			6
[N.2] Daños por agua	5,4			5,4
[N.*] Desastres naturales	6			6
[I.1] Fuego	6,6			6,6
[I.2] Daños por agua	6,1			6,1
[I.*] Desastres industriales	6,6			6,6
[I.3] Contaminación medioambiental	6,3			6,3
[I.7] Condiciones inadecuadas de temperatura o humedad	6,9			6,9
[E.1] Errores de los usuarios	3,4	4,6	5,1	4,4
[E.15] Alteración de la información		3,4		3,4
[E.18] Destrucción de la información	6,9			6,9
[E.19] Fugas de información			5,1	5,1
[A.7] Uso no previsto	3,5		3,5	3,5
[A.11] Acceso no autorizado		3,4	6,4	4,9
[A.15] Modificación de la información		7,5		7,5
[A.18] Destrucción de la información	6,9			6,9
[A.26] Ataques destructivos	5			5
CARPETAS COMPARTIDAS	4,4	6,9	8,2	6,5
[E.15] Alteración de la información		3,4		3,4
[E.18] Destrucción de la información	3,4			3,4
[E.19] Fugas de información			5,1	5,1
[A.5] Suplantación de la identidad		6	7,3	6,7
[A.6] Abuso de privilegios de acceso	4,4	6,1	7,4	6
[A.11] Acceso no autorizado		6,9	8,2	7,6
APLICACIONES	6,9	7	7,3	7,1
MOTOR DE BASE DE DATOS	6,9	7	7,2	7
[I.5.1] Avería de origen lógico	6,3			6,3

[E.8] Difusión de software dañino	5,1	5,1	5,1	5,1
[E.20]Vulnerabilidades de los programas (software)	3,3	5,6	5,6	4,8
[E.21] Errores de mantenimiento/actualización de programas (software)	4,2	6	7,2	5,8
[A.8] Difusión de software dañino	6,9	6,9	6,9	6,9
[A.22] Manipulación de programas	6,5	7	7	6,8
REPOSITORIO DE APLICACIONES DESARROLLADAS	6,9	7	7,2	7
[I.5.1] Avería de origen lógico	6,3			6,3
[E.8] Difusión de software dañino	5,1	5,1	5,1	5,1
[E.20]Vulnerabilidades de los programas (software)	3,3	5,6	5,6	4,8
[E.21] Errores de mantenimiento/actualización de programas (software)	4,2	6	7,2	5,8
[A.8] Difusión de software dañino	6,9	6,9	6,9	6,9
[A.22] Manipulación de programas	6,5	7	7	6,8
ANTIVIRUS	6,9	7	7,2	7
[I.5.1] Avería de origen lógico	6,3			6,3
[E.8] Difusión de software dañino	5,1	5,1	5,1	5,1
[E.20]Vulnerabilidades de los programas (software)	3,3	5,6	5,6	4,8
[E.21] Errores de mantenimiento/actualización de programas (software)	4,2	6	7,2	5,8
[A.8] Difusión de software dañino	6,9	6,9	6,9	6,9
[A.22] Manipulación de programas	6,5	7	7	6,8
FIREWALL	6,9	7	7,3	7
[I.5.1] Avería de origen lógico	6,3			6,3
[E.4] Errores de configuración		3,4		3,4
[E.8] Difusión de software dañino	5,1	5,1	5,1	5,1
[E.18] Destrucción de la información	3,4			3,4
[E.20]Vulnerabilidades de los programas (software)	3,3	5,6	5,6	4,8
[E.21] Errores de mantenimiento/actualización de programas (software)	4,2	6	7,2	5,8
[A.4] Manipulación de los ficheros de configuración	5,9	5,9	5,9	5,9
[A.5] Suplantación de la identidad		6	7,3	6,7
[A.8] Difusión de software dañino	6,9	6,9	6,9	6,9
[A.22] Manipulación de programas	6,5	7	7	6,8
LICENCIAS	6,9	7	7,2	7

[I.5.1] Avería de origen lógico	6,3			6,3
[E.8] Difusión de software dañino	5,1	5,1	5,1	5,1
[E.20]Vulnerabilidades de los programas (software)	3,3	5,6	5,6	4,8
[E.21] Errores de mantenimiento/actualización de programas (software)	4,2	6	7,2	5,8
[A.8] Difusión de software dañino	6,9	6,9	6,9	6,9
[A.22] Manipulación de programas	6,5	7	7	6,8
NAVEGADORES	6,9	7	7,2	7
[I.5.1] Avería de origen lógico	6,3			6,3
[E.8] Difusión de software dañino	5,1	5,1	5,1	5,1
[E.20]Vulnerabilidades de los programas (software)	3,3	5,6	5,6	4,8
[E.21] Errores de mantenimiento/actualización de programas (software)	4,2	6	7,2	5,8
[A.8] Difusión de software dañino	6,9	6,9	6,9	6,9
[A.22] Manipulación de programas	6,5	7	7	6,8
SISTEMAS OPERATIVOS	6,9	7	7,2	7
[I.5.1] Avería de origen lógico	6,3			6,3
[E.8] Difusión de software dañino	5,1	5,1	5,1	5,1
[E.20]Vulnerabilidades de los programas (software)	3,3	5,6	5,6	4,8
[E.21] Errores de mantenimiento/actualización de programas (software)	4,2	6	7,2	5,8
[A.8] Difusión de software dañino	6,9	6,9	6,9	6,9
[A.22] Manipulación de programas	6,5	7	7	6,8
EQUIPOS	7,3	5,2	6,4	6,3
DISPOSITIVOS DE ALMACENAMIENTO	7,3	5,2	6,4	6,3
[N.1] Fuego	6			6
[N.2] Daños por agua	5,4			5,4
[N.*] Desastres naturales	6			6
[I.1] Fuego	6,6			6,6
[I.2] Daños por agua	6,1			6,1
[I.*] Desastres industriales	6,6			6,6
[I.3] Contaminación medioambiental	5,4			5,4
[I.4] Contaminación electromagnética	5,1			5,1
[I.5.2] Avería de origen físico	6,3			6,3
[I.6] Corte del suministro eléctrico	6,9			6,9
[I.7] Condiciones inadecuadas de temperatura o humedad	6,9			6,9

[I.11] Emanaciones electromagnéticas (TEMPEST)			3,3	3,3
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1			5,1
[E.24] Caída del sistema por agotamiento de recursos	7,2			7,2
[E.25] Pérdida de equipos	6,9		6,4	6,7
[A.11] Acceso no autorizado	5,2	5,2	6,4	5,6
[A.23] Manipulación de hardware	6		6	6
[A.24] Denegación de servicio	7,3			7,3
[A.25] Robo de equipos	6,5		6	6,3
[A.26] Ataques destructivos	6,8			6,8
COMPUTADORAS	7,3	5,2	6,4	6,3
[N.1] Fuego	6			6
[N.2] Daños por agua	5,4			5,4
[N.*] Desastres naturales	6			6
[I.1] Fuego	6,6			6,6
[I.2] Daños por agua	6,1			6,1
[I.*] Desastres industriales	6,6			6,6
[I.3] Contaminación medioambiental	5,4			5,4
[I.4] Contaminación electromagnética	5,1			5,1
[I.5.2] Avería de origen físico	6,3			6,3
[I.6] Corte del suministro eléctrico	6,9			6,9
[I.7] Condiciones inadecuadas de temperatura o humedad	6,9			6,9
[I.11] Emanaciones electromagnéticas (TEMPEST)			3,3	3,3
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1			5,1
[E.24] Caída del sistema por agotamiento de recursos	7,2			7,2
[E.25] Pérdida de equipos	6,9		6,4	6,7
[A.11] Acceso no autorizado	5,2	5,2	6,4	5,6
[A.23] Manipulación de hardware	6		6	6
[A.24] Denegación de servicio	7,3			7,3
[A.25] Robo de equipos	6,5		6	6,3
[A.26] Ataques destructivos	6,8			6,8
TELÉFONOS IP	7,3	5,2	6,4	6,3
[N.1] Fuego	6			6
[N.2] Daños por agua	5,4			5,4
[N.*] Desastres naturales	6			6
[I.1] Fuego	6,6			6,6
[I.2] Daños por agua	6,1			6,1

[I.*] Desastres industriales	6,6			6,6
[I.3] Contaminación medioambiental	5,4			5,4
[I.4] Contaminación electromagnética	5,1			5,1
[I.5.2] Avería de origen físico	6,3			6,3
[I.6] Corte del suministro eléctrico	6,9			6,9
[I.7] Condiciones inadecuadas de temperatura o humedad	6,9			6,9
[I.11] Emanaciones electromagnéticas (TEMPEST)			3,3	3,3
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1			5,1
[E.24] Caída del sistema por agotamiento de recursos	7,2			7,2
[E.25] Pérdida de equipos	6,9		6,4	6,7
[A.11] Acceso no autorizado	5,2	5,2	6,4	5,6
[A.23] Manipulación de hardware	6		6	6
[A.24] Denegación de servicio	7,3			7,3
[A.25] Robo de equipos	6,5		6	6,3
[A.26] Ataques destructivos	6,8			6,8
SERVIDORES	7,3	5,2	6,4	6,3
[N.1] Fuego	6			6
[N.2] Daños por agua	5,4			5,4
[N.*] Desastres naturales	6			6
[I.1] Fuego	6,6			6,6
[I.2] Daños por agua	6,1			6,1
[I.*] Desastres industriales	6,6			6,6
[I.3] Contaminación medioambiental	5,4			5,4
[I.4] Contaminación electromagnética	5,1			5,1
[I.5.2] Avería de origen físico	6,3			6,3
[I.6] Corte del suministro eléctrico	6,9			6,9
[I.7] Condiciones inadecuadas de temperatura o humedad	6,9			6,9
[I.11] Emanaciones electromagnéticas (TEMPEST)			3,3	3,3
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1			5,1
[E.24] Caída del sistema por agotamiento de recursos	7,2			7,2
[E.25] Pérdida de equipos	6,9		6,4	6,7
[A.11] Acceso no autorizado	5,2	5,2	6,4	5,6
[A.23] Manipulación de hardware	6		6	6
[A.24] Denegación de servicio	7,3			7,3
[A.25] Robo de equipos	6,5		6	6,3

[A.26] Ataques destructivos	6,8			6,8
EQUIPO PARA EL FUNCIONAMIENTO DE RED	7,3	5,2	6,4	6,3
[N.1] Fuego	6			6
[N.2] Daños por agua	5,4			5,4
[N.*] Desastres naturales	6			6
[I.1] Fuego	6,6			6,6
[I.2] Daños por agua	6,1			6,1
[I.*] Desastres industriales	6,6			6,6
[I.3] Contaminación medioambiental	5,4			5,4
[I.4] Contaminación electromagnética	5,1			5,1
[I.5.2] Avería de origen físico	6,3			6,3
[I.6] Corte del suministro eléctrico	6,9			6,9
[I.7] Condiciones inadecuadas de temperatura o humedad	6,9			6,9
[I.11] Emanaciones electromagnéticas (TEMPEST)			3,3	3,3
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1			5,1
[E.24] Caída del sistema por agotamiento de recursos	7,2			7,2
[E.25] Pérdida de equipos	6,9		6,4	6,7
[A.11] Acceso no autorizado	5,2	5,2	6,4	5,6
[A.23] Manipulación de hardware	6		6	6
[A.24] Denegación de servicio	7,3			7,3
[A.25] Robo de equipos	6,5		6	6,3
[A.26] Ataques destructivos	6,8			6,8
EQUIPO MULTIFUNCIONAL	7,3	5,2	6,4	6,3
[N.1] Fuego	6			6
[N.2] Daños por agua	5,4			5,4
[N.*] Desastres naturales	6			6
[I.1] Fuego	6,6			6,6
[I.2] Daños por agua	6,1			6,1
[I.*] Desastres industriales	6,6			6,6
[I.3] Contaminación medioambiental	5,4			5,4
[I.4] Contaminación electromagnética	5,1			5,1
[I.5.2] Avería de origen físico	6,3			6,3
[I.6] Corte del suministro eléctrico	6,9			6,9
[I.7] Condiciones inadecuadas de temperatura o humedad	6,9			6,9
[I.11] Emanaciones electromagnéticas (TEMPEST)			3,3	3,3

[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1			5,1
[E.24] Caída del sistema por agotamiento de recursos	7,2			7,2
[E.25] Pérdida de equipos	6,9		6,4	6,7
[A.11] Acceso no autorizado	5,2	5,2	6,4	5,6
[A.23] Manipulación de hardware	6		6	6
[A.24] Denegación de servicio	7,3			7,3
[A.25] Robo de equipos	6,5		6	6,3
[A.26] Ataques destructivos	6,8			6,8
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	7,3	5,2	6,4	6,3
[N.1] Fuego	6			6
[N.2] Daños por agua	5,4			5,4
[N.*] Desastres naturales	6			6
[I.1] Fuego	6,6			6,6
[I.2] Daños por agua	6,1			6,1
[I.*] Desastres industriales	6,6			6,6
[I.3] Contaminación medioambiental	5,4			5,4
[I.4] Contaminación electromagnética	5,1			5,1
[I.5.2] Avería de origen físico	6,3			6,3
[I.6] Corte del suministro eléctrico	6,9			6,9
[I.7] Condiciones inadecuadas de temperatura o humedad	6,9			6,9
[I.11] Emanaciones electromagnéticas (TEMPEST)			3,3	3,3
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1			5,1
[E.24] Caída del sistema por agotamiento de recursos	7,2			7,2
[E.25] Pérdida de equipos	6,9		6,4	6,7
[A.11] Acceso no autorizado	5,2	5,2	6,4	5,6
[A.23] Manipulación de hardware	6		6	6
[A.24] Denegación de servicio	7,3			7,3
[A.25] Robo de equipos	6,5		6	6,3
[A.26] Ataques destructivos	6,8			6,8
RADIOS DE COMUNICACIÓN	7,3	5,2	6,4	6,3
[N.1] Fuego	6			6
[N.2] Daños por agua	5,4			5,4
[N.*] Desastres naturales	6			6
[I.1] Fuego	6,6			6,6
[I.2] Daños por agua	6,1			6,1
[I.*] Desastres industriales	6,6			6,6

[I.3] Contaminación medioambiental	5,4			5,4
[I.4] Contaminación electromagnética	5,1			5,1
[I.5.2] Avería de origen físico	6,3			6,3
[I.6] Corte del suministro eléctrico	6,9			6,9
[I.7] Condiciones inadecuadas de temperatura o humedad	6,9			6,9
[I.11] Emanaciones electromagnéticas (TEMPEST)			3,3	3,3
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1			5,1
[E.24] Caída del sistema por agotamiento de recursos	7,2			7,2
[E.25] Pérdida de equipos	6,9		6,4	6,7
[A.11] Acceso no autorizado	5,2	5,2	6,4	5,6
[A.23] Manipulación de hardware	6		6	6
[A.24] Denegación de servicio	7,3			7,3
[A.25] Robo de equipos	6,5		6	6,3
[A.26] Ataques destructivos	6,8			6,8
COMUNICACIÓN	7,4	5,6	6,4	6,5
ETHERNET	7,4	5,6	6,4	6,5
[I.8] Fallo de servicios de comunicación	6,3			6,3
[E.2] Errores del administrador del sistema	5,6	5,6	5,6	5,6
[E.9] Errores de [re-]encaminamiento			5,1	5,1
[E.10] Errores de secuencia		5,1		5,1
[E.15] Alteración de la información		3,4		3,4
[E.19] Fugas de información			5,1	5,1
[E.24] Caída del sistema por agotamiento de recursos	6,4			6,4
[A.5] Suplantación de la identidad		5,2	6,4	5,8
[A.7] Uso no previsto	5,2	5,2	5,2	5,2
[A.9] [Re-]encaminamiento de mensajes			5,1	5,1
[A.10] Alteración de secuencia		5,1		5,1
[A.11] Acceso no autorizado		5,2	6,4	5,8
[A.12] Análisis de tráfico			3,9	3,9
[A.14] Interceptación de información (escucha)			5,2	5,2
[A.15] Modificación de la información		5,2		5,2
[A.18] Destrucción de la información	6,4			6,4
[A.24] Denegación de servicio	7,4			7,4
RED INALAMBRICA	7,4	5,6	6,4	6,5

[I.8] Fallo de servicios de comunicación	6,3			6,3
[E.2] Errores del administrador del sistema	5,6	5,6	5,6	5,6
[E.9] Errores de [re-]encaminamiento			5,1	5,1
[E.10] Errores de secuencia		5,1		5,1
[E.15] Alteración de la información		3,4		3,4
[E.19] Fugas de información			5,1	5,1
[E.24] Caída del sistema por agotamiento de recursos	6,4			6,4
[A.5] Suplantación de la identidad		5,2	6,4	5,8
[A.7] Uso no previsto	5,2	5,2	5,2	5,2
[A.9] [Re-]encaminamiento de mensajes			5,1	5,1
[A.10] Alteración de secuencia		5,1		5,1
[A.11] Acceso no autorizado		5,2	6,4	5,8
[A.12] Análisis de tráfico			3,9	3,9
[A.14] Interceptación de información (escucha)			5,2	5,2
[A.15] Modificación de la información		5,2		5,2
[A.18] Destrucción de la información	6,4			6,4
[A.24] Denegación de servicio	7,4			7,4
RED LAN	7,4	5,6	6,4	6,5
[I.8] Fallo de servicios de comunicación	6,3			6,3
[E.2] Errores del administrador del sistema	5,6	5,6	5,6	5,6
[E.9] Errores de [re-]encaminamiento			5,1	5,1
[E.10] Errores de secuencia		5,1		5,1
[E.15] Alteración de la información		3,4		3,4
[E.19] Fugas de información			5,1	5,1
[E.24] Caída del sistema por agotamiento de recursos	6,4			6,4
[A.5] Suplantación de la identidad		5,2	6,4	5,8
[A.7] Uso no previsto	5,2	5,2	5,2	5,2
[A.9] [Re-]encaminamiento de mensajes			5,1	5,1
[A.10] Alteración de secuencia		5,1		5,1
[A.11] Acceso no autorizado		5,2	6,4	5,8
[A.12] Análisis de tráfico			3,9	3,9
[A.14] Interceptación de información (escucha)			5,2	5,2
[A.15] Modificación de la información		5,2		5,2
[A.18] Destrucción de la información	6,4			6,4
[A.24] Denegación de servicio	7,4			7,4

RED TELEFÓNICA	7,4	5,6	6,4	6,5
[I.8] Fallo de servicios de comunicación	6,3			6,3
[E.2] Errores del administrador del sistema	5,6	5,6	5,6	5,6
[E.9] Errores de [re-]encaminamiento			5,1	5,1
[E.10] Errores de secuencia		5,1		5,1
[E.15] Alteración de la información		3,4		3,4
[E.19] Fugas de información			5,1	5,1
[E.24] Caída del sistema por agotamiento de recursos	6,4			6,4
[A.5] Suplantación de la identidad		5,2	6,4	5,8
[A.7] Uso no previsto	5,2	5,2	5,2	5,2
[A.9] [Re-]encaminamiento de mensajes			5,1	5,1
[A.10] Alteración de secuencia		5,1		5,1
[A.11] Acceso no autorizado		5,2	6,4	5,8
[A.12] Análisis de tráfico			3,9	3,9
[A.14] Interceptación de información (escucha)			5,2	5,2
[A.15] Modificación de la información		5,2		5,2
[A.18] Destrucción de la información	6,4			6,4
[A.24] Denegación de servicio	7,4			7,4
ELEMENTOS AUXILIARES	6,6	3,5	6,3	5,5
UPS	6,6	3,5	6,3	5,5
[N.1] Fuego	6			6
[N.2] Daños por agua	5,4			5,4
[N.*] Desastres naturales	6			6
[I.1] Fuego	6,6			6,6
[I.2] Daños por agua	6,1			6,1
[I.*] Desastres industriales	6,6			6,6
[I.3] Contaminación medioambiental	5,4			5,4
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1			5,1
[A.7] Uso no previsto	6,5	3,5	3,5	4,5
[A.23] Manipulación de hardware	6,3		6,3	6,3
[A.25] Robo de equipos	4,8			4,8
[A.26] Ataques destructivos	5			5
GENERADOR ELÉCTRICO	6,6	3,5	6,3	5,5
[N.1] Fuego	6			6
[N.2] Daños por agua	5,4			5,4
[N.*] Desastres naturales	6			6
[I.1] Fuego	6,6			6,6

[I.2] Daños por agua	6,1			6,1
[I.*] Desastres industriales	6,6			6,6
[I.3] Contaminación medioambiental	5,4			5,4
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1			5,1
[A.7] Uso no previsto	6,5	3,5	3,5	4,5
[A.23] Manipulación de hardware	6,3		6,3	6,3
[A.25] Robo de equipos	4,8			4,8
[A.26] Ataques destructivos	5			5
EQUIPOS DE CLIMATIZACIÓN	6,6	3,5	6,3	5,5
[N.1] Fuego	6			6
[N.2] Daños por agua	5,4			5,4
[N.*] Desastres naturales	6			6
[I.1] Fuego	6,6			6,6
[I.2] Daños por agua	6,1			6,1
[I.*] Desastres industriales	6,6			6,6
[I.3] Contaminación medioambiental	5,4			5,4
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1			5,1
[A.7] Uso no previsto	6,5	3,5	3,5	4,5
[A.23] Manipulación de hardware	6,3		6,3	6,3
[A.25] Robo de equipos	4,8			4,8
[A.26] Ataques destructivos	5			5
MOBILIARIO	6,6	3,5	6,3	5,5
[N.1] Fuego	6			6
[N.2] Daños por agua	5,4			5,4
[N.*] Desastres naturales	6			6
[I.1] Fuego	6,6			6,6
[I.2] Daños por agua	6,1			6,1
[I.*] Desastres industriales	6,6			6,6
[I.3] Contaminación medioambiental	5,4			5,4
[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1			5,1
[A.7] Uso no previsto	6,5	3,5	3,5	4,5
[A.23] Manipulación de hardware	6,3		6,3	6,3
[A.25] Robo de equipos	4,8			4,8
[A.26] Ataques destructivos	5			5
SERVICIOS	7,4	7,5	6,4	7
TELEFONÍA	6,5	6,4	5,1	6
[E.15] Alteración de la información		5,1		5,1
[E.18] Destrucción de la información	5,1			5,1

[E.19] Fugas de información			5,1	5,1
[A.15] Modificación de la información		6,4		6,4
[A.18] Destrucción de la información	6,4			6,4
[A.24] Denegación de servicio	6,5			6,5
INTERNET	6,5	6,4	6,3	6,4
[E.15] Alteración de la información		5,1		5,1
[E.18] Destrucción de la información	5,1			5,1
[E.19] Fugas de información			5,1	5,1
[A.5] Suplantación de la identidad		6,3	6,3	6,3
[A.15] Modificación de la información		6,4		6,4
[A.18] Destrucción de la información	6,4			6,4
[A.24] Denegación de servicio	6,5			6,5
ELECTRICIDAD	6,3	5,1		5,7
[I.9] Interrupción de otros servicios o suministros esenciales	6,3			6,3
[E.15] Alteración de la información		5,1		5,1
[E.18] Destrucción de la información	5,1			5,1
CORREO INSTITUCIONAL	7,4	7,3	6,4	7,0
[E.1] Errores de los usuarios	5,1	5,1	5,1	5,1
[E.2] Errores del administrador del sistema	5,6	5,6	5,6	5,6
[E.15] Alteración de la información		3,4		3,4
[E.18] Destrucción de la información	5,1			5,1
[E.19] Fugas de información			5,1	5,1
[E.24] Caída del sistema por agotamiento de recursos	7,2			7,2
[A.5] Suplantación de la identidad		6,4	6,4	6,4
[A.6] Abuso de privilegios de acceso	3,5	5,2	5,2	4,6
[A.7] Uso no previsto	3,5	5,2	5,2	4,6
[A.11] Acceso no autorizado		5,2	6,4	5,8
[A.15] Modificación de la información		7,3		7,3
[A.18] Destrucción de la información	6,4			6,4
[A.24] Denegación de servicio	7,4			7,4
SOPORTE DE RED	6,9	7,5	6,4	7
[E.1] Errores de los usuarios	3,4	4,6	5,1	4,4
[E.15] Alteración de la información		3,4		3,4
[E.18] Destrucción de la información	6,9			6,9
[E.19] Fugas de información			5,1	5,1
[A.7] Uso no previsto	3,5		3,5	3,5
[A.11] Acceso no autorizado		3,4	6,4	4,9
[A.15] Modificación de la información		7,5		7,5
[A.18] Destrucción de la información	6,9			6,9
SOPORTE A LOS SERVICIOS INFORMÁTICOS	7,4	7,3	5,2	7

[E.1] Errores de los usuarios	5,1	5,1	3,9	4,7
[E.2] Errores del administrador del sistema	5,6	5,6	4,4	5,2
[E.15] Alteración de la información		3,4		3,4
[E.18] Destrucción de la información	5,1			5,1
[E.19] Fugas de información			3,9	3,9
[E.24] Caída del sistema por agotamiento de recursos	7,2			7,2
[A.5] Suplantación de la identidad		6,4	5,2	5,8
[A.6] Abuso de privilegios de acceso	3,5	5,2	4,1	4,3
[A.7] Uso no previsto	3,5	5,2	4,1	4,3
[A.11] Acceso no autorizado		5,2	5,2	5,2
[A.15] Modificación de la información		7,3		7,3
[A.18] Destrucción de la información	6,4			6,4
[A.24] Denegación de servicio	7,4			7,4
MANTENIMIENTO DE EQUIPOS	6,5	6,4	6,4	6,4
[I.9] Interrupción de otros servicios o suministros esenciales	6,3			6,3
[E.15] Alteración de la información		5,1		5,1
[E.18] Destrucción de la información	5,1			5,1
[E.19] Fugas de información			5,1	5,1
[A.5] Suplantación de la identidad		6,3	6,3	6,3
[A.15] Modificación de la información		6,4		6,4
[A.18] Destrucción de la información	6,4			6,4
[A.19] Revelación de información			6,4	6,4
[A.24] Denegación de servicio	6,5			6,5
INFRAESTRUCTURA	6,9		7,7	7,3
INSTALACIÓN DE RED DE DATOS	6,9		7,7	7,3
[N.1] Fuego	6,9			6,9
[N.2] Daños por agua	6,9			6,9
[N.*] Desastres naturales	6,6			6,6
[I.1] Fuego	6,9			6,9
[I.2] Daños por agua	6,9			6,9
[I.*] Desastres industriales	6,9			6,9
[I.3] Contaminación medioambiental	5,1			5,1
[I.4] Contaminación electromagnética	4,2			4,2
[E.25] Pérdida de equipos			6	6
[A.6] Abuso de privilegios de acceso	5,2			5,2
[A.7] Uso no previsto	5,2			5,2
[A.25] Robo de equipos			7,7	7,7
[A.26] Ataques destructivos	5,9			5,9
[A.27] Ocupación enemiga	6,8			6,8
INSTALACIÓN DE RED ELÉCTRICA	6,9		7,7	7,3

[N.1] Fuego	6,9		6,9
[N.2] Daños por agua	6,9		6,9
[N.*] Desastres naturales	6,6		6,6
[I.1] Fuego	6,9		6,9
[I.2] Daños por agua	6,9		6,9
[I.*] Desastres industriales	6,9		6,9
[I.3] Contaminación medioambiental	5,1		5,1
[I.4] Contaminación electromagnética	4,2		4,2
[E.25] Pérdida de equipos		6	6
[A.6] Abuso de privilegios de acceso	5,2		5,2
[A.7] Uso no previsto	5,2		5,2
[A.25] Robo de equipos		7,7	7,7
[A.26] Ataques destructivos	5,9		5,9
[A.27] Ocupación enemiga	6,8		6,8
UPS DEL CENTRO CABLEADO	6,9	7,7	7,3
[N.1] Fuego	6,9		6,9
[N.2] Daños por agua	6,9		6,9
[N.*] Desastres naturales	6,6		6,6
[I.1] Fuego	6,9		6,9
[I.2] Daños por agua	6,9		6,9
[I.*] Desastres industriales	6,9		6,9
[I.3] Contaminación medioambiental	5,1		5,1
[I.4] Contaminación electromagnética	4,2		4,2
[E.25] Pérdida de equipos		6	6
[A.6] Abuso de privilegios de acceso	5,2		5,2
[A.7] Uso no previsto	5,2		5,2
[A.25] Robo de equipos		7,7	7,7
[A.26] Ataques destructivos	5,9		5,9
[A.27] Ocupación enemiga	6,8		6,8
ESPACIO FÍSICO DDTI	6,9	7,7	7,3
[N.1] Fuego	6,9		6,9
[N.2] Daños por agua	6,9		6,9
[N.*] Desastres naturales	6,6		6,6
[I.1] Fuego	6,9		6,9
[I.2] Daños por agua	6,9		6,9
[I.*] Desastres industriales	6,9		6,9
[I.3] Contaminación medioambiental	5,1		5,1
[I.4] Contaminación electromagnética	4,2		4,2
[E.25] Pérdida de equipos		6	6
[A.6] Abuso de privilegios de acceso	5,2		5,2
[A.7] Uso no previsto	5,2		5,2
[A.25] Robo de equipos		7,7	7,7
[A.26] Ataques destructivos	5,9		5,9

[A.27] Ocupación enemiga	6,8			6,8
PERSONAL	5,2	6,4	6,4	6
PERSONAL ADMINISTRATIVO	5,2	6,4	6,4	6
[E.15] Alteración de la información		5,1		5,1
[E.18] Destrucción de la información	3,4			3,4
[E.19] Fugas de información			5,1	5,1
[A.15] Modificación de la información		6,4		6,4
[A.18] Destrucción de la información	5,2			5,2
[A.19] Revelación de información			6,4	6,4
[A.28] Indisponibilidad del personal	4,8			4,8
[A.29] Extorsión	5,1	5,1	6,3	5,5
[A.30] Ingeniería social (picaresca)	4,9	4,9	6,1	5,3
PERSONAL DE DESARROLLO	5,2	6,4	6,4	6
[E.15] Alteración de la información		5,1		5,1
[E.18] Destrucción de la información	3,4			3,4
[E.19] Fugas de información			5,1	5,1
[A.15] Modificación de la información		6,4		6,4
[A.18] Destrucción de la información	5,2			5,2
[A.19] Revelación de información			6,4	6,4
[A.28] Indisponibilidad del personal	4,8			4,8
[A.29] Extorsión	5,1	5,1	6,3	5,5
[A.30] Ingeniería social (picaresca)	4,9	4,9	6,1	5,3

Nota: Elaboración propia

Anexo 7: Matriz de tratamiento de riesgos

ACTIVOS	AMENAZAS	PESO PONDERADO	ACCIÓN
INSTALACIÓN DE RED DE DATOS	[A.25] Robo de equipos	7,7	Evitar
INSTALACIÓN DE RED ELÉCTRICA	[A.25] Robo de equipos	7,7	Evitar
UPS DEL CENTRO CABLEADO	[A.25] Robo de equipos	7,7	Evitar
ESPACIO FÍSICO DDTI	[A.25] Robo de equipos	7,7	Evitar
ARCHIVO DE DATOS	[A.11] Acceso no autorizado	7,6	Reducir
BASE DE DATOS	[A.11] Acceso no autorizado	7,6	Reducir
DOCUMENTACIÓN INTERNA	[A.11] Acceso no autorizado	7,6	Reducir
CARPETAS COMPARTIDAS	[A.11] Acceso no autorizado	7,6	Reducir

SOPORTE DE RED	[A.15] Modificación de la información	7,5	Evitar
MATERIAL IMPRESO	[A.15] Modificación de la información	7,5	Evitar
ETHERNET	[A.24] Denegación de servicio	7,4	Evitar
RED INALAMBRICA	[A.24] Denegación de servicio	7,4	Evitar
RED LAN	[A.24] Denegación de servicio	7,4	Evitar
RED TELEFÓNICA	[A.24] Denegación de servicio	7,4	Evitar
CORREO INSTITUCIONAL	[A.24] Denegación de servicio	7,4	Evitar
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[A.24] Denegación de servicio	7,4	Evitar
DISPOSITIVOS DE ALMACENAMIENTO	[A.24] Denegación de servicio	7,3	Evitar
COMPUTADORAS	[A.24] Denegación de servicio	7,3	Evitar
TELÉFONOS IP	[A.24] Denegación de servicio	7,3	Evitar
SERVIDORES	[A.24] Denegación de servicio	7,3	Evitar
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[A.24] Denegación de servicio	7,3	Evitar
EQUIPO MULTIFUNCIONAL	[A.24] Denegación de servicio	7,3	Evitar
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[A.24] Denegación de servicio	7,3	Evitar
RADIOS DE COMUNICACIÓN	[A.24] Denegación de servicio	7,3	Evitar
CORREO INSTITUCIONAL	[A.15] Modificación de la información	7,3	Evitar
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[A.15] Modificación de la información	7,3	Evitar
DISPOSITIVOS DE ALMACENAMIENTO	[E.24] Caída del sistema por agotamiento de recursos	7,2	Reducir
COMPUTADORAS	[E.24] Caída del sistema por agotamiento de recursos	7,2	Reducir
TELÉFONOS IP	[E.24] Caída del sistema por agotamiento de recursos	7,2	Reducir
SERVIDORES	[E.24] Caída del sistema por agotamiento de recursos	7,2	Reducir
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[E.24] Caída del sistema por agotamiento de recursos	7,2	Reducir
EQUIPO MULTIFUNCIONAL	[E.24] Caída del sistema por agotamiento de recursos	7,2	Reducir

DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[E.24] Caída del sistema por agotamiento de recursos	7,2	Reducir
RADIOS DE COMUNICACIÓN	[E.24] Caída del sistema por agotamiento de recursos	7,2	Reducir
CORREO INSTITUCIONAL	[E.24] Caída del sistema por agotamiento de recursos	7,2	Reducir
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[E.24] Caída del sistema por agotamiento de recursos	7,2	Reducir
MOTOR DE BASE DE DATOS	[A.8] Difusión de software dañino	6,9	Evitar
REPOSITORIO DE APLICACIONES DESARROLLADAS	[A.8] Difusión de software dañino	6,9	Evitar
ANTIVIRUS	[A.8] Difusión de software dañino	6,9	Evitar
FIREWALL	[A.8] Difusión de software dañino	6,9	Evitar
LICENCIAS	[A.8] Difusión de software dañino	6,9	Evitar
NAVEGADORES	[A.8] Difusión de software dañino	6,9	Evitar
SISTEMAS OPERATIVOS	[A.8] Difusión de software dañino	6,9	Evitar
SOPORTE DE RED	[E.18] Destrucción de la información	6,9	Reducir
SOPORTE DE RED	[A.18] Destrucción de la información	6,9	Evitar
DISPOSITIVOS DE ALMACENAMIENTO	[I.6] Corte del suministro eléctrico	6,9	Reducir
DISPOSITIVOS DE ALMACENAMIENTO	[I.7] Condiciones inadecuadas de temperatura o humedad	6,9	Reducir
COMPUTADORAS	[I.6] Corte del suministro eléctrico	6,9	Reducir
COMPUTADORAS	[I.7] Condiciones inadecuadas de temperatura o humedad	6,9	Reducir
TELÉFONOS IP	[I.6] Corte del suministro eléctrico	6,9	Reducir
TELÉFONOS IP	[I.7] Condiciones inadecuadas de temperatura o humedad	6,9	Reducir
SERVIDORES	[I.6] Corte del suministro eléctrico	6,9	Reducir
SERVIDORES	[I.7] Condiciones inadecuadas de temperatura o humedad	6,9	Reducir
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[I.6] Corte del suministro eléctrico	6,9	Reducir
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[I.7] Condiciones inadecuadas de temperatura o humedad	6,9	Reducir

EQUIPO MULTIFUNCIONAL	[I.6] Corte del suministro eléctrico	6,9	Reducir
EQUIPO MULTIFUNCIONAL	[I.7] Condiciones inadecuadas de temperatura o humedad	6,9	Reducir
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[I.6] Corte del suministro eléctrico	6,9	Reducir
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[I.7] Condiciones inadecuadas de temperatura o humedad	6,9	Reducir
RADIOS DE COMUNICACIÓN	[I.6] Corte del suministro eléctrico	6,9	Reducir
RADIOS DE COMUNICACIÓN	[I.7] Condiciones inadecuadas de temperatura o humedad	6,9	Reducir
INSTALACIÓN DE RED DE DATOS	[N.1] Fuego	6,9	Reducir
INSTALACIÓN DE RED DE DATOS	[N.2] Daños por agua	6,9	Reducir
INSTALACIÓN DE RED DE DATOS	[I.1] Fuego	6,9	Reducir
INSTALACIÓN DE RED DE DATOS	[I.2] Daños por agua	6,9	Reducir
INSTALACIÓN DE RED DE DATOS	[I.*] Desastres industriales	6,9	Reducir
INSTALACIÓN DE RED ELÉCTRICA	[N.1] Fuego	6,9	Reducir
INSTALACIÓN DE RED ELÉCTRICA	[N.2] Daños por agua	6,9	Reducir
INSTALACIÓN DE RED ELÉCTRICA	[I.1] Fuego	6,9	Reducir
INSTALACIÓN DE RED ELÉCTRICA	[I.2] Daños por agua	6,9	Reducir
INSTALACIÓN DE RED ELÉCTRICA	[I.*] Desastres industriales	6,9	Reducir
UPS DEL CENTRO CABLEADO	[N.1] Fuego	6,9	Reducir
UPS DEL CENTRO CABLEADO	[N.2] Daños por agua	6,9	Reducir
UPS DEL CENTRO CABLEADO	[I.1] Fuego	6,9	Reducir
UPS DEL CENTRO CABLEADO	[I.2] Daños por agua	6,9	Reducir
UPS DEL CENTRO CABLEADO	[I.*] Desastres industriales	6,9	Reducir
ESPACIO FÍSICO DDTI	[N.1] Fuego	6,9	Reducir
ESPACIO FÍSICO DDTI	[N.2] Daños por agua	6,9	Reducir
ESPACIO FÍSICO DDTI	[I.1] Fuego	6,9	Reducir
ESPACIO FÍSICO DDTI	[I.2] Daños por agua	6,9	Reducir
ESPACIO FÍSICO DDTI	[I.*] Desastres industriales	6,9	Reducir

MATERIAL IMPRESO	[I.7] Condiciones inadecuadas de temperatura o humedad	6,9	Reducir
MATERIAL IMPRESO	[E.18] Destrucción de la información	6,9	Reducir
MATERIAL IMPRESO	[A.18] Destrucción de la información	6,9	Evitar
MOTOR DE BASE DE DATOS	[A.22] Manipulación de programas	6,8	Evitar
REPOSITORIO DE APLICACIONES DESARROLLADAS	[A.22] Manipulación de programas	6,8	Evitar
ANTIVIRUS	[A.22] Manipulación de programas	6,8	Evitar
FIREWALL	[A.22] Manipulación de programas	6,8	Evitar
LICENCIAS	[A.22] Manipulación de programas	6,8	Evitar
NAVEGADORES	[A.22] Manipulación de programas	6,8	Evitar
SISTEMAS OPERATIVOS	[A.22] Manipulación de programas	6,8	Evitar
DISPOSITIVOS DE ALMACENAMIENTO	[A.26] Ataques destructivos	6,8	Evitar
COMPUTADORAS	[A.26] Ataques destructivos	6,8	Evitar
TELÉFONOS IP	[A.26] Ataques destructivos	6,8	Evitar
SERVIDORES	[A.26] Ataques destructivos	6,8	Evitar
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[A.26] Ataques destructivos	6,8	Evitar
EQUIPO MULTIFUNCIONAL	[A.26] Ataques destructivos	6,8	Evitar
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[A.26] Ataques destructivos	6,8	Evitar
RADIOS DE COMUNICACIÓN	[A.26] Ataques destructivos	6,8	Evitar
INSTALACIÓN DE RED DE DATOS	[A.27] Ocupación enemiga	6,8	Evitar
INSTALACIÓN DE RED ELÉCTRICA	[A.27] Ocupación enemiga	6,8	Evitar
UPS DEL CENTRO CABLEADO	[A.27] Ocupación enemiga	6,8	Evitar
ESPACIO FÍSICO DDTI	[A.27] Ocupación enemiga	6,8	Evitar
BASE DE DATOS	[A.5] Suplantación de la identidad	6,7	Evitar
FIREWALL	[A.5] Suplantación de la identidad	6,7	Evitar

ARCHIVO DE DATOS	[A.5] Suplantación de la identidad	6,7	Evitar
DOCUMENTACIÓN INTERNA	[A.5] Suplantación de la identidad	6,7	Evitar
CARPETAS COMPARTIDAS	[A.5] Suplantación de la identidad	6,7	Evitar
DISPOSITIVOS DE ALMACENAMIENTO	[E.25] Pérdida de equipos	6,7	Reducir
COMPUTADORAS	[E.25] Pérdida de equipos	6,7	Reducir
TELÉFONOS IP	[E.25] Pérdida de equipos	6,7	Reducir
SERVIDORES	[E.25] Pérdida de equipos	6,7	Reducir
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[E.25] Pérdida de equipos	6,7	Reducir
EQUIPO MULTIFUNCIONAL	[E.25] Pérdida de equipos	6,7	Reducir
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[E.25] Pérdida de equipos	6,7	Reducir
RADIOS DE COMUNICACIÓN	[E.25] Pérdida de equipos	6,7	Reducir
MATERIAL IMPRESO	[I.1] Fuego	6,6	Reducir
MATERIAL IMPRESO	[I.*] Desastres industriales	6,6	Reducir
DISPOSITIVOS DE ALMACENAMIENTO	[I.1] Fuego	6,6	Reducir
DISPOSITIVOS DE ALMACENAMIENTO	[I.*] Desastres industriales	6,6	Reducir
COMPUTADORAS	[I.1] Fuego	6,6	Reducir
COMPUTADORAS	[I.*] Desastres industriales	6,6	Reducir
TELÉFONOS IP	[I.1] Fuego	6,6	Reducir
TELÉFONOS IP	[I.*] Desastres industriales	6,6	Reducir
SERVIDORES	[I.1] Fuego	6,6	Reducir
SERVIDORES	[I.*] Desastres industriales	6,6	Reducir
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[I.1] Fuego	6,6	Reducir
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[I.*] Desastres industriales	6,6	Reducir
EQUIPO MULTIFUNCIONAL	[I.1] Fuego	6,6	Reducir
EQUIPO MULTIFUNCIONAL	[I.*] Desastres industriales	6,6	Reducir
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[I.1] Fuego	6,6	Reducir

DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[I.*] Desastres industriales	6,6	Reducir
RADIOS DE COMUNICACIÓN	[I.1] Fuego	6,6	Reducir
RADIOS DE COMUNICACIÓN	[I.*] Desastres industriales	6,6	Reducir
UPS	[I.1] Fuego	6,6	Reducir
UPS	[I.*] Desastres industriales	6,6	Reducir
GENERADOR ELÉCTRICO	[I.1] Fuego	6,6	Reducir
GENERADOR ELÉCTRICO	[I.*] Desastres industriales	6,6	Reducir
EQUIPOS DE CLIMATIZACIÓN	[I.1] Fuego	6,6	Reducir
EQUIPOS DE CLIMATIZACIÓN	[I.*] Desastres industriales	6,6	Reducir
MOBILIARIO	[I.1] Fuego	6,6	Reducir
MOBILIARIO	[I.*] Desastres industriales	6,6	Reducir
INSTALACIÓN DE RED DE DATOS	[N.*] Desastres naturales	6,6	Reducir
INSTALACIÓN DE RED ELÉCTRICA	[N.*] Desastres naturales	6,6	Reducir
UPS DEL CENTRO CABLEADO	[N.*] Desastres naturales	6,6	Reducir
ESPACIO FÍSICO DDTI	[N.*] Desastres naturales	6,6	Reducir
MANTENIMIENTO DE EQUIPOS	[A.24] Denegación de servicio	6,5	Evitar
TELEFONÍA	[A.24] Denegación de servicio	6,5	Evitar
INTERNET	[A.24] Denegación de servicio	6,5	Evitar
ETHERNET	[E.24] Caída del sistema por agotamiento de recursos	6,4	Reducir
ETHERNET	[A.18] Destrucción de la información	6,4	Evitar
RED INALAMBRICA	[E.24] Caída del sistema por agotamiento de recursos	6,4	Reducir
RED INALAMBRICA	[A.18] Destrucción de la información	6,4	Evitar
RED LAN	[E.24] Caída del sistema por agotamiento de recursos	6,4	Reducir
RED LAN	[A.18] Destrucción de la información	6,4	Evitar
RED TELEFÓNICA	[E.24] Caída del sistema por agotamiento de recursos	6,4	Reducir
RED TELEFÓNICA	[A.18] Destrucción de la información	6,4	Evitar
TELEFONÍA	[A.15] Modificación de la información	6,4	Evitar

CORREO INSTITUCIONAL	[A.5] Suplantación de la identidad	6,4	Evitar
CORREO INSTITUCIONAL	[A.18] Destrucción de la información	6,4	Evitar
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[A.18] Destrucción de la información	6,4	Evitar
MANTENIMIENTO DE EQUIPOS	[A.18] Destrucción de la información	6,4	Evitar
PERSONAL ADMINISTRATIVO	[A.15] Modificación de la información	6,4	Evitar
PERSONAL ADMINISTRATIVO	[A.19] Revelación de información	6,4	Evitar
PERSONAL DE DESARROLLO	[A.15] Modificación de la información	6,4	Evitar
PERSONAL DE DESARROLLO	[A.19] Revelación de información	6,4	Evitar
TELEFONÍA	[A.18] Destrucción de la información	6,4	Evitar
INTERNET	[A.15] Modificación de la información	6,4	Evitar
INTERNET	[A.18] Destrucción de la información	6,4	Evitar
MANTENIMIENTO DE EQUIPOS	[A.15] Modificación de la información	6,4	Evitar
MANTENIMIENTO DE EQUIPOS	[A.19] Revelación de información	6,4	Evitar
MANTENIMIENTO DE EQUIPOS	[I.9] Interrupción de otros servicios o suministros esenciales	6,3	Reducir
INTERNET	[A.5] Suplantación de la identidad	6,3	Evitar
MATERIAL IMPRESO	[I.3] Contaminación medioambiental	6,3	Reducir
MOTOR DE BASE DE DATOS	[I.5.1] Avería de origen lógico	6,3	Reducir
REPOSITORIO DE APLICACIONES DESARROLLADAS	[I.5.1] Avería de origen lógico	6,3	Reducir
ANTIVIRUS	[I.5.1] Avería de origen lógico	6,3	Reducir
FIREWALL	[I.5.1] Avería de origen lógico	6,3	Reducir
LICENCIAS	[I.5.1] Avería de origen lógico	6,3	Reducir
NAVEGADORES	[I.5.1] Avería de origen lógico	6,3	Reducir
SISTEMAS OPERATIVOS	[I.5.1] Avería de origen lógico	6,3	Reducir
DISPOSITIVOS DE ALMACENAMIENTO	[I.5.2] Avería de origen físico	6,3	Reducir
COMPUTADORAS	[I.5.2] Avería de origen físico	6,3	Reducir

TELÉFONOS IP	[I.5.2] Avería de origen físico	6,3	Reducir
SERVIDORES	[I.5.2] Avería de origen físico	6,3	Reducir
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[I.5.2] Avería de origen físico	6,3	Reducir
EQUIPO MULTIFUNCIONAL	[I.5.2] Avería de origen físico	6,3	Reducir
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[I.5.2] Avería de origen físico	6,3	Reducir
RADIOS DE COMUNICACIÓN	[I.5.2] Avería de origen físico	6,3	Reducir
ETHERNET	[I.8] Fallo de servicios de comunicación	6,3	Reducir
RED INALAMBRICA	[I.8] Fallo de servicios de comunicación	6,3	Reducir
RED LAN	[I.8] Fallo de servicios de comunicación	6,3	Reducir
RED TELEFÓNICA	[I.8] Fallo de servicios de comunicación	6,3	Reducir
UPS	[A.23] Manipulación de hardware	6,3	Evitar
GENERADOR ELÉCTRICO	[A.23] Manipulación de hardware	6,3	Evitar
EQUIPOS DE CLIMATIZACIÓN	[A.23] Manipulación de hardware	6,3	Evitar
MOBILIARIO	[A.23] Manipulación de hardware	6,3	Evitar
ELECTRICIDAD	[I.9] Interrupción de otros servicios o suministros esenciales	6,3	Reducir
MANTENIMIENTO DE EQUIPOS	[A.5] Suplantación de la identidad	6,3	Evitar
DISPOSITIVOS DE ALMACENAMIENTO	[A.25] Robo de equipos	6,3	Evitar
COMPUTADORAS	[A.25] Robo de equipos	6,3	Evitar
TELÉFONOS IP	[A.25] Robo de equipos	6,3	Evitar
SERVIDORES	[A.25] Robo de equipos	6,3	Evitar
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[A.25] Robo de equipos	6,25	Evitar
EQUIPO MULTIFUNCIONAL	[A.25] Robo de equipos	6,3	Evitar
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[A.25] Robo de equipos	6,3	Evitar
RADIOS DE COMUNICACIÓN	[A.25] Robo de equipos	6,3	Evitar
MATERIAL IMPRESO	[I.2] Daños por agua	6,1	Reducir

DISPOSITIVOS DE ALMACENAMIENTO	[I.2] Daños por agua	6,1	Reducir
COMPUTADORAS	[I.2] Daños por agua	6,1	Reducir
TELÉFONOS IP	[I.2] Daños por agua	6,1	Reducir
SERVIDORES	[I.2] Daños por agua	6,1	Reducir
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[I.2] Daños por agua	6,1	Reducir
EQUIPO MULTIFUNCIONAL	[I.2] Daños por agua	6,1	Reducir
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[I.2] Daños por agua	6,1	Reducir
RADIOS DE COMUNICACIÓN	[I.2] Daños por agua	6,1	Reducir
UPS	[I.2] Daños por agua	6,1	Reducir
GENERADOR ELÉCTRICO	[I.2] Daños por agua	6,1	Reducir
EQUIPOS DE CLIMATIZACIÓN	[I.2] Daños por agua	6,1	Reducir
MOBILIARIO	[I.2] Daños por agua	6,1	Reducir
MATERIAL IMPRESO	[N.1] Fuego	6	Reducir
MATERIAL IMPRESO	[N.*] Desastres naturales	6	Reducir
DISPOSITIVOS DE ALMACENAMIENTO	[N.1] Fuego	6	Reducir
DISPOSITIVOS DE ALMACENAMIENTO	[N.*] Desastres naturales	6	Reducir
DISPOSITIVOS DE ALMACENAMIENTO	[A.23] Manipulación de hardware	6	Evitar
COMPUTADORAS	[N.1] Fuego	6	Reducir
COMPUTADORAS	[N.*] Desastres naturales	6	Reducir
COMPUTADORAS	[A.23] Manipulación de hardware	6	Evitar
TELÉFONOS IP	[N.1] Fuego	6	Reducir
TELÉFONOS IP	[N.*] Desastres naturales	6	Reducir
TELÉFONOS IP	[A.23] Manipulación de hardware	6	Evitar
SERVIDORES	[N.1] Fuego	6	Reducir
SERVIDORES	[N.*] Desastres naturales	6	Reducir
SERVIDORES	[A.23] Manipulación de hardware	6	Evitar
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[N.1] Fuego	6	Reducir
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[N.*] Desastres naturales	6	Reducir
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[A.23] Manipulación de hardware	6	Evitar

EQUIPO MULTIFUNCIONAL	[N.1] Fuego	6	Reducir
EQUIPO MULTIFUNCIONAL	[N.*] Desastres naturales	6	Reducir
EQUIPO MULTIFUNCIONAL	[A.23] Manipulación de hardware	6	Evitar
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[N.1] Fuego	6	Reducir
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[N.*] Desastres naturales	6	Reducir
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[A.23] Manipulación de hardware	6	Evitar
RADIOS DE COMUNICACIÓN	[N.1] Fuego	6	Reducir
RADIOS DE COMUNICACIÓN	[N.*] Desastres naturales	6	Reducir
RADIOS DE COMUNICACIÓN	[A.23] Manipulación de hardware	6	Evitar
UPS	[N.1] Fuego	6	Reducir
UPS	[N.*] Desastres naturales	6	Reducir
GENERADOR ELÉCTRICO	[N.1] Fuego	6	Reducir
GENERADOR ELÉCTRICO	[N.*] Desastres naturales	6	Reducir
EQUIPOS DE CLIMATIZACIÓN	[N.1] Fuego	6	Reducir
EQUIPOS DE CLIMATIZACIÓN	[N.*] Desastres naturales	6	Reducir
MOBILIARIO	[N.1] Fuego	6	Reducir
MOBILIARIO	[N.*] Desastres naturales	6	Reducir
INSTALACIÓN DE RED DE DATOS	[E.25] Pérdida de equipos	6	Reducir
INSTALACIÓN DE RED ELÉCTRICA	[E.25] Pérdida de equipos	6	Reducir
UPS DEL CENTRO CABLEADO	[E.25] Pérdida de equipos	6	Reducir
ESPACIO FÍSICO DDTI	[E.25] Pérdida de equipos	6	Reducir
BASE DE DATOS	[A.6] Abuso de privilegios de acceso	6	Evitar
ARCHIVO DE DATOS	[A.6] Abuso de privilegios de acceso	6	Evitar
DOCUMENTACIÓN INTERNA	[A.6] Abuso de privilegios de acceso	6	Evitar
CARPETAS COMPARTIDAS	[A.6] Abuso de privilegios de acceso	6	Evitar

FIREWALL	[A.4] Manipulación de los ficheros de configuración	5,9	Evitar
INSTALACIÓN DE RED DE DATOS	[A.26] Ataques destructivos	5,9	Evitar
INSTALACIÓN DE RED ELÉCTRICA	[A.26] Ataques destructivos	5,9	Evitar
UPS DEL CENTRO CABLEADO	[A.26] Ataques destructivos	5,9	Evitar
ESPACIO FÍSICO DDTI	[A.26] Ataques destructivos	5,9	Evitar
ETHERNET	[A.5] Suplantación de la identidad	5,8	Evitar
ETHERNET	[A.11] Acceso no autorizado	5,8	Reducir
RED INALAMBRICA	[A.5] Suplantación de la identidad	5,8	Evitar
RED INALAMBRICA	[A.11] Acceso no autorizado	5,8	Reducir
RED LAN	[A.5] Suplantación de la identidad	5,8	Evitar
RED LAN	[A.11] Acceso no autorizado	5,8	Reducir
RED TELEFÓNICA	[A.5] Suplantación de la identidad	5,8	Evitar
RED TELEFÓNICA	[A.11] Acceso no autorizado	5,8	Reducir
CORREO INSTITUCIONAL	[A.11] Acceso no autorizado	5,8	Reducir
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[A.5] Suplantación de la identidad	5,8	Evitar
MOTOR DE BASE DE DATOS	[E.21] Errores de mantenimiento/actualización de programas (software)	5,8	Reducir
REPOSITORIO DE APLICACIONES DESARROLLADAS	[E.21] Errores de mantenimiento/actualización de programas (software)	5,8	Reducir
ANTIVIRUS	[E.21] Errores de mantenimiento/actualización de programas (software)	5,8	Reducir
FIREWALL	[E.21] Errores de mantenimiento/actualización de programas (software)	5,8	Reducir
LICENCIAS	[E.21] Errores de mantenimiento/actualización de programas (software)	5,8	Reducir
NAVEGADORES	[E.21] Errores de mantenimiento/actualización de programas (software)	5,8	Reducir
SISTEMAS OPERATIVOS	[E.21] Errores de mantenimiento/actualización de programas (software)	5,8	Reducir

DISPOSITIVOS DE ALMACENAMIENTO	[A.11] Acceso no autorizado	5,6	Reducir
COMPUTADORAS	[A.11] Acceso no autorizado	5,6	Reducir
TELÉFONOS IP	[A.11] Acceso no autorizado	5,6	Reducir
SERVIDORES	[A.11] Acceso no autorizado	5,6	Reducir
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[A.11] Acceso no autorizado	5,6	Reducir
EQUIPO MULTIFUNCIONAL	[A.11] Acceso no autorizado	5,6	Reducir
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[A.11] Acceso no autorizado	5,6	Reducir
RADIOS DE COMUNICACIÓN	[A.11] Acceso no autorizado	5,6	Reducir
ETHERNET	[E.2] Errores del administrador del sistema	5,6	Reducir
RED INALAMBRICA	[E.2] Errores del administrador del sistema	5,6	Reducir
RED LAN	[E.2] Errores del administrador del sistema	5,6	Reducir
RED TELEFÓNICA	[E.2] Errores del administrador del sistema	5,6	Reducir
CORREO INSTITUCIONAL	[E.2] Errores del administrador del sistema	5,6	Reducir
PERSONAL ADMINISTRATIVO	[A.29] Extorsión	5,5	Evitar
PERSONAL DE DESARROLLO	[A.29] Extorsión	5,5	Evitar
MATERIAL IMPRESO	[N.2] Daños por agua	5,4	Reducir
DISPOSITIVOS DE ALMACENAMIENTO	[N.2] Daños por agua	5,4	Reducir
DISPOSITIVOS DE ALMACENAMIENTO	[I.3] Contaminación medioambiental	5,4	Reducir
COMPUTADORAS	[N.2] Daños por agua	5,4	Reducir
COMPUTADORAS	[I.3] Contaminación medioambiental	5,4	Reducir
TELÉFONOS IP	[N.2] Daños por agua	5,4	Reducir
TELÉFONOS IP	[I.3] Contaminación medioambiental	5,4	Reducir
SERVIDORES	[N.2] Daños por agua	5,4	Reducir
SERVIDORES	[I.3] Contaminación medioambiental	5,4	Reducir
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[N.2] Daños por agua	5,4	Reducir

EQUIPO PARA EL FUNCIONAMIENTO DE RED	[I.3] Contaminación medioambiental	5,4	Reducir
EQUIPO MULTIFUNCIONAL	[N.2] Daños por agua	5,4	Reducir
EQUIPO MULTIFUNCIONAL	[I.3] Contaminación medioambiental	5,4	Reducir
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[N.2] Daños por agua	5,4	Reducir
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[I.3] Contaminación medioambiental	5,4	Reducir
RADIOS DE COMUNICACIÓN	[N.2] Daños por agua	5,4	Reducir
RADIOS DE COMUNICACIÓN	[I.3] Contaminación medioambiental	5,4	Reducir
UPS	[N.2] Daños por agua	5,4	Reducir
UPS	[I.3] Contaminación medioambiental	5,4	Reducir
GENERADOR ELÉCTRICO	[N.2] Daños por agua	5,4	Reducir
GENERADOR ELÉCTRICO	[I.3] Contaminación medioambiental	5,4	Reducir
EQUIPOS DE CLIMATIZACIÓN	[N.2] Daños por agua	5,4	Reducir
EQUIPOS DE CLIMATIZACIÓN	[I.3] Contaminación medioambiental	5,4	Reducir
MOBILIARIO	[N.2] Daños por agua	5,4	Reducir
MOBILIARIO	[I.3] Contaminación medioambiental	5,4	Reducir
PERSONAL ADMINISTRATIVO	[A.30] Ingeniería social (picaresca)	5,3	Evitar
PERSONAL DE DESARROLLO	[A.30] Ingeniería social (picaresca)	5,3	Evitar
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[A.11] Acceso no autorizado	5,2	Reducir
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[E.2] Errores del administrador del sistema	5,2	Reducir
ETHERNET	[A.7] Uso no previsto	5,2	Evitar
ETHERNET	[A.14] Interceptación de información (escucha)	5,2	Evitar
ETHERNET	[A.15] Modificación de la información	5,2	Evitar
RED INALAMBRICA	[A.7] Uso no previsto	5,2	Evitar

RED INALAMBRICA	[A.14] Interceptación de información (escucha)	5,2	Evitar
RED INALAMBRICA	[A.15] Modificación de la información	5,2	Evitar
RED LAN	[A.7] Uso no previsto	5,2	Evitar
RED LAN	[A.14] Interceptación de información (escucha)	5,2	Evitar
RED LAN	[A.15] Modificación de la información	5,2	Evitar
RED TELEFÓNICA	[A.7] Uso no previsto	5,2	Evitar
RED TELEFÓNICA	[A.14] Interceptación de información (escucha)	5,2	Evitar
RED TELEFÓNICA	[A.15] Modificación de la información	5,2	Evitar
INSTALACIÓN DE RED DE DATOS	[A.6] Abuso de privilegios de acceso	5,2	Evitar
INSTALACIÓN DE RED DE DATOS	[A.7] Uso no previsto	5,2	Evitar
INSTALACIÓN DE RED ELÉCTRICA	[A.6] Abuso de privilegios de acceso	5,2	Evitar
INSTALACIÓN DE RED ELÉCTRICA	[A.7] Uso no previsto	5,2	Evitar
UPS DEL CENTRO CABLEADO	[A.6] Abuso de privilegios de acceso	5,2	Evitar
UPS DEL CENTRO CABLEADO	[A.7] Uso no previsto	5,2	Evitar
ESPACIO FÍSICO DDTI	[A.6] Abuso de privilegios de acceso	5,2	Evitar
ESPACIO FÍSICO DDTI	[A.7] Uso no previsto	5,2	Evitar
PERSONAL ADMINISTRATIVO	[A.18] Destrucción de la información	5,2	Evitar
PERSONAL DE DESARROLLO	[A.18] Destrucción de la información	5,2	Evitar
TELEFONÍA	[E.15] Alteración de la información	5,1	Reducir
INTERNET	[E.15] Alteración de la información	5,1	Reducir
TELEFONÍA	[E.18] Destrucción de la información	5,1	Reducir
INTERNET	[E.18] Destrucción de la información	5,1	Reducir
MANTENIMIENTO DE EQUIPOS	[E.15] Alteración de la información	5,1	Reducir
TELEFONÍA	[E.19] Fugas de información	5,1	Reducir
INTERNET	[E.19] Fugas de información	5,1	Reducir
SOPORTE DE RED	[E.19] Fugas de información	5,1	Reducir

MANTENIMIENTO DE EQUIPOS	[E.18] Destrucción de la información	5,1	Reducir
ARCHIVO DE DATOS	[E.19] Fugas de información	5	Reducir
DOCUMENTACIÓN INTERNA	[E.19] Fugas de información	5	Reducir
CARPETAS COMPARTIDAS	[E.19] Fugas de información	5	Reducir
MANTENIMIENTO DE EQUIPOS	[E.19] Fugas de información	5,1	Reducir
BASE DE DATOS	[E.19] Fugas de información	5	Reducir
MATERIAL IMPRESO	[E.19] Fugas de información	5,1	Reducir
MOTOR DE BASE DE DATOS	[E.8] Difusión de software dañino	5,1	Reducir
REPOSITORIO DE APLICACIONES DESARROLLADAS	[E.8] Difusión de software dañino	5,1	Reducir
ANTIVIRUS	[E.8] Difusión de software dañino	5,1	Reducir
FIREWALL	[E.8] Difusión de software dañino	5,1	Reducir
LICENCIAS	[E.8] Difusión de software dañino	5,1	Reducir
NAVEGADORES	[E.8] Difusión de software dañino	5,1	Reducir
SISTEMAS OPERATIVOS	[E.8] Difusión de software dañino	5,1	Reducir
DISPOSITIVOS DE ALMACENAMIENTO	[I.4] Contaminación electromagnética	5,1	Reducir
DISPOSITIVOS DE ALMACENAMIENTO	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1	Reducir
COMPUTADORAS	[I.4] Contaminación electromagnética	5,1	Reducir
COMPUTADORAS	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1	Reducir
TELÉFONOS IP	[I.4] Contaminación electromagnética	5,1	Reducir
TELÉFONOS IP	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1	Reducir
SERVIDORES	[I.4] Contaminación electromagnética	5,1	Reducir
SERVIDORES	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1	Reducir
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[I.4] Contaminación electromagnética	5,1	Reducir
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1	Reducir

EQUIPO MULTIFUNCIONAL	[I.4] Contaminación electromagnética	5,1	Reducir
EQUIPO MULTIFUNCIONAL	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1	Reducir
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[I.4] Contaminación electromagnética	5,1	Reducir
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1	Reducir
RADIOS DE COMUNICACIÓN	[I.4] Contaminación electromagnética	5,1	Reducir
RADIOS DE COMUNICACIÓN	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1	Reducir
ETHERNET	[E.9] Errores de [re-]encaminamiento	5,1	Reducir
ETHERNET	[E.10] Errores de secuencia	5,1	Reducir
ETHERNET	[E.19] Fugas de información	5,1	Reducir
ETHERNET	[A.9] [Re-]encaminamiento de mensajes	5,1	Evitar
ETHERNET	[A.10] Alteración de secuencia	5,1	Evitar
RED INALAMBRICA	[E.9] Errores de [re-]encaminamiento	5,1	Reducir
RED INALAMBRICA	[E.10] Errores de secuencia	5,1	Reducir
RED INALAMBRICA	[E.19] Fugas de información	5,1	Reducir
RED INALAMBRICA	[A.9] [Re-]encaminamiento de mensajes	5,1	Evitar
RED INALAMBRICA	[A.10] Alteración de secuencia	5,1	Evitar
RED LAN	[E.9] Errores de [re-]encaminamiento	5,1	Reducir
RED LAN	[E.10] Errores de secuencia	5,1	Reducir
RED LAN	[E.19] Fugas de información	5,1	Reducir
RED LAN	[A.9] [Re-]encaminamiento de mensajes	5,1	Evitar
RED LAN	[A.10] Alteración de secuencia	5,1	Evitar
RED TELEFÓNICA	[E.9] Errores de [re-]encaminamiento	5,1	Reducir
RED TELEFÓNICA	[E.10] Errores de secuencia	5,1	Reducir
RED TELEFÓNICA	[E.19] Fugas de información	5,1	Reducir
RED TELEFÓNICA	[A.9] [Re-]encaminamiento de mensajes	5,1	Evitar
RED TELEFÓNICA	[A.10] Alteración de secuencia	5,1	Evitar
UPS	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1	Reducir

GENERADOR ELÉCTRICO	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1	Reducir
EQUIPOS DE CLIMATIZACIÓN	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1	Reducir
MOBILIARIO	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5,1	Reducir
ELECTRICIDAD	[E.15] Alteración de la información	5,1	Reducir
ELECTRICIDAD	[E.18] Destrucción de la información	5,1	Reducir
CORREO INSTITUCIONAL	[E.1] Errores de los usuarios	5,1	Reducir
CORREO INSTITUCIONAL	[E.18] Destrucción de la información	5,1	Reducir
CORREO INSTITUCIONAL	[E.19] Fugas de información	5,1	Reducir
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[E.18] Destrucción de la información	5,1	Reducir
INSTALACIÓN DE RED DE DATOS	[I.3] Contaminación medioambiental	5,1	Reducir
INSTALACIÓN DE RED ELÉCTRICA	[I.3] Contaminación medioambiental	5,1	Reducir
UPS DEL CENTRO CABLEADO	[I.3] Contaminación medioambiental	5,1	Reducir
ESPACIO FÍSICO DDTI	[I.3] Contaminación medioambiental	5,1	Reducir
PERSONAL ADMINISTRATIVO	[E.15] Alteración de la información	5,1	Reducir
PERSONAL ADMINISTRATIVO	[E.19] Fugas de información	5,1	Reducir
PERSONAL DE DESARROLLO	[E.15] Alteración de la información	5,1	Reducir
PERSONAL DE DESARROLLO	[E.19] Fugas de información	5,1	Reducir
UPS	[A.26] Ataques destructivos	5	Evitar
GENERADOR ELÉCTRICO	[A.26] Ataques destructivos	5	Evitar
EQUIPOS DE CLIMATIZACIÓN	[A.26] Ataques destructivos	5	Evitar
MOBILIARIO	[A.26] Ataques destructivos	5	Evitar
MATERIAL IMPRESO	[A.26] Ataques destructivos	5	Evitar
SOPORTE DE RED	[A.11] Acceso no autorizado	4,9	Reducir
MATERIAL IMPRESO	[A.11] Acceso no autorizado	4,9	Reducir

MOTOR DE BASE DE DATOS	[E.20]Vulnerabilidades de los programas (software)	4,8	Reducir
REPOSITORIO DE APLICACIONES DESARROLLADAS	[E.20]Vulnerabilidades de los programas (software)	4,8	Reducir
ANTIVIRUS	[E.20]Vulnerabilidades de los programas (software)	4,8	Reducir
FIREWALL	[E.20]Vulnerabilidades de los programas (software)	4,8	Reducir
LICENCIAS	[E.20]Vulnerabilidades de los programas (software)	4,8	Reducir
NAVEGADORES	[E.20]Vulnerabilidades de los programas (software)	4,8	Reducir
SISTEMAS OPERATIVOS	[E.20]Vulnerabilidades de los programas (software)	4,8	Reducir
UPS	[A.25] Robo de equipos	4,8	Evitar
GENERADOR ELÉCTRICO	[A.25] Robo de equipos	4,8	Evitar
EQUIPOS DE CLIMATIZACIÓN	[A.25] Robo de equipos	4,8	Evitar
MOBILIARIO	[A.25] Robo de equipos	4,8	Evitar
PERSONAL ADMINISTRATIVO	[A.28] Indisponibilidad del personal	4,8	Reducir
PERSONAL DE DESARROLLO	[A.28] Indisponibilidad del personal	4,8	Reducir
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[E.1] Errores de los usuarios	4,7	Reducir
CORREO INSTITUCIONAL	[A.6] Abuso de privilegios de acceso	4,6	Evitar
CORREO INSTITUCIONAL	[A.7] Uso no previsto	4,6	Evitar
UPS	[A.7] Uso no previsto	4,5	Evitar
GENERADOR ELÉCTRICO	[A.7] Uso no previsto	4,5	Evitar
EQUIPOS DE CLIMATIZACIÓN	[A.7] Uso no previsto	4,5	Evitar
MOBILIARIO	[A.7] Uso no previsto	4,5	Evitar
MATERIAL IMPRESO	[E.1] Errores de los usuarios	4,4	Reducir
SOPORTE DE RED	[E.1] Errores de los usuarios	4,4	Reducir
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[A.6] Abuso de privilegios de acceso	4,3	Evitar
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[A.7] Uso no previsto	4,3	Evitar
INSTALACIÓN DE RED DE DATOS	[I.4] Contaminación electromagnética	4,2	Reducir

INSTALACIÓN DE RED ELÉCTRICA	[I.4] Contaminación electromagnética	4,2	Reducir
UPS DEL CENTRO CABLEADO	[I.4] Contaminación electromagnética	4,2	Reducir
ESPACIO FÍSICO DDTI	[I.4] Contaminación electromagnética	4,2	Reducir
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[E.19] Fugas de información	3,9	Reducir
ETHERNET	[A.12] Análisis de tráfico	3,9	Evitar
RED INALAMBRICA	[A.12] Análisis de tráfico	3,9	Evitar
RED LAN	[A.12] Análisis de tráfico	3,9	Evitar
RED TELEFÓNICA	[A.12] Análisis de tráfico	3,9	Evitar
SOPORTE DE RED	[A.7] Uso no previsto	3,5	Evitar
MATERIAL IMPRESO	[A.7] Uso no previsto	3,5	Evitar
ARCHIVO DE DATOS	[E.15] Alteración de la información	3,4	Reducir
DOCUMENTACIÓN INTERNA	[E.15] Alteración de la información	3,4	Reducir
CARPETAS COMPARTIDAS	[E.15] Alteración de la información	3,4	Reducir
ARCHIVO DE DATOS	[E.18] Destrucción de la información	3,4	Reducir
DOCUMENTACIÓN INTERNA	[E.18] Destrucción de la información	3,4	Reducir
CARPETAS COMPARTIDAS	[E.18] Destrucción de la información	3,4	Reducir
MATERIAL IMPRESO	[E.15] Alteración de la información	3,4	Reducir
SOPORTE DE RED	[E.15] Alteración de la información	3,4	Reducir
BASE DE DATOS	[E.15] Alteración de la información	3,4	Reducir
BASE DE DATOS	[E.18] Destrucción de la información	3,4	Reducir
FIREWALL	[E.4] Errores de configuración	3,4	Reducir
FIREWALL	[E.18] Destrucción de la información	3,4	Reducir
ETHERNET	[E.15] Alteración de la información	3,4	Reducir
RED INALAMBRICA	[E.15] Alteración de la información	3,4	Reducir
RED LAN	[E.15] Alteración de la información	3,4	Reducir
RED TELEFÓNICA	[E.15] Alteración de la información	3,4	Reducir
CORREO INSTITUCIONAL	[E.15] Alteración de la información	3,4	Reducir

SOPORTE A LOS SERVICIOS INFORMÁTICOS	[E.15] Alteración de la información	3,4	Reducir
PERSONAL ADMINISTRATIVO	[E.18] Destrucción de la información	3,4	Reducir
PERSONAL DE DESARROLLO	[E.18] Destrucción de la información	3,4	Reducir
DISPOSITIVOS DE ALMACENAMIENTO	[I.11] Emanaciones electromagnéticas (TEMPEST)	3,3	Reducir
COMPUTADORAS	[I.11] Emanaciones electromagnéticas (TEMPEST)	3,3	Reducir
TELÉFONOS IP	[I.11] Emanaciones electromagnéticas (TEMPEST)	3,3	Reducir
SERVIDORES	[I.11] Emanaciones electromagnéticas (TEMPEST)	3,3	Reducir
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[I.11] Emanaciones electromagnéticas (TEMPEST)	3,3	Reducir
EQUIPO MULTIFUNCIONAL	[I.11] Emanaciones electromagnéticas (TEMPEST)	3,3	Reducir
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[I.11] Emanaciones electromagnéticas (TEMPEST)	3,3	Reducir
RADIOS DE COMUNICACIÓN	[I.11] Emanaciones electromagnéticas (TEMPEST)	3,3	Reducir

Nota: Elaboración propia

Anexo 8: Controles a implementar por activo del DDTI-UTN

ACTIVOS	AMENAZAS	TIPO DE CONTROL	CONTROL A IMPLEMENTAR
INSTALACIÓN DE RED DE DATOS	[A.25] Robo de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
INSTALACIÓN DE RED ELÉCTRICA	[A.25] Robo de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
UPS DEL CENTRO CABLEADO	[A.25] Robo de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
ESPACIO FÍSICO DDTI	[A.25] Robo de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos

ARCHIVO DE DATOS	[A.11] Acceso no autorizado	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
BASE DE DATOS	[A.11] Acceso no autorizado	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
DOCUMENTACIÓN INTERNA	[A.11] Acceso no autorizado	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
CARPETAS COMPARTIDAS	[A.11] Acceso no autorizado	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
SOPORTE DE RED	[A.15] Modificación de la información	A. 12 Seguridad de las operaciones	A. 12.4.1 Registro de eventos
MATERIAL IMPRESO	[A.15] Modificación de la información	A. 11 Seguridad física y del entorno	A. 11.1.1 Perímetro de seguridad física
ETHERNET	[A.24] Denegación de servicio	A. 12 Seguridad de las operaciones	A. 12.4.2 Protección de la información del registro
RED INALAMBRICA	[A.24] Denegación de servicio	A. 12 Seguridad de las operaciones	A. 12.4.2 Protección de la información del registro
RED LAN	[A.24] Denegación de servicio	A. 12 Seguridad de las operaciones	A. 12.4.2 Protección de la información del registro
RED TELEFÓNICA	[A.24] Denegación de servicio	A. 12 Seguridad de las operaciones	A. 12.4.2 Protección de la información del registro
CORREO INSTITUCIONAL	[A.24] Denegación de servicio	A. 12 Seguridad de las operaciones	A. 12.4.2 Protección de la información del registro
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[A.24] Denegación de servicio	A. 12 Seguridad de las operaciones	A. 12.4.2 Protección de la información del registro
DISPOSITIVOS DE ALMACENAMIENTO	[A.24] Denegación de servicio	A. 12 Seguridad de las operaciones	A. 12.4.2 Protección de la información del registro
COMPUTADORAS	[A.24] Denegación de servicio	A. 12 Seguridad de las operaciones	A. 12.4.2 Protección de la información del registro
TELÉFONOS IP	[A.24] Denegación de servicio	A. 12 Seguridad de	A. 12.4.2 Protección de la información del registro

		las operaciones	
SERVIDORES	[A.24] Denegación de servicio	A. 12 Seguridad de las operaciones	A. 12.4.2 Protección de la información del registro
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[A.24] Denegación de servicio	A. 12 Seguridad de las operaciones	A. 12.4.2 Protección de la información del registro
EQUIPO MULTIFUNCIONAL	[A.24] Denegación de servicio	A. 12 Seguridad de las operaciones	A. 12.4.2 Protección de la información del registro
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[A.24] Denegación de servicio	A. 12 Seguridad de las operaciones	A. 12.4.2 Protección de la información del registro
RADIOS DE COMUNICACIÓN	[A.24] Denegación de servicio	A. 12 Seguridad de las operaciones	A. 12.4.2 Protección de la información del registro
CORREO INSTITUCIONAL	[A.15] Modificación de la información	A. 13 Seguridad de las comunicaciones	A. 13.1.1 Controles de red
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[A.15] Modificación de la información	A. 12 Seguridad de las operaciones	A. 12.4.1 Registro de eventos
DISPOSITIVOS DE ALMACENAMIENTO	[E.24] Caída del sistema por agotamiento de recursos	A. 12 Seguridad de las operaciones	A. 12.1.3 Gestión de capacidades
COMPUTADORAS	[E.24] Caída del sistema por agotamiento de recursos	A. 12 Seguridad de las operaciones	A. 12.1.3 Gestión de capacidades
TELÉFONOS IP	[E.24] Caída del sistema por agotamiento de recursos	A. 12 Seguridad de las operaciones	A. 12.1.3 Gestión de capacidades
SERVIDORES	[E.24] Caída del sistema por agotamiento de recursos	A. 12 Seguridad de las operaciones	A. 12.1.3 Gestión de capacidades
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[E.24] Caída del sistema por agotamiento de recursos	A. 12 Seguridad de	A. 12.1.3 Gestión de capacidades

		las operaciones	
EQUIPO MULTIFUNCIONAL	[E.24] Caída del sistema por agotamiento de recursos	A. 12 Seguridad de las operaciones	A. 12.1.3 Gestión de capacidades
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[E.24] Caída del sistema por agotamiento de recursos	A. 12 Seguridad de las operaciones	A. 12.1.3 Gestión de capacidades
RADIOS DE COMUNICACIÓN	[E.24] Caída del sistema por agotamiento de recursos	A. 12 Seguridad de las operaciones	A. 12.1.3 Gestión de capacidades
CORREO INSTITUCIONAL	[E.24] Caída del sistema por agotamiento de recursos	A. 12 Seguridad de las operaciones	A. 12.1.3 Gestión de capacidades
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[E.24] Caída del sistema por agotamiento de recursos	A. 12 Seguridad de las operaciones	A. 12.1.3 Gestión de capacidades
MOTOR DE BASE DE DATOS	[A.8] Difusión de software dañino	A. 12 Seguridad de las operaciones	A. 12.6.2 restricciones en la instalación del software
REPOSITORIO DE APLICACIONES DESARROLLADAS	[A.8] Difusión de software dañino	A. 12 Seguridad de las operaciones	A. 12.6.2 restricciones en la instalación del software
ANTIVIRUS	[A.8] Difusión de software dañino	A. 12 Seguridad de las operaciones	A. 12.6.2 restricciones en la instalación del software
FIREWALL	[A.8] Difusión de software dañino	A. 12 Seguridad de las operaciones	A. 12.6.2 restricciones en la instalación del software
LICENCIAS	[A.8] Difusión de software dañino	A. 12 Seguridad de las operaciones	A. 12.6.2 restricciones en la instalación del software
NAVEGADORES	[A.8] Difusión de software dañino	A. 12 Seguridad de las operaciones	A. 12.6.2 restricciones en la instalación del software
SISTEMAS OPERATIVOS	[A.8] Difusión de software dañino	A. 12 Seguridad de las operaciones	A. 12.6.2 restricciones en la instalación del software

SOPORTE DE RED	[E.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.2 Acceso a redes y servicios de red
SOPORTE DE RED	[A.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.2 Acceso a redes y servicios de red
DISPOSITIVOS DE ALMACENAMIENTO	[I.6] Corte del suministro eléctrico	A. 11 Seguridad física y del entorno	A. 11.2.2 Instalaciones de suministro
DISPOSITIVOS DE ALMACENAMIENTO	[I.7] Condiciones inadecuadas de temperatura o humedad	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
COMPUTADORAS	[I.6] Corte del suministro eléctrico	A. 11 Seguridad física y del entorno	A. 11.2.2 Instalaciones de suministro
COMPUTADORAS	[I.7] Condiciones inadecuadas de temperatura o humedad	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
TELÉFONOS IP	[I.6] Corte del suministro eléctrico	A. 11 Seguridad física y del entorno	A. 11.2.2 Instalaciones de suministro
TELÉFONOS IP	[I.7] Condiciones inadecuadas de temperatura o humedad	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
SERVIDORES	[I.6] Corte del suministro eléctrico	A. 11 Seguridad física y del entorno	A. 11.2.2 Instalaciones de suministro
SERVIDORES	[I.7] Condiciones inadecuadas de temperatura o humedad	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[I.6] Corte del suministro eléctrico	A. 11 Seguridad física y del entorno	A. 11.2.2 Instalaciones de suministro
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[I.7] Condiciones inadecuadas de temperatura o humedad	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
EQUIPO MULTIFUNCIONAL	[I.6] Corte del suministro eléctrico	A. 11 Seguridad física y del entorno	A. 11.2.2 Instalaciones de suministro

EQUIPO MULTIFUNCIONAL	[I.7] Condiciones inadecuadas de temperatura o humedad	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[I.6] Corte del suministro eléctrico	A. 11 Seguridad física y del entorno	A. 11.2.2 Instalaciones de suministro
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[I.7] Condiciones inadecuadas de temperatura o humedad	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
RADIOS DE COMUNICACIÓN	[I.6] Corte del suministro eléctrico	A. 11 Seguridad física y del entorno	A. 11.2.2 Instalaciones de suministro
RADIOS DE COMUNICACIÓN	[I.7] Condiciones inadecuadas de temperatura o humedad	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
INSTALACIÓN DE RED DE DATOS	[N.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
INSTALACIÓN DE RED DE DATOS	[N.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
INSTALACIÓN DE RED DE DATOS	[I.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
INSTALACIÓN DE RED DE DATOS	[I.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
INSTALACIÓN DE RED DE DATOS	[I.*] Desastres industriales	A. 17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	A. 17.1.1 Planififación de la continuidad de la seguridad de la información
INSTALACIÓN DE RED ELÉCTRICA	[N.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
INSTALACIÓN DE RED ELÉCTRICA	[N.2] Daños por agua	A. 11 Seguridad	A. 11.1.5 El trabajo en áreas seguras

		física y del entorno	
INSTALACIÓN DE RED ELÉCTRICA	[I.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
INSTALACIÓN DE RED ELÉCTRICA	[I.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
INSTALACIÓN DE RED ELÉCTRICA	[I.*] Desastres industriales	A. 17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	A. 17.1.1 Planififación de la continuidad de la seguridad de la información
UPS DEL CENTRO CABLEADO	[N.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
UPS DEL CENTRO CABLEADO	[N.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
UPS DEL CENTRO CABLEADO	[I.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
UPS DEL CENTRO CABLEADO	[I.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
UPS DEL CENTRO CABLEADO	[I.*] Desastres industriales	A. 17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	A. 17.1.1 Planificación de la continuidad de la seguridad de la información
ESPACIO FÍSICO DDTI	[N.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
ESPACIO FÍSICO DDTI	[N.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras

ESPACIO FÍSICO DDTI	[I.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
ESPACIO FÍSICO DDTI	[I.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
ESPACIO FÍSICO DDTI	[I.*] Desastres industriales	A. 17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	A. 17.1.1 Planificación de la continuidad de la seguridad de la información
MATERIAL IMPRESO	[I.7] Condiciones inadecuadas de temperatura o humedad	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
MATERIAL IMPRESO	[E.18] Destrucción de la información	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
MATERIAL IMPRESO	[A.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
MOTOR DE BASE DE DATOS	[A.22] Manipulación de programas	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
REPOSITORIO DE APLICACIONES DESARROLLADAS	[A.22] Manipulación de programas	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
ANTIVIRUS	[A.22] Manipulación de programas	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
FIREWALL	[A.22] Manipulación de programas	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
LICENCIAS	[A.22] Manipulación de programas	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
NAVEGADORES	[A.22] Manipulación de programas	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
SISTEMAS OPERATIVOS	[A.22] Manipulación de programas	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
DISPOSITIVOS DE ALMACENAMIENTO	[A.26] Ataques destructivos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
COMPUTADORAS	[A.26] Ataques destructivos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos

TELÉFONOS IP	[A.26] Ataques destructivos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
SERVIDORES	[A.26] Ataques destructivos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[A.26] Ataques destructivos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
EQUIPO MULTIFUNCIONAL	[A.26] Ataques destructivos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[A.26] Ataques destructivos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
RADIOS DE COMUNICACIÓN	[A.26] Ataques destructivos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
INSTALACIÓN DE RED DE DATOS	[A.27] Ocupación enemiga	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
INSTALACIÓN DE RED ELÉCTRICA	[A.27] Ocupación enemiga	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
UPS DEL CENTRO CABLEADO	[A.27] Ocupación enemiga	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
ESPACIO FÍSICO DDTI	[A.27] Ocupación enemiga	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
BASE DE DATOS	[A.5] Suplantación de la identidad	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
FIREWALL	[A.5] Suplantación de la identidad	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
ARCHIVO DE DATOS	[A.5] Suplantación de la identidad	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
DOCUMENTACIÓN INTERNA	[A.5] Suplantación de la identidad	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
CARPETAS COMPARTIDAS	[A.5] Suplantación de la identidad	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
DISPOSITIVOS DE ALMACENAMIENTO	[E.25] Pérdida de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
COMPUTADORAS	[E.25] Pérdida de equipos	A. 11 Seguridad	A. 11.2.1 Emplazamiento y protección de equipos

		física y del entorno	
TELÉFONOS IP	[E.25] Pérdida de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
SERVIDORES	[E.25] Pérdida de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[E.25] Pérdida de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
EQUIPO MULTIFUNCIONAL	[E.25] Pérdida de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[E.25] Pérdida de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
RADIOS DE COMUNICACIÓN	[E.25] Pérdida de equipos	A. 8 Gestión de activos	A. 8.1.1 Inventario de activos
MATERIAL IMPRESO	[I.1] Fuego		
MATERIAL IMPRESO	[I.*] Desastres industriales	A. 17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	A. 17.1.1 Planificación de la continuidad de la seguridad de la información
DISPOSITIVOS DE ALMACENAMIENTO	[I.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
DISPOSITIVOS DE ALMACENAMIENTO	[I.*] Desastres industriales	A. 17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	A. 17.1.1 Planificación de la continuidad de la seguridad de la información
COMPUTADORAS	[I.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales

COMPUTADORAS	[I.*] Desastres industriales	A. 17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	A. 17.1.1 Planificación de la continuidad de la seguridad de la información
TELÉFONOS IP	[I.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
TELÉFONOS IP	[I.*] Desastres industriales	A. 17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	A. 17.1.1 Planificación de la continuidad de la seguridad de la información
SERVIDORES	[I.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
SERVIDORES	[I.*] Desastres industriales	A. 17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	A. 17.1.1 Planificación de la continuidad de la seguridad de la información
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[I.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[I.*] Desastres industriales	A. 17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	A. 17.1.1 Planificación de la continuidad de la seguridad de la información
EQUIPO MULTIFUNCIONAL	[I.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales

EQUIPO MULTIFUNCIONAL	[I.*] Desastres industriales	A. 17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	A. 17.1.1 Planificación de la continuidad de la seguridad de la información
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[I.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[I.*] Desastres industriales	A. 17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	A. 17.1.1 Planificación de la continuidad de la seguridad de la información
RADIOS DE COMUNICACIÓN	[I.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
RADIOS DE COMUNICACIÓN	[I.*] Desastres industriales	A. 17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	A. 17.1.1 Planificación de la continuidad de la seguridad de la información
UPS	[I.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
UPS	[I.*] Desastres industriales	A. 17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	A. 17.1.1 Planificación de la continuidad de la seguridad de la información
GENERADOR ELÉCTRICO	[I.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales

GENERADOR ELÉCTRICO	[I.*] Desastres industriales	A. 17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	A. 17.1.1 Planificación de la continuidad de la seguridad de la información
EQUIPOS DE CLIMATIZACIÓN	[I.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
EQUIPOS DE CLIMATIZACIÓN	[I.*] Desastres industriales	A. 17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	A. 17.1.1 Planificación de la continuidad de la seguridad de la información
MOBILIARIO	[I.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
MOBILIARIO	[I.*] Desastres industriales	A. 17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	A. 17.1.1 Planificación de la continuidad de la seguridad de la información
INSTALACIÓN DE RED DE DATOS	[N.*] Desastres naturales	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
INSTALACIÓN DE RED ELÉCTRICA	[N.*] Desastres naturales	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
UPS DEL CENTRO CABLEADO	[N.*] Desastres naturales	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
ESPACIO FÍSICO DDTI	[N.*] Desastres naturales	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
MANTENIMIENTO DE EQUIPOS	[A.24] Denegación de servicio	A. 12 Seguridad de	A. 12.4.2 Protección de la información del registro

		las operaciones	
TELEFONÍA	[A.24] Denegación de servicio	A. 12 Seguridad de las operaciones	A. 12.4.2 Protección de la información del registro
INTERNET	[A.24] Denegación de servicio	A. 12 Seguridad de las operaciones	A. 12.4.2 Protección de la información del registro
ETHERNET	[E.24] Caída del sistema por agotamiento de recursos	A. 12 Seguridad de las operaciones	A. 12.1.3 Gestión de capacidades
ETHERNET	[A.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.2 Acceso a redes y servicios de red
RED INALAMBRICA	[E.24] Caída del sistema por agotamiento de recursos	A. 12 Seguridad de las operaciones	A. 12.1.3 Gestión de capacidades
RED INALAMBRICA	[A.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.2 Acceso a redes y servicios de red
RED LAN	[E.24] Caída del sistema por agotamiento de recursos	A. 12 Seguridad de las operaciones	A. 12.1.3 Gestión de capacidades
RED LAN	[A.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.2 Acceso a redes y servicios de red
RED TELEFÓNICA	[E.24] Caída del sistema por agotamiento de recursos	A. 12 Seguridad de las operaciones	A. 12.1.3 Gestión de capacidades
RED TELEFÓNICA	[A.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.2 Acceso a redes y servicios de red
TELEFONÍA	[A.15] Modificación de la información	A. 13 Seguridad de las comunicaciones	A. 13.1.1 Controles de red
CORREO INSTITUCIONAL	[A.5] Suplantación de la identidad	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
CORREO INSTITUCIONAL	[A.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.2 Acceso a redes y servicios de red
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[A.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.2 Acceso a redes y servicios de red
MANTENIMIENTO DE EQUIPOS	[A.18] Destrucción de la información	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos

PERSONAL ADMINISTRATIVO	[A.15] Modificación de la información	A. 12 Seguridad de las operaciones	A. 12.4.1 Registro de eventos
PERSONAL ADMINISTRATIVO	[A.19] Revelación de información	A. 7 Seguridad relativa a los recursos humanos	A.7.2.2 Concienciación, educación y capacitación en seguridad de la información
PERSONAL DE DESARROLLO	[A.15] Modificación de la información	A. 12 Seguridad de las operaciones	A. 12.4.1 Registro de eventos
PERSONAL DE DESARROLLO	[A.19] Revelación de información	A. 7 Seguridad relativa a los recursos humanos	A.7.2.2 Concienciación, educación y capacitación en seguridad de la información
TELEFONÍA	[A.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.2 Acceso a redes y servicios de red
INTERNET	[A.15] Modificación de la información	A. 13 Seguridad de las comunicaciones	A. 13.1.1 Controles de red
INTERNET	[A.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.2 Acceso a redes y servicios de red
MANTENIMIENTO DE EQUIPOS	[A.15] Modificación de la información	A. 12 Seguridad de las operaciones	A. 12.4.1 Registro de eventos
MANTENIMIENTO DE EQUIPOS	[A.19] Revelación de información	A. 7 Seguridad relativa a los recursos humanos	A.7.2.2 Concienciación, educación y capacitación en seguridad de la información
MANTENIMIENTO DE EQUIPOS	[I.9] Interrupción de otros servicios o suministros esenciales	A. 11 Seguridad física y del entorno	A. 11.2.2 Instalaciones de suministro
INTERNET	[A.5] Suplantación de la identidad	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
MATERIAL IMPRESO	[I.3] Contaminación medioambiental	A. 11 Seguridad física y del entorno	
MOTOR DE BASE DE DATOS	[I.5.1] Avería de origen lógico	A. 12 Seguridad de las operaciones	A. 12.3.1 Copias de seguridad de la información
REPOSITORIO DE APLICACIONES	[I.5.1] Avería de origen lógico	A. 12 Seguridad de	A. 12.3.1 Copias de seguridad de la información

DESARROLLADAS		las operaciones	
ANTIVIRUS	[I.5.1] Avería de origen lógico	A. 12 Seguridad de las operaciones	A. 12.3.1 Copias de seguridad de la información
FIREWALL	[I.5.1] Avería de origen lógico	A. 12 Seguridad de las operaciones	A. 12.3.1 Copias de seguridad de la información
LICENCIAS	[I.5.1] Avería de origen lógico	A. 12 Seguridad de las operaciones	A. 12.3.1 Copias de seguridad de la información
NAVEGADORES	[I.5.1] Avería de origen lógico	A. 12 Seguridad de las operaciones	A. 12.3.1 Copias de seguridad de la información
SISTEMAS OPERATIVOS	[I.5.1] Avería de origen lógico	A. 12 Seguridad de las operaciones	A. 12.3.1 Copias de seguridad de la información
DISPOSITIVOS DE ALMACENAMIENTO	[I.5.2] Avería de origen físico	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
COMPUTADORAS	[I.5.2] Avería de origen físico	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
TELÉFONOS IP	[I.5.2] Avería de origen físico	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
SERVIDORES	[I.5.2] Avería de origen físico	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[I.5.2] Avería de origen físico	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
EQUIPO MULTIFUNCIONAL	[I.5.2] Avería de origen físico	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[I.5.2] Avería de origen físico	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos

RADIOS DE COMUNICACIÓN	[I.5.2] Avería de origen físico	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
ETHERNET	[I.8] Fallo de servicios de comunicación	A. 13 Seguridad de las comunicaciones	A. 13.1.2 Seguridad de los servicios de red
RED INALAMBRICA	[I.8] Fallo de servicios de comunicación	A. 13 Seguridad de las comunicaciones	A. 13.1.2 Seguridad de los servicios de red
RED LAN	[I.8] Fallo de servicios de comunicación	A. 13 Seguridad de las comunicaciones	A. 13.1.2 Seguridad de los servicios de red
RED TELEFÓNICA	[I.8] Fallo de servicios de comunicación	A. 13 Seguridad de las comunicaciones	A. 13.1.2 Seguridad de los servicios de red
UPS	[A.23] Manipulación de hardware	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
GENERADOR ELÉCTRICO	[A.23] Manipulación de hardware	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
EQUIPOS DE CLIMATIZACIÓN	[A.23] Manipulación de hardware	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
MOBILIARIO	[A.23] Manipulación de hardware	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
ELECTRICIDAD	[I.9] Interrupción de otros servicios o suministros esenciales	A. 11 Seguridad física y del entorno	A. 11.2.2 Instalaciones de suministro
MANTENIMIENTO DE EQUIPOS	[A.5] Suplantación de la identidad	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
DISPOSITIVOS DE ALMACENAMIENTO	[A.25] Robo de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos

COMPUTADORAS	[A.25] Robo de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
TELÉFONOS IP	[A.25] Robo de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
SERVIDORES	[A.25] Robo de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[A.25] Robo de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
EQUIPO MULTIFUNCIONAL	[A.25] Robo de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[A.25] Robo de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
RADIOS DE COMUNICACIÓN	[A.25] Robo de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
MATERIAL IMPRESO	[I.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
DISPOSITIVOS DE ALMACENAMIENTO	[I.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
COMPUTADORAS	[I.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
TELÉFONOS IP	[I.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
SERVIDORES	[I.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos

EQUIPO PARA EL FUNCIONAMIENTO DE RED	[I.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
EQUIPO MULTIFUNCIONAL	[I.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[I.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
RADIOS DE COMUNICACIÓN	[I.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
UPS	[I.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
GENERADOR ELÉCTRICO	[I.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
EQUIPOS DE CLIMATIZACIÓN	[I.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
MOBILIARIO	[I.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
MATERIAL IMPRESO	[N.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
MATERIAL IMPRESO	[N.*] Desastres naturales	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
DISPOSITIVOS DE ALMACENAMIENTO	[N.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
DISPOSITIVOS DE ALMACENAMIENTO	[N.*] Desastres naturales	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras

DISPOSITIVOS DE ALMACENAMIENTO	[A.23] Manipulación de hardware	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
COMPUTADORAS	[N.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
COMPUTADORAS	[N.*] Desastres naturales	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
COMPUTADORAS	[A.23] Manipulación de hardware	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
TELÉFONOS IP	[N.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
TELÉFONOS IP	[N.*] Desastres naturales	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
TELÉFONOS IP	[A.23] Manipulación de hardware	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
SERVIDORES	[N.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
SERVIDORES	[N.*] Desastres naturales	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
SERVIDORES	[A.23] Manipulación de hardware	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[N.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[N.*] Desastres naturales	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras

EQUIPO PARA EL FUNCIONAMIENTO DE RED	[A.23] Manipulación de hardware	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
EQUIPO MULTIFUNCIONAL	[N.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
EQUIPO MULTIFUNCIONAL	[N.*] Desastres naturales	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
EQUIPO MULTIFUNCIONAL	[A.23] Manipulación de hardware	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[N.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[N.*] Desastres naturales	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[A.23] Manipulación de hardware	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
RADIOS DE COMUNICACIÓN	[N.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
RADIOS DE COMUNICACIÓN	[N.*] Desastres naturales	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
RADIOS DE COMUNICACIÓN	[A.23] Manipulación de hardware	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
UPS	[N.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
UPS	[N.*] Desastres naturales	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras

GENERADOR ELÉCTRICO	[N.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
GENERADOR ELÉCTRICO	[N.*] Desastres naturales	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
EQUIPOS DE CLIMATIZACIÓN	[N.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
EQUIPOS DE CLIMATIZACIÓN	[N.*] Desastres naturales	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
MOBILIARIO	[N.1] Fuego	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
MOBILIARIO	[N.*] Desastres naturales	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
INSTALACIÓN DE RED DE DATOS	[E.25] Pérdida de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
INSTALACIÓN DE RED ELÉCTRICA	[E.25] Pérdida de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
UPS DEL CENTRO CABLEADO	[E.25] Pérdida de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
ESPACIO FÍSICO DDTI	[E.25] Pérdida de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
BASE DE DATOS	[A.6] Abuso de privilegios de acceso	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
ARCHIVO DE DATOS	[A.6] Abuso de privilegios de acceso	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información

DOCUMENTACIÓN INTERNA	[A.6] Abuso de privilegios de acceso	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
CARPETAS COMPARTIDAS	[A.6] Abuso de privilegios de acceso	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
FIREWALL	[A.4] Manipulación de los ficheros de configuración	A. 14 Adquisición, desarrollo y mantenimiento de los sistemas de información	A. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
INSTALACIÓN DE RED DE DATOS	[A.26] Ataques destructivos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
INSTALACIÓN DE RED ELÉCTRICA	[A.26] Ataques destructivos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
UPS DEL CENTRO CABLEADO	[A.26] Ataques destructivos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
ESPACIO FÍSICO DDTI	[A.26] Ataques destructivos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
ETHERNET	[A.5] Suplantación de la identidad	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
ETHERNET	[A.11] Acceso no autorizado	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
RED INALAMBRICA	[A.5] Suplantación de la identidad	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
RED INALAMBRICA	[A.11] Acceso no autorizado	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
RED LAN	[A.5] Suplantación de la identidad	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
RED LAN	[A.11] Acceso no autorizado	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
RED TELEFÓNICA	[A.5] Suplantación de la identidad	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
RED TELEFÓNICA	[A.11] Acceso no autorizado	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso

CORREO INSTITUCIONAL	[A.11] Acceso no autorizado	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[A.5] Suplantación de la identidad	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
MOTOR DE BASE DE DATOS	[E.21] Errores de mantenimiento/actualización de programas (software)	A. 12 Seguridad de las operaciones	A. 12.1.2 Gestión de cambios
REPOSITORIO DE APLICACIONES DESARROLLADAS	[E.21] Errores de mantenimiento/actualización de programas (software)	A. 12 Seguridad de las operaciones	A. 12.1.2 Gestión de cambios
ANTIVIRUS	[E.21] Errores de mantenimiento/actualización de programas (software)	A. 12 Seguridad de las operaciones	A. 12.1.2 Gestión de cambios
FIREWALL	[E.21] Errores de mantenimiento/actualización de programas (software)	A. 12 Seguridad de las operaciones	A. 12.1.2 Gestión de cambios
LICENCIAS	[E.21] Errores de mantenimiento/actualización de programas (software)	A. 12 Seguridad de las operaciones	A. 12.1.2 Gestión de cambios
NAVEGADORES	[E.21] Errores de mantenimiento/actualización de programas (software)	A. 12 Seguridad de las operaciones	A. 12.1.2 Gestión de cambios
SISTEMAS OPERATIVOS	[E.21] Errores de mantenimiento/actualización de programas (software)	A. 12 Seguridad de las operaciones	A. 12.1.2 Gestión de cambios
DISPOSITIVOS DE ALMACENAMIENTO	[A.11] Acceso no autorizado	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
COMPUTADORAS	[A.11] Acceso no autorizado	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
TELÉFONOS IP	[A.11] Acceso no autorizado	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
SERVIDORES	[A.11] Acceso no autorizado	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[A.11] Acceso no autorizado	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
EQUIPO MULTIFUNCIONAL	[A.11] Acceso no autorizado	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso

DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[A.11] Acceso no autorizado	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
RADIOS DE COMUNICACIÓN	[A.11] Acceso no autorizado	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
ETHERNET	[E.2] Errores del administrador del sistema	A. 12 Seguridad de las operaciones	A. 12.4.3 Registro de administración y operación
RED INALAMBRICA	[E.2] Errores del administrador del sistema	A. 12 Seguridad de las operaciones	A. 12.4.3 Registro de administración y operación
RED LAN	[E.2] Errores del administrador del sistema	A. 12 Seguridad de las operaciones	A. 12.4.3 Registro de administración y operación
RED TELEFÓNICA	[E.2] Errores del administrador del sistema	A. 12 Seguridad de las operaciones	A. 12.4.3 Registro de administración y operación
CORREO INSTITUCIONAL	[E.2] Errores del administrador del sistema	A. 12 Seguridad de las operaciones	A. 12.4.3 Registro de administración y operación
PERSONAL ADMINISTRATIVO	[A.29] Extorsión	A. 7 Seguridad relativa a los recursos humanos	A.7.2.2 Concienciación, educación y capacitación en seguridad de la información
PERSONAL DE DESARROLLO	[A.29] Extorsión	A. 7 Seguridad relativa a los recursos humanos	A.7.2.2 Concienciación, educación y capacitación en seguridad de la información
MATERIAL IMPRESO	[N.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
DISPOSITIVOS DE ALMACENAMIENTO	[N.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
DISPOSITIVOS DE ALMACENAMIENTO	[I.3] Contaminación medioambiental	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
COMPUTADORAS	[N.2] Daños por agua	A. 11 Seguridad	A. 11.1.5 El trabajo en áreas seguras

		física y del entorno	
COMPUTADORAS	[I.3] Contaminación medioambiental	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
TELÉFONOS IP	[N.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
TELÉFONOS IP	[I.3] Contaminación medioambiental	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
SERVIDORES	[N.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
SERVIDORES	[I.3] Contaminación medioambiental	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[N.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[I.3] Contaminación medioambiental	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
EQUIPO MULTIFUNCIONAL	[N.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
EQUIPO MULTIFUNCIONAL	[I.3] Contaminación medioambiental	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[N.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[I.3] Contaminación medioambiental	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
RADIOS DE COMUNICACIÓN	[N.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras

RADIOS DE COMUNICACIÓN	[I.3] Contaminación medioambiental	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
UPS	[N.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
UPS	[I.3] Contaminación medioambiental	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
GENERADOR ELÉCTRICO	[N.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
GENERADOR ELÉCTRICO	[I.3] Contaminación medioambiental	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
EQUIPOS DE CLIMATIZACIÓN	[N.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
EQUIPOS DE CLIMATIZACIÓN	[I.3] Contaminación medioambiental	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
MOBILIARIO	[N.2] Daños por agua	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
MOBILIARIO	[I.3] Contaminación medioambiental	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
PERSONAL ADMINISTRATIVO	[A.30] Ingeniería social (picaresca)	A. 7 Seguridad relativa a los recursos humanos	A.7.2.2 Concienciación, educación y capacitación en seguridad de la información
PERSONAL DE DESARROLLO	[A.30] Ingeniería social (picaresca)	A. 7 Seguridad relativa a los recursos humanos	A.7.2.2 Concienciación, educación y capacitación en seguridad de la información
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[A.11] Acceso no autorizado	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso

SOPORTE A LOS SERVICIOS INFORMÁTICOS	[E.2] Errores del administrador del sistema	A. 12 Seguridad de las operaciones	A. 12.4.3 Registro de administración y operación
ETHERNET	[A.7] Uso no previsto	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
ETHERNET	[A.14] Interceptación de información (escucha)	A. 13 Seguridad de las comunicaciones	A. 13.1.2 Seguridad de los servicios de red
ETHERNET	[A.15] Modificación de la información	A. 13 Seguridad de las comunicaciones	A. 13.1.1 Controles de red
RED INALAMBRICA	[A.7] Uso no previsto	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
RED INALAMBRICA	[A.14] Interceptación de información (escucha)	A. 13 Seguridad de las comunicaciones	A. 13.1.2 Seguridad de los servicios de red
RED INALAMBRICA	[A.15] Modificación de la información	A. 13 Seguridad de las comunicaciones	A. 13.1.1 Controles de red
RED LAN	[A.7] Uso no previsto	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
RED LAN	[A.14] Interceptación de información (escucha)	A. 13 Seguridad de las comunicaciones	A. 13.1.2 Seguridad de los servicios de red
RED LAN	[A.15] Modificación de la información	A. 13 Seguridad de las comunicaciones	A. 13.1.1 Controles de red

RED TELEFÓNICA	[A.7] Uso no previsto	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
RED TELEFÓNICA	[A.14] Interceptación de información (escucha)	A. 13 Seguridad de las comunicaciones	A. 13.1.2 Seguridad de los servicios de red
RED TELEFÓNICA	[A.15] Modificación de la información	A. 13 Seguridad de las comunicaciones	A. 13.1.1 Controles de red
INSTALACIÓN DE RED DE DATOS	[A.6] Abuso de privilegios de acceso	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
INSTALACIÓN DE RED DE DATOS	[A.7] Uso no previsto	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
INSTALACIÓN DE RED ELÉCTRICA	[A.6] Abuso de privilegios de acceso	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
INSTALACIÓN DE RED ELÉCTRICA	[A.7] Uso no previsto	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
UPS DEL CENTRO CABLEADO	[A.6] Abuso de privilegios de acceso	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
UPS DEL CENTRO CABLEADO	[A.7] Uso no previsto	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
ESPACIO FÍSICO DDTI	[A.6] Abuso de privilegios de acceso	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información

ESPACIO FÍSICO DDTI	[A.7] Uso no previsto	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
PERSONAL ADMINISTRATIVO	[A.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
PERSONAL DE DESARROLLO	[A.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
TELEFONÍA	[E.15] Alteración de la información	A. 12 Seguridad de las operaciones	A. 12.4.2 Protección de la información del registro
INTERNET	[E.15] Alteración de la información	A. 12 Seguridad de las operaciones	A. 12.4.2 Protección de la información del registro
TELEFONÍA	[E.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.2 Acceso a redes y servicios de red
INTERNET	[E.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.2 Acceso a redes y servicios de red
MANTENIMIENTO DE EQUIPOS	[E.15] Alteración de la información	A. 12 Seguridad de las operaciones	A. 12.4.1 Registro de eventos
TELEFONÍA	[E.19] Fugas de información	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
INTERNET	[E.19] Fugas de información	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
SOPORTE DE RED	[E.19] Fugas de información	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
MANTENIMIENTO DE EQUIPOS	[E.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
ARCHIVO DE DATOS	[E.19] Fugas de información	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
DOCUMENTACIÓN INTERNA	[E.19] Fugas de información	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
CARPETAS COMPARTIDAS	[E.19] Fugas de información	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
MANTENIMIENTO DE EQUIPOS	[E.19] Fugas de información	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
BASE DE DATOS	[E.19] Fugas de información	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
MATERIAL IMPRESO	[E.19] Fugas de información	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
MOTOR DE BASE DE DATOS	[E.8] Difusión de software dañino	A. 12 Seguridad de las operaciones	A. 12.6.2 restricciones en la instalación del software

REPOSITORIO DE APLICACIONES DESARROLLADAS	[E.8] Difusión de software dañino	A. 12 Seguridad de las operaciones	A. 12.6.2 restricciones en la instalación del software
ANTIVIRUS	[E.8] Difusión de software dañino	A. 12 Seguridad de las operaciones	A. 12.6.2 restricciones en la instalación del software
FIREWALL	[E.8] Difusión de software dañino	A. 12 Seguridad de las operaciones	A. 12.6.2 restricciones en la instalación del software
LICENCIAS	[E.8] Difusión de software dañino	A. 12 Seguridad de las operaciones	A. 12.6.2 restricciones en la instalación del software
NAVEGADORES	[E.8] Difusión de software dañino	A. 12 Seguridad de las operaciones	A. 12.6.2 restricciones en la instalación del software
SISTEMAS OPERATIVOS	[E.8] Difusión de software dañino	A. 12 Seguridad de las operaciones	A. 12.6.2 restricciones en la instalación del software
DISPOSITIVOS DE ALMACENAMIENTO	[I.4] Contaminación electromagnética	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
DISPOSITIVOS DE ALMACENAMIENTO	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
COMPUTADORAS	[I.4] Contaminación electromagnética	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
COMPUTADORAS	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
TELÉFONOS IP	[I.4] Contaminación electromagnética	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
TELÉFONOS IP	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
SERVIDORES	[I.4] Contaminación electromagnética	A. 11 Seguridad	A. 11.2.1 Emplazamiento y protección de equipos

		física y del entorno	
SERVIDORES	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[I.4] Contaminación electromagnética	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
EQUIPO MULTIFUNCIONAL	[I.4] Contaminación electromagnética	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
EQUIPO MULTIFUNCIONAL	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[I.4] Contaminación electromagnética	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
RADIOS DE COMUNICACIÓN	[I.4] Contaminación electromagnética	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
RADIOS DE COMUNICACIÓN	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
ETHERNET	[E.9] Errores de [re-]encaminamiento	A. 13 Seguridad de las comunicaciones	A. 13.1.1 Controles de red
ETHERNET	[E.10] Errores de secuencia	A. 12 Seguridad de las operaciones	A. 12.4.1 Registro de eventos
ETHERNET	[E.19] Fugas de información	A. 13 Seguridad de las	A. 13.2.4 Acuerdos de confidencialidad o no revelación

		comunicaciones	
ETHERNET	[A.9] [Re-]encaminamiento de mensajes	A. 13 Seguridad de las comunicaciones	A. 13.1.1 Controles de red
ETHERNET	[A.10] Alteración de secuencia	A. 13 Seguridad de las comunicaciones	A. 13.1.1 Controles de red
RED INALAMBRICA	[E.9] Errores de [re-]encaminamiento	A. 13 Seguridad de las comunicaciones	A. 13.1.1 Controles de red
RED INALAMBRICA	[E.10] Errores de secuencia	A. 12 Seguridad de las operaciones	A. 12.4.1 Registro de eventos
RED INALAMBRICA	[E.19] Fugas de información	A. 13 Seguridad de las comunicaciones	A. 13.2.4 Acuerdos de confidencialidad o no revelación
RED INALAMBRICA	[A.9] [Re-]encaminamiento de mensajes	A. 13 Seguridad de las comunicaciones	A. 13.1.1 Controles de red
RED INALAMBRICA	[A.10] Alteración de secuencia	A. 13 Seguridad de las comunicaciones	A. 13.1.1 Controles de red
RED LAN	[E.9] Errores de [re-]encaminamiento	A. 13 Seguridad de las comunicaciones	A. 13.1.1 Controles de red
RED LAN	[E.10] Errores de secuencia	A. 12 Seguridad de las operaciones	A. 12.4.1 Registro de eventos
RED LAN	[E.19] Fugas de información	A. 13 Seguridad de las comunicaciones	A. 13.2.4 Acuerdos de confidencialidad o no revelación

RED LAN	[A.9] [Re-]encaminamiento de mensajes	A. 13 Seguridad de las comunicaciones	A. 13.1.1 Controles de red
RED LAN	[A.10] Alteración de secuencia	A. 13 Seguridad de las comunicaciones	A. 13.1.1 Controles de red
RED TELEFÓNICA	[E.9] Errores de [re-]encaminamiento	A. 13 Seguridad de las comunicaciones	A. 13.1.1 Controles de red
RED TELEFÓNICA	[E.10] Errores de secuencia	A. 12 Seguridad de las operaciones	A. 12.4.1 Registro de eventos
RED TELEFÓNICA	[E.19] Fugas de información	A. 13 Seguridad de las comunicaciones	A. 13.2.4 Acuerdos de confidencialidad o no revelación
RED TELEFÓNICA	[A.9] [Re-]encaminamiento de mensajes	A. 13 Seguridad de las comunicaciones	A. 13.1.1 Controles de red
RED TELEFÓNICA	[A.10] Alteración de secuencia	A. 13 Seguridad de las comunicaciones	A. 13.1.1 Controles de red
UPS	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
GENERADOR ELÉCTRICO	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
EQUIPOS DE CLIMATIZACIÓN	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos
MOBILIARIO	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	A. 11 Seguridad física y del entorno	A. 11.2.4 Mantenimiento de los equipos

ELECTRICIDAD	[E.15] Alteración de la información	A. 12 Seguridad de las operaciones	A. 12.3.1 Copias de seguridad de la información
ELECTRICIDAD	[E.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.2 Acceso a redes y servicios de red
CORREO INSTITUCIONAL	[E.1] Errores de los usuarios	A. 12 Seguridad de las operaciones	A. 12.1.1 Documentación de procedimientos de operación
CORREO INSTITUCIONAL	[E.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.2 Acceso a redes y servicios de red
CORREO INSTITUCIONAL	[E.19] Fugas de información	A. 13 Seguridad de las comunicaciones	A. 13.2.4 Acuerdos de confidencialidad o no revelación
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[E.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.2 Acceso a redes y servicios de red
INSTALACIÓN DE RED DE DATOS	[I.3] Contaminación medioambiental	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
INSTALACIÓN DE RED ELÉCTRICA	[I.3] Contaminación medioambiental	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
UPS DEL CENTRO CABLEADO	[I.3] Contaminación medioambiental	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
ESPACIO FÍSICO DDTI	[I.3] Contaminación medioambiental	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
PERSONAL ADMINISTRATIVO	[E.15] Alteración de la información	A. 12 Seguridad de las operaciones	A. 12.4.1 Registro de eventos
PERSONAL ADMINISTRATIVO	[E.19] Fugas de información	A. 9 Control de acceso	A. 9.2.3 Gestión de privilegios de derechos de accesos
PERSONAL DE DESARROLLO	[E.15] Alteración de la información	A. 12 Seguridad de las operaciones	A. 12.4.1 Registro de eventos
PERSONAL DE DESARROLLO	[E.19] Fugas de información	A. 9 Control de acceso	A. 9.2.3 Gestión de privilegios de derechos de accesos

UPS	[A.26] Ataques destructivos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
GENERADOR ELÉCTRICO	[A.26] Ataques destructivos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
EQUIPOS DE CLIMATIZACIÓN	[A.26] Ataques destructivos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
MOBILIARIO	[A.26] Ataques destructivos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
MATERIAL IMPRESO	[A.26] Ataques destructivos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
SOPORTE DE RED	[A.11] Acceso no autorizado	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
MATERIAL IMPRESO	[A.11] Acceso no autorizado	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
MOTOR DE BASE DE DATOS	[E.20]Vulnerabilidades de los programas (software)	A. 12 Seguridad de las operaciones	A. 12.6.1 Gestión de vulnerabilidades técnicas
REPOSITORIO DE APLICACIONES DESARROLLADAS	[E.20]Vulnerabilidades de los programas (software)	A. 12 Seguridad de las operaciones	A. 12.6.1 Gestión de vulnerabilidades técnicas
ANTIVIRUS	[E.20]Vulnerabilidades de los programas (software)	A. 12 Seguridad de las operaciones	A. 12.6.1 Gestión de vulnerabilidades técnicas
FIREWALL	[E.20]Vulnerabilidades de los programas (software)	A. 12 Seguridad de las operaciones	A. 12.6.1 Gestión de vulnerabilidades técnicas
LICENCIAS	[E.20]Vulnerabilidades de los programas (software)	A. 12 Seguridad de las operaciones	A. 12.6.1 Gestión de vulnerabilidades técnicas
NAVEGADORES	[E.20]Vulnerabilidades de los programas (software)	A. 12 Seguridad de las operaciones	A. 12.6.1 Gestión de vulnerabilidades técnicas
SISTEMAS OPERATIVOS	[E.20]Vulnerabilidades de los programas (software)	A. 12 Seguridad de	A. 12.6.1 Gestión de vulnerabilidades técnicas

		las operaciones	
UPS	[A.25] Robo de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
GENERADOR ELÉCTRICO	[A.25] Robo de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
EQUIPOS DE CLIMATIZACIÓN	[A.25] Robo de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
MOBILIARIO	[A.25] Robo de equipos	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
PERSONAL ADMINISTRATIVO	[A.28] Indisponibilidad del personal	A. 7 Seguridad relativa a los recursos humanos	A. 7.1.1 Investigación de antecedentes
PERSONAL DE DESARROLLO	[A.28] Indisponibilidad del personal	A. 7 Seguridad relativa a los recursos humanos	A. 7.1.2 Términos y condiciones de empleo
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[E.1] Errores de los usuarios	A. 12 Seguridad de las operaciones	A. 12.1.1 Documentación de procedimientos de operación
CORREO INSTITUCIONAL	[A.6] Abuso de privilegios de acceso	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
CORREO INSTITUCIONAL	[A.7] Uso no previsto	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
UPS	[A.7] Uso no previsto	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
GENERADOR ELÉCTRICO	[A.7] Uso no previsto	A. 7 Seguridad relativa a los	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información

		recursos humanos	
EQUIPOS DE CLIMATIZACIÓN	[A.7] Uso no previsto	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
MOBILIARIO	[A.7] Uso no previsto	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
MATERIAL IMPRESO	[E.1] Errores de los usuarios	A. 8 Gestión de activos	A. 8.2.1 Clasificación de la información
SOPORTE DE RED	[E.1] Errores de los usuarios	A. 12 Seguridad de las operaciones	A. 12.1.1 Documentación de procedimientos de operación
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[A.6] Abuso de privilegios de acceso	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[A.7] Uso no previsto	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
INSTALACIÓN DE RED DE DATOS	[I.4] Contaminación electromagnética	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
INSTALACIÓN DE RED ELÉCTRICA	[I.4] Contaminación electromagnética	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
UPS DEL CENTRO CABLEADO	[I.4] Contaminación electromagnética	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
ESPACIO FÍSICO DDTI	[I.4] Contaminación electromagnética	A. 11 Seguridad física y del entorno	A. 11.2.1 Emplazamiento y protección de equipos
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[E.19] Fugas de información	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
ETHERNET	[A.12] Análisis de tráfico	A. 13 Seguridad de las	A. 13.2.1 Políticas y procedimientos de transferencia de información

		comunicaciones	
RED INALAMBRICA	[A.12] Análisis de tráfico	A. 13 Seguridad de las comunicaciones	A. 13.2.1 Políticas y procedimientos de transferencia de información
RED LAN	[A.12] Análisis de tráfico	A. 13 Seguridad de las comunicaciones	A. 13.2.1 Políticas y procedimientos de transferencia de información
RED TELEFÓNICA	[A.12] Análisis de tráfico	A. 13 Seguridad de las comunicaciones	A. 13.2.1 Políticas y procedimientos de transferencia de información
SOPORTE DE RED	[A.7] Uso no previsto	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
MATERIAL IMPRESO	[A.7] Uso no previsto	A. 7 Seguridad relativa a los recursos humanos	A. 7.2.2 Concienciación, educación y capacitación en seguridad de la información
ARCHIVO DE DATOS	[E.15] Alteración de la información	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
DOCUMENTACIÓN INTERNA	[E.15] Alteración de la información	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
CARPETAS COMPARTIDAS	[E.15] Alteración de la información	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras
ARCHIVO DE DATOS	[E.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
DOCUMENTACIÓN INTERNA	[E.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
CARPETAS COMPARTIDAS	[E.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
MATERIAL IMPRESO	[E.15] Alteración de la información	A. 11 Seguridad física y del entorno	A. 11.1.5 El trabajo en áreas seguras

SOPORTE DE RED	[E.15] Alteración de la información	A. 12 Seguridad de las operaciones	A. 12.4.1 Registro de eventos
BASE DE DATOS	[E.15] Alteración de la información	A. 12 Seguridad de las operaciones	A. 12.4.1 Registro de eventos
BASE DE DATOS	[E.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
FIREWALL	[E.4] Errores de configuración	A. 12 Seguridad de las operaciones	A. 12.1.2 Gestión de cambios
FIREWALL	[E.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.2 Acceso a redes y servicios de red
ETHERNET	[E.15] Alteración de la información	A. 12 Seguridad de las operaciones	A. 12.4.1 Registro de eventos
RED INALAMBRICA	[E.15] Alteración de la información	A. 12 Seguridad de las operaciones	A. 12.4.1 Registro de eventos
RED LAN	[E.15] Alteración de la información	A. 12 Seguridad de las operaciones	A. 12.4.1 Registro de eventos
RED TELEFÓNICA	[E.15] Alteración de la información	A. 12 Seguridad de las operaciones	A. 12.4.1 Registro de eventos
CORREO INSTITUCIONAL	[E.15] Alteración de la información	A. 12 Seguridad de las operaciones	A. 12.4.1 Registro de eventos
SOPORTE A LOS SERVICIOS INFORMÁTICOS	[E.15] Alteración de la información	A. 12 Seguridad de las operaciones	A. 12.4.1 Registro de eventos
PERSONAL ADMINISTRATIVO	[E.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
PERSONAL DE DESARROLLO	[E.18] Destrucción de la información	A. 9 Control de acceso	A. 9.1.1 Política de control de acceso
DISPOSITIVOS DE ALMACENAMIENTO	[I.11] Emanaciones electromagnéticas (TEMPEST)	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales

COMPUTADORAS	[I.11] Emanaciones electromagnéticas (TEMPEST)	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
TELÉFONOS IP	[I.11] Emanaciones electromagnéticas (TEMPEST)	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
SERVIDORES	[I.11] Emanaciones electromagnéticas (TEMPEST)	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
EQUIPO PARA EL FUNCIONAMIENTO DE RED	[I.11] Emanaciones electromagnéticas (TEMPEST)	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
EQUIPO MULTIFUNCIONAL	[I.11] Emanaciones electromagnéticas (TEMPEST)	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
DISPOSITIVO DE GRABACIÓN Y FOTOGRAFÍA	[I.11] Emanaciones electromagnéticas (TEMPEST)	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales
RADIOS DE COMUNICACIÓN	[I.11] Emanaciones electromagnéticas (TEMPEST)	A. 11 Seguridad física y del entorno	A. 11.1.4 Protección contra las amenazas externas y ambientales

Nota: Elaboración propia

Anexo 9: Material Capacitaciones

DIAPOSITIVAS

SEGURIDAD VS. INFORMÁTICA

Son las estructuras de las tecnologías de la información que sobrellevan las viviendas u organizaciones.

SEGURIDAD DE LA INFORMACIÓN

Se refiere a la protección de los activos de la información y con ello lograr éxito y continuidad en la organización.

- La seguridad de la información es la protección a la información que puede ser comprometida por diversas razones, por este motivo se encarga de garantizar la continuidad del negocio y minimizar los posibles riesgos.
- La implementación de controles al ser analizados, monitoreados y mejorados, se convierte en la herramienta que asegura la información.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

Es una herramienta que se encarga de proteger la seguridad de la información, para ello la norma ISO 27001 ayuda a indentificar, conocer y minimizar los riesgos que afectan a la confidencialidad, disponibilidad e integridad de la información, a través de procedimientos, controles y políticas implementadas para disminuir los riesgos organizacionales.


DEFINICIÓN DE TÉRMINOS
ACTIVO
Información indispensable que proteje los riesgos y las amenazas en las organizaciones.
AMENAZA
Elemento o acción que ocasiona peligro o daños a los usuarios, hardware o datos.
VULNERABILIDAD
Activo o control que puede ser provocado por una o más amenazas y causar daños irreparables.
RIESGO
Posibilidad de que una amenaza explote una vulnerabilidad de uno o varios activos


LA TRIADA DE LA SEGURIDAD
Confidencialidad
Con un adecuado uso de los recursos se evita la divulgación de la información y el acceso será completamente personal.
Integridad
Garantiza la consistencia y no modificcación de la información por parte de porsonas no autorizadas.
Disponibilidad
Permite que la información sea accesible y esté disponible para el personal autorizado.

02

MÉTODOS PARA OBTENER INFORMACIÓN

INGENIERÍA SOCIAL

1

INVESTIGACIÓN

La ciberdelincuencia se da cuando el delincuente indaga la información más útil sobre la victima.

2

GANCHO

A través de la manipulación la víctima confía en el delincuente y él empieza a tomar control de la situación.

3

EJECUCIÓN

El plan comienza a ser ejecutado y la victima facilita lainformación que se ordene.

4

SALIDA

Al conseguir el objetivo, el atacante borra toda sus huellas.

INGENIERÍA SOCIAL

"Es la práctica de obtener información confidencial a través de la manipulación de las personas"

PREVENCIÓN

- Ser precavido al entregar información personal para actividades sociales como rifas o encuestas, sobre todo si le están preguntando datos personales o contraseñas.
- No se deje intimidar para entregar información mediante llamadas telefónicas extrañas, procure solicitar datos de su interlocutor, no confíe fácilmente.

PHISHING

1

INFECCIÓN

El atacante aloja el paquete fraudulento en la red zombi.

2

EJECUCIÓN

La victima accede a la pagina falsa e ingresa los datos de su tarjeta de crédito.

3

SALIDA

La ciberdelincuencia comercializa los datos y obtiene ganancia.

PHISHING

"Duplicación ilegal de una pagina web que tiene como objetivo adquirir información confidencial de manera fraudulenta"

PREVENCIÓN

- No confíe en cualquier correo electrónico que solicite datos personales, cerciórese que la fuente sea segura.
- No ingresar a sitios web por medio de correos electrónicos o paginas no confiables, es recomendable escribir en el navegador el sitio al que desea ingresar.

SPAM

1

ENVÍO

El atacante envía varios correos, en alguno de ellos contiene un virus o enlaces a paginas ilegales.

2

RECEPCIÓN

La víctima recibe el mensaje que envió el ciberdelincuente.

3

DESCUBRIR

La victima abre el correo y el virus afecta al computador directamente o por medio del enlace

SPAM

"Hace referencia al envío de correo electrónico masivo no solicitado"

PREVENCIÓN

- Tener dos cuentas de correo electrónico, uno de uso personal y otro de uso público.
- Utilizar en el computador Software Antispam.
- No compartir los mensajes masivos, leer bien los mensajes recibidos antes de abrir y no aceptar comunicaciones corporativas

MALWARE (TROYANO)

1 **INSERTAR**

El ciberdelincuente oculta la alicación maliciosa en aplicaciones aparentemente legítimas.

2 **DESCARGAR**

La víctima descarga la aplicación por medio de un sitio web.

3 **INFECCIÓN**

La victima pone en ejecución la aplicación y el malware inmediatamente infecta el computador

MALWARE (TROYANO)

"Programa malicioso que tiene como objetivo infiltrarse en una computadora para obtener datos o dañarla"

PREVENCIÓN

- Instalar un buen antivirus y mantener el sistema operativo actualizado.
- En caso de que se utilice Windows es recomendable tener una cuenta de administrador para gestionar el sistema y otra para realizar trabajos y distracción.
- Procurar usar un cifrado WPA o WPA2 para la red WifI.
- Es importante ocultar SSID es decir, el nombre de la red WiFi.

DUMPSTER DIVING

1

CREACIÓN

La víctima generación y almacena su información confidencial.

2

DESECHO

Fase de desecho de la información confidencial.

3

MUESTRA

El atacante utiliza la infomacióon desechada con la finalidad de suplantar la identidad y producir fraude.

4

SALIDA

El atacante consigue el objetivo de obtener la información.

DUMPSTER DIVING

"Buscar entre la basura información confidencial con el fin de suplantar la identidad de alguien o realizar fraude"

PREVENCIÓN

- Restrinja su información confidencial a través de un mecanismo seguro, en el caso de no conseguirlo destruya los documentos físicos que contengan información personal o laborales como memorandos, recibos de pago, extractos bancarios, entre otros.

SHOULDER SURFING

1

REGISTRO

Al encender el computador la victima procede a ingresar sus credenciales.

2

EJECUCIÓN

El atacante observa a la victima cautelosamente y memoriza las credenciales.

3

SALIDA

Finalmente el objetivo se cumple, el atacante obtiene la información de la victima


SHOULDER SURFING
"Esta técnica implica simplemente mirar por encima del hombro de la víctima para obtener una contraseño o dato confidencial"
PREVENCIÓN
Colocar filtros de privacidad en todos los dispositivos tecnológicos, esto ayudará a eliminar la visibilidad lateral de las pantallas puesto a que es un plástico polarizado.
Utilizar un administrador de contraseñas o incluso autenticación en dos paso, conectado con el dispositivo móvil.
Si se encuentra en un lugar público se recomienda sentarse de espaldas a la pared para formar una barrera y su información personal no pueda ser visible fácilmente.


03
LEYES Y REGULACIONES

LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTE PERSONAL

Prioriza el derecho obligatio de las personas a conocer, actualizar y rectificar las informaciones que se hayan recopilado sobre ellas, mediante bases de datos y archivos tratados por entidades publicas o privadas.

LEY ESPECIAL DE TELECOMUNICACIONES

Su objetivo se basa en mejorar el servicio de sistemas radioeléctricos y telecomunacionales, por medio de la instalación, operación, utilización y desarrollo de la transmisión, emisión o recpeción de todos los sistemas electromagnéticos.

LEY DE PROPIEDAD INTELECTUAL

Enfocado en tres direcciones principales:

- La Dirección Nacional de propiedad Industrial protege marcas, logos o lemas con la ayuda de patentes, las mismas que otorgan exclusividad durante 20 años.
- La Dirección Nacional de derecho de autor brinda respaldo a obras literarias, artísticas, musicales, entre otras, siempre y cuando sean inéditas y se encuentren publicadas.
- La Dirección de obtención vegetal y conocimientos tradicionales, defienden los haberes de naciones, pueblos indígenas, afroecuatorianos, montubios y campesinos transmitidos de generación en generación.

LEY DE FIRMA ELECTRÓNICA

- At. 13.- Firma electrónica: Son los datos en forma electrónica consignados en un mensaje de datos, utilizada para que el titular apruebe y reconozca la información contenida.
- Art. 14.- Efectos de la firma electrónica: La firma tendrá igual validez y se reconocerá con el mismo efecto jurídico al de una firma manuscrita y será admitida como prueba en juicio.

LEY DE FIRMA ELECTRÓNICA

- At. 15.- Requisitos de la firma electrónica: para su validez la firma electrónica reunirá los siguientes requisitos:

a) Ser individual y estar vinculada exclusivamente al titular.
b) Verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación.
c) Su método de creación y verificación debe ser confiable, seguro e inalterable.

LEY DE FIRMA ELECTRÓNICA

- At. 17.- Obligaciones del titular de la firma electrónica:

a) Cumplir con las obligaciones derivadas del uso de la firma electrónica.
b) Actuar con la debida diligencia y tomar las medidas de seguridad necesarias para evitar utilización no autorizada.
c) Verificar la exactitud de sus declaraciones.
d) Responder por las obligaciones derivadas del uso no autorizado de su firma y solicitar oportunamente la cancelación de los certificados.

Nota: Elaboración propia

INFOGRAFÍAS

[ESCRITORIO ORGANIZADO]

1. Guardar en cajones bajo llaves los documentos importantes, tablets o celulares, cuando no este en uso.
2. No dejar a la vista documentos que tengan datos confidenciales y datos personales de los funcionarios públicos y cualquier información importante.
3. Cuidar los dispositivos de respaldo de información como USB, CD o discos duros, con la finalidaad de evitar acceso a cualquier persona.

4. Evitar mantener iniciada la sesión en el equipo cuando se ausenta del puesto de trabajo por tiempo prolongado.
5. No pegar autoadhesivos ni figuras en las pantallas de la computadora que contenga contraseñas.

CONTRASEÑA SEGURA

1. Evitar el uso de nombres, fechas de nacimiento o cualquier dato personal similar.

2. Debe incluis mayúsculas, minúsculas, carácteres especiales y números.

3. No debe ser tan facil de decifrar ni tampoco tan dificil de recordar. Utiliza un nivel de complejidad correcto para ti.

4. La longitud de las contraseñas alfabnuméricas deben ser mínimo 8 carácteres, y 6 para numéricas.

Nota: Elaboración propia

Anexo 10: Formato Evaluación Capacitaciones

UNIVERSIDAD TÉCNICA DEL NORTE
UNIVERSIDAD ACREDITADA RESOLUCIÓN 002-CONEA-2010-129-DC
Resolución No 001-073 CEAACES – 2013 – 13
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

Seguridad de la Información

El presente cuestionario tiene como finalidad de reflejar lo aprendido en la sesión 1 sobre Seguridad de la Información. En las preguntas que se presenta a continuación se sebe marcar solo una respuesta.

1. **¿Qué es un ataque de phishing?**

   a) Un virus que se propaga a través de correos electrónicos
   b) Un intento de engañar a alguien para que revele información confidencial
   c) Una técnica de hacking que utiliza un software malicioso

2. **¿Qué es un software antivirus?**

   a) Un software que ayuda a proteger su ordenador de virus y otros programas maliciosos
   b) Un software que se utiliza para realizar copias de seguridad de archivos importantes
   c) Un software que le ayuda a navegar por Internet de forma segura

3. **¿Qué es el cifrado?**

   a) Un proceso que convierte datos legibles en un código secreto
   b) Un proceso que elimina los datos de un ordenador
   c) Un proceso que realiza copias de seguridad de datos importantes

4. **¿Qué es un cortafuegos?**

   a) Un software que ayuda a bloquear el acceso no autorizado a su red
   b) Un software que le ayuda a enviar correos electrónicos de forma segura
   c) Un software que le ayuda a proteger su ordenador de virus y otros programas maliciosos

5. **¿Qué es la ingeniería social?**

   a) Un conjunto de técnicas utilizadas para manipular a las personas para que divulguen información confidencial
   b) Un software que ayuda a proteger su ordenador de virus y otros programas maliciosos
   c) Una técnica utilizada para realizar copias de seguridad de archivos importantes

6. **¿Qué es la autenticación de dos factores?**

a) Un proceso que requiere dos formas diferentes de identificación para acceder a un sistema
b) Un proceso que ayuda a proteger su ordenador de virus y otros programas maliciosos
c) Un proceso que se utiliza para eliminar datos de un ordenador

7. ¿Qué es un ataque de denegación de servicio (DoS)?

a) Un ataque que intenta hacer que un sitio web o servidor se vuelva inaccesible para los usuarios legítimos
b) Un ataque que se propaga a través de correos electrónicos
c) Una técnica de hacking que utiliza un software malicioso

8. ¿Qué es la seguridad física?

a) Un conjunto de medidas que se utilizan para proteger el acceso físico a los recursos de la información
b) Un conjunto de medidas que se utilizan para proteger los datos importantes en línea
c) Un conjunto de medidas que se utilizan para proteger el software de virus y otros programas maliciosos

9. ¿Qué es el phishing de suplantación de identidad?

a) Un intento de engañar a alguien haciéndose pasar por una entidad legítima para que revele información confidencial
b) Un virus que se propaga a través de correos electrónicos
c) Una técnica utilizada para proteger los datos importantes en línea

10. ¿Qué es un certificado SSL?

a) Un certificado que se utiliza para cifrar la información entre el servidor web y el navegador del usuario.
b) Un software que se utiliza para realizar copias de seguridad de archivos importantes.
c) Un software que le ayuda a enviar correos electrónicos de forma segura

Anexo 11: Cuestionario Inicial Validación con el Método Delphi

UNIVERSIDAD TÉCNICA DEL NORTE
UNIVERSIDAD ACREDITADA RESOLUCIÓN 002-CONEA-2010-129-DC
Resolución No 001-073 CEAACES – 2013 – 13
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

Cuestionario Inicial

El presente cuestionario tiene como finalidad recolectar información sobre distintos puntos relevantes al Diseño del Sistema de Gestión de Seguridad de la Información para el Departamento de Desarrollo Tecnológico e Informático (DDTI) de la Universidad Técnica del Norte (UTN).

1. **¿Cree usted que es indispensable que se implemente un Diseño de Sistema de Gestión de Seguridad de la Información para el DDTI-UTN?**

    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

2. **¿Estaría de acuerdo en que el informe sobre el Diseño del Sistema de Gestión de la Seguridad de la Información para el DDTI-UTN se escribió de manera clara y comprensible?**

    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

3. **¿Está de acuerdo en que el Diseño de un Sistema de Gestión de la Seguridad de la Información para el DDTI-UTN cuenta con los datos esenciales?**
    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

4. **¿Considera que se da cumplimiento a los objetivos principales del Diseño del Sistema de Gestión de la Seguridad de la Información para el DDTI-UTN?**

    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

5. **¿Considera que los procedimientos implementados durante la creación de un Sistema de Gestión de la Seguridad de la Información para el DDTI-UTN fueron adecuados y suficientes?**
    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

6. **¿Considera esencial que se realice evaluaciones sobre las capacitaciones del Sistema de Gestión de la Seguridad de la Información para el DDTI-UTN?**
    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

7. **¿En su opinión, las tareas propuestas a manera de controles para la mitigación de riesgos en el Diseño de un Sistema de Gestión de la Seguridad de la Información para el DDTI-UTN fueron las idóneas?**
    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

8. **¿Considera que las tareas asignadas como controles para reducir riesgos en la implementación de un Sistema de Gestión de la Seguridad de la Información en el DDTI-UTN fueron apropiadas según su criterio?**
    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

9. **¿Cree usted que el Sistema de Gestión de la Seguridad de la Información creado específicamente para el DDTI-UTN podría ser utilizado con éxito en otras instituciones de educación superior?**
    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo
10. **¿Cree usted que las políticas de seguridad implementadas para la creación de un Sistema de Gestión de Seguridad de la Información del DDTI-UTN fueron idóneas?**

6) Totalmente de acuerdo
7) De acuerdo
8) Indiferente o neutro
9) En desacuerdo
10) Totalmente en desacuerdo

11. ¿Considera que mediante el plan de tratamiento de riesgos implementado se garantiza la confidencialidad, integridad y disponibilidad de la información en el Sistema de Gestión de la Seguridad de la Información del DDTI-UTN?

11) Totalmente de acuerdo
12) De acuerdo
13) Indiferente o neutro
14) En desacuerdo
15) Totalmente en desacuerdo

12. ¿Cree usted que mediante las acciones de los directivos y los controles establecidos se puede garantizar el cumplimiento de las normas y regulaciones de un Sistema de Gestión de Seguridad de la Información del DDTI-UTN?

16) Totalmente de acuerdo
17) De acuerdo
18) Indiferente o neutro
19) En desacuerdo
20) Totalmente en desacuerdo

13. ¿ Considera usted que se puede garantizar que un Sistema de Gestión de Seguridad de la Información del DDTI-UTN sea escalable y adaptable a los cambios en el entorno tecnológico y empresarial mediante la evaluación continua, una adecuada capacitación y la integración de estándares?

21) Totalmente de acuerdo
22) De acuerdo
23) Indiferente o neutro
24) En desacuerdo
25) Totalmente en desacuerdo

14. ¿ En su opinión, está de acuerdo que mediante el Diseño de un Sistema de Gestión de Seguridad de la Información del DDTI-UTN se puede minimizar los impactos que podrían resultar si se produce una violación de seguridad ?

26) Totalmente de acuerdo
27) De acuerdo
28) Indiferente o neutro
29) En desacuerdo
30) Totalmente en desacuerdo

15. **¿ Modificaría algún componente del plan de acción diseñado para el Sistema de Gestión de la Seguridad de la Información del DDTI-UTN? En caso afirmativo, ¿cuál sería el elemento que se propondría cambiar?**

_____
_____
____

Anexo 12: Cuestionario Final Validación con el Método Delphi

UNIVERSIDAD TÉCNICA DEL NORTE
UNIVERSIDAD ACREDITADA RESOLUCIÓN 002-CONEA-2010-129-DC
Resolución No 001-073 CEAACES – 2013 – 13
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

Cuestionario Inicial

El presente cuestionario tiene como finalidad recolectar información sobre distintos puntos relevantes al Diseño del Sistema de Gestión de Seguridad de la Información para el Departamento de Desarrollo Tecnológico e Informático (DDTI) de la Universidad Técnica del Norte (UTN).

1. **¿ Considera que las políticas de Mejora Continua que se han establecido en el Diseño del Sistema de Gestión de la Seguridad de la Información están acordes con el DDTI-UTN?**

    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

2. **¿ Estaría de acuerdo en que el uso la norma ISO/IEC 27001:2013 fue acertada para el Diseño de un Sistema de Gestión de la Seguridad de la Información para el DDTI-UTN ?**

    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

3. **¿ Está de acuerdo en que el Monitoreo Continuo es fundamental para mejorar el Sistema de Gestión de la Seguridad de la Información para el DDTI-UTN?**
    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro

4) En desacuerdo
5) Totalmente en desacuerdo

4. **¿ Considera usted que, en respuesta al enfoque de Mejora Continua, sea acertado plantear un seguimiento por lo menos una vez al año en el Departamento de Desarrollo Tecnológico e Informático de la UTN?**

    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

5. **¿Considera que los cambios en el Informe del Sistema de Gestión de la Seguridad de la Información desarrollados para el Departamento de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte fue adecuado y suficientes a fin de mejorar la calidad de este, tomando en cuenta las consideraciones extraídas del análisis del primer cuestionario?**
    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

Anexo 13: Certificado de recepción por parte del director del DDTI

REPUBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

DEPARTAMENTO DE DESARROLLO TECNOLÓGICO E INFORMÁTICO

CERTIFICACIÓN

Ibarra 01 de junio de 2023

Certifico haber recibido el CONTENIDO y FORMATO del trabajo de titulación denominado: **DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA EL DEPARTAMENTO DE DESARROLLO TECNOLÓGICO E INFORMÁTICO DE LA UNIVERSIDAD TÉCNICA DEL NORTE BASADO EN LA NORMA ISO/IEC 27001,** desarrollado por el señor Stalin Santiago Guzmán Iles con número de cédula 1003557715.

Atentamente,

MSc. Jorge Caraguay

Director DDTI

Av. 17 de Julio s-21 y José María Córdova
Ciudadela Universitaria Barrio El Olivo
Teléfono: (06)2997800 Casilla 199
E-mail: info@utn.edu.ec
www.utn.edu.ec
Ibarra - Ecuador