UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

"PLAN DE SEGURIDAD PARA LA GESTIÓN DE RIESGOS EN EL DATACENTER DE LA FACULTAD DE INGENIERA EN CIENCIAS APLICADAS CON LA METODOLOGÍA MAGERIT V3.0"

AUTOR(A): VANESSA MARILYN JÁCOME CHÁVEZ

DIRECTOR: MSC. JAIME ROBERTO MICHILENA CALDERÓN

IBARRA-ECUADOR

2019

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:	100296982-0		
APELLIDOS Y NOMBRES:	Jácome Chávez Vanessa Marilyn		
DIRECCIÓN:	Yacucalle, Miguel Sánchez 2-54 y Tobías Mena		
EMAIL:	vmjacomec@utn.edu.ec		
TELÉFONO FIJO:	062906245	**TELÉFONO MÓVIL:**	0960945442

DATOS DE LA OBRA	
TÍTULO:	PLAN DE SEGURIDAD PARA LA GESTIÓN DE RIESGOS EN EL DATACENTER DE LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS CON LA METODOLOGÍA MAGERIT V3.0
AUTOR (ES):	Jácome Chávez Vanessa Marilyn
FECHA:	
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	[x] **PREGRADO** [ ] **POSGRADO**
TITULO POR EL QUE OPTA:	Ingeniera en Electrónica y Redes de Comunicación
ASESOR /DIRECTOR:	Ing. Jaime Roberto Michilena Calderón. MSc.

2. CONSTANCIAS

El autor manifiesta 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 el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 27 días del mes de Marzo de 2019

EL AUTOR(A):

.....

Vanessa Marilyn Jácome Chávez

CI. 1002969820

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, Vanessa Marilyn Jácome Chávez con cédula de ciudadanía Nro. 100296982-0 manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador artículos 4, 5 y 6, en calidad de autor del trabajo de grado con el tema: "PLAN DE SEGURIDAD PARA LA GESTIÓN DE RIESGOS EN EL DATACENTER DE LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS CON LA METODOLOGÍA MAGERIT V3.0". Que ha sido desarrollado con el propósito de obtener el título de Ingeniera en Electrónica y Redes de Comunicación de la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autora me reserva los derechos morales de la obra antes citada. En concordancia suscribo en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

.....

Vanessa Marilyn Jácome Chávez
100296982-0
Ibarra, marzo de 2019

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

MAGISTER JAIME MICHILENA, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN CERTIFICO:

Que, el presente Trabajo de Titulación "PLAN DE SEGURIDAD PARA LA GESTIÓN DE RIESGOS EN EL DATACENTER DE LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS CON LA METODOLOGÍA MAGERIT V3.0". Ha sido desarrollado por la señora Vanessa Marilyn Jácome Chávez bajo mi supervisión.

Es todo cuanto puedo certificar en honor a la verdad.

.....

Ing. Jaime Michilena, MSc.
DIRECTOR

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DEDICATORIA

Este proyecto de titulación, lo dedico con mucho amor a mi madre y a la memoria de mi padre que con su trabajo, esfuerzo y sacrificio, me dieron la oportunidad de estudiar, además por el apoyo incondicional y la fe que mi madre tuvo en mí.

A mis hijos Pablo Andrés y Jorge Andrés; que son, los dos amores de mí vida, la motivación por la que me levanto cada día, siendo mi inspiración para superarme.

A hermanos Jacqueline, Fabián y Jairo por ser un pilar muy importante en mi vida, porque nunca me dejaron caer cuando me vieron vencida, por el ánimo y palabras de aliento, que me motivaron a continuar. A mis sobrinos Nidia, Matheo, Keyla, Aly y Ainoha que me transmitieron día a día un pedacito de su alegría.

A todos los que pusieron un granito de arena para que este esfuerzo valga la pena.

Vanessa Jácome

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

AGRADECIMIENTO

Agradezco a Dios, por las pruebas que pone en mi camino y las fuerzas que me da para superarlas. Y por cada una de las oportunidades que me da para corregir mis errores y emendar mi camino. Y así, cumplir con los planes que él tiene para mí.

A mi familia, por nunca perder la fe en mí, y haber sido un apoyo incondicional a lo largo de toda mi vida.

A la Universidad Técnica del Norte, a todos los docentes y amigos de la Carrera de Ingeniería en Electrónica y Redes de Comunicación que fueron parte a lo largo de mi vida universitaria, siendo una ayuda valiosa durante todo este camino.

A mi director de Trabajo de Grado MSc. Jaime Michilena, que más que un docente fue un amigo, brindándome su apoyo y tiempo para el desarrollo y culminación de este proyecto.

De la misma manera agradecer a mis opositores MSc. Mauricio Dominguez y MSc. Fabián Cuzme; a mis amigos MSc. Fernado Ortiz, Ing. Jenny Villegas e Ing. Diana Guerrero, por su ayuda y colaboración a lo largo de este proceso, con el aporte de sus conocimientos y experiencia.

Gracias a todos.

Vanessa Jácome.

RESUMEN

La seguridad de la información es un tema importante que abarca un conjunto de técnicas y actividades que una organización debe adoptar para resguardar la información que maneja, para que no sea mal utilizada, robada, divulgada o borrada; y no afecte a su disponibilidad, integridad o confidencialidad.

El Data Center de la Facultad de Ingeniería en Ciencias Aplicadas tiene implementado una infraestructura que maneja información importante para la facultad; pero no se aplican políticas, ni procedimientos lo cual pone en riesgo la información y a los activos que lo procesan.

Magerit es una metodología que permite realizar el análisis y gestión de riesgos mediante un proceso sistemático; mediante la aplicación de esta metodología se logra definir paso a paso cada uno de estos procesos, con la finalidad de mejorar la seguridad de la información en el Data Center de la FICA. Inicialmente se recopiló información relevante del Data Center, determinando los activos importantes mediante una entrevista al técnico encargado; luego se procede a evaluar estos activos en la herramienta PILAR (herramienta sugerida por la metodología Magerit para análisis y gestión de riesgos), concluyendo que las salvaguardas existentes no eran las suficientes para evitar que una amenaza se materialice, poniendo a la información en riesgo potencial.

Después de haber determinado los riesgos, se propone un Plan de Seguridad, que sugiere una guía, que permitirá gestionar los riesgos latentes identificados en el Data Center de la Facultad de Ingeniería Ciencias Aplicadas; como parte de este plan se establecen políticas y procedimientos, basados en los controles que define la norma ISO/IEC 27002; además se plantea un plan de acción donde se estipulan actividades, responsables y tiempos, que con el apoyo de las autoridades y responsables del Data Center, pueda llegar a ejecutarse, para tener

un ambiente controlado y organizado, donde la seguridad de la información sea el principal propósito.

Palabras calve: Seguridad de la Información, Magerit, ISO/IEC 27002, Análisis y gestión de riesgos.

ABSTRACT

Information security is a practice that require a set of techniques and activities that an organization must adopt to safeguard the information it handles, so that it is not misused, stolen, disclosed or deleted; without affecting its availability, integrity or confidentiality.

The Data Center of the Faculty of Engineering in Applied Sciences (FICA) has an infrastructure that handles important information, though the policies and procedures to safeguard information are not applied, putting at risk the processed information and Data Center facilities.

The Magerit methodology allows analysis and risk management through a systematic process; by the application of this methodology, each of these processes is defined step by step to improve information security in the FICA Data Center. Initially, relevant information from the Data Center was collected, determining the important assets through an interview with the technician in charge; then these assets were evaluated with PILAR (tool suggested by the Magerit methodology), concluding that the existing safeguards were not enough to prevent a threat.

Once the risks were determined, a Safety Plan is proposed, by means a guide to manage the identified risks in the Data Center of the Faculty; as part of this proposal, policies and procedures are established, based on the controls defined by ISO / IEC 27002; in addition, a plan of action is proposed, with activities, responsibilities and times, which with the support of the Faculty authorities and Data Center managers, can be applied, to have a well-managed environment, where information security is the main objective.

Keywords: Information Security, Magerit, ISO / IEC 27002, Analysis and risk management.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ECUACIONES

Capítulo 1

Antecedentes

En este capítulo se describe el problema que se va a resolver, los objetivos que se van a cumplir, el proceso que se va a realizar para alcanzar la solución y el porque es importante tratar este tema.

1.1. Problema

La Facultad de Ingeniería en Ciencias Aplicadas cuenta con un Data Center en el cual, se da apertura, de que estudiantes como ingenieros puedan plantear proyectos que aporten mejoras en el mismo. El Data Center fue sometido a varios cambios en su infraestructura, tanto físicos como lógicos con el fin de aumentar la disponibilidad de los servicios. Uno de los cambios más relevantes es la virtualización de los servidores.

La reingeniería a la que se sometió la red del Data Center es innovadora, pero eso no quiere decir, que garantiza la seguridad de la información. Dentro de la administración del Data Center no existe un proceso a seguir, para resguardar la información o sus activos. La falta de mantenimiento a su entorno y a los soportes de información, la han puesto en peligro. Además, no tiene una normativa que establezca el control del personal que tiene acceso a este espacio, poniendo en riesgo a la información. Lo anteriormente mencionado, son vulnerabilidades percibidas a primera vista que tiene el Data Center, siendo un blanco perfecto para que una amenaza se materialice.

Es necesario realizar el análisis y gestión de riesgos para identificar las amenazas y vulnerabilidades a la que está expuesta la red. Usando la metodología Magerit, la cual permita desarrollar un método sistemático para analizar tales riesgos. Con el cual, se pueda implementar planes de seguridad, que su ejecución permita mejorar la seguridad de la información.

Toda organización está expuesta a ataques y más aún un entorno donde se albergar un sistema de información de componentes asociados, como es el Data Center de la FICA, siendo este un blanco perfecto para ello. Por ende es necesario contar con un método que permita identificar y minimizar el riesgo al que está expuesto la información.

1.2. Objetivos

1.2.1. Objetivo General

Desarrollar un Plan de Seguridad para la gestión de riesgos en el Data Center de la Facultad de Ingeniería en Ciencias Aplicadas con la metodología Magerit v3.0, para mejorar la seguridad de la información.

1.2.2. Objetivos Específicos

- Investigar información sobre la gestión de riesgos, seguridad de la información y Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Magerit).
- Analizar la situación actual del Data Center de la FICA e identificar los activos más significativos que posee el Data Center, mediante entrevistas y encuestas al personal directamente relacionado con esta área.
- Identificar las amenazas y vulnerabilidades al que están expuestos los activos críticos y evaluar el riesgo e impacto sobre ellos.
- Escoger salvaguardas apropiadas para los activos más importantes del Data Center.
- Elaborar un plan de seguridad, donde se establezcan procedimientos para disminuir los riesgos a los que están expuestos los activos críticos.

1.3. Justificación

La seguridad de la información consiste en preservar la confidencialidad, integridad y disponibilidad de la información. Y esto depende mucho de cómo se gestiona los riesgos en la red que maneja dicha información. Pretendiendo que la información de una organización no este comprometida, por ende no afecte los objetivos de la misma.

El análisis y gestión de riesgos tiene como propósito mejorar la seguridad de la información, y esto se consigue realizando un proceso sistemático, documentado y conocido por toda la organización (ISO/IEC 27000, 2005). Lo cual permite, que al presentarse un inconveniente se proceda con una acción rápida y efectiva, existiendo menos demoras en el proceso. Además, este sistema será un aporte muy importante que facilitará la administración de la red.

Existen varias metodologías en el medio para la gestión de riesgos, entre ellas se tiene COBIT e ITIL, que ofrece unas buenas prácticas y herramientas para el seguimiento y la gestión de las actividades de las Tecnologías de la Información (TI); COBIT ofrece un modelo de evaluación y monitoreo para el control y seguridad de una organización, que abarca controles específicos de TI desde una perspectiva de negocios e ITIL es un conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información, más orientada a la entrega de servicios TI al cliente. Magerit ofrece una metodología más detallada y comprensible para análisis y gestionar los riesgos, además de tener las mejores prácticas, ya que se basa en estándares reconocidos.

Magerit es una metodología de carácter público, perteneciente al Ministerio de Administraciones Públicas y fue elaborado por el Consejo Superior de Administración Electrónica. Ofrece una clasificación amplia de activos y describe métodos prácticos para la realización de análisis de los riesgos (Ministerio de Administraciones Públicas de España, 2005), por tal razón es la fundamental en este proyecto.

Magerit es la metodología de análisis de riesgos más completa, por sus años en el medio tiene madurez y es adaptable a cualquier tipo de organización; cuenta con tres libros que ejemplifican su metodología, ayudando a su mejor comprensión y es compatible con normas ISO 27005 e ISO 31010.

Con el desarrollo de esta metodología se pretende establecer un plan de seguridad, el cual ayudarán a controlar a medida de lo posible los riesgos. Lamentablemente, ningún método puede garantizar en su totalidad la seguridad de información, pero mediante este sistema de gestión de riesgos se puede garantizar que los riesgos sean conocidos, asumidos, gestionados y minimizados; mejorando la seguridad de la información y minimiza los daños en los activos de información.

Este proyecto forma parte esencial de los requerimientos para implementar un Sistema de Gestión de la Seguridad de la Información; por tanto puede ser tomado como punto de partida para futuras investigaciones dentro de este tema.

1.4. Alcance

El presente proyecto propone el análisis y gestión de riesgos en el Data Center de la Facultad de Ingeniería en Ciencias Aplicadas con la metodología Magerit v3.0. Siendo su propósito mejorar la seguridad de la información.

Se investiga información relevante para la realización de este proyecto de la metodología Magerit v3.0. Además se revisará contenido sobre la gestión de riesgos y seguridad de información que sea adecuada para el desarrollo y comprensión de este proyecto.

Antes de iniciar con la metodología se debe hacer una breve descripción de la situación actual y realizar un inventario del Data Center, para ser conocedores de como esta y como se maneja la infraestructura del mismo.

Para dar cumplimiento a la metodología se debe cumplir las siguientes etapas:

Primeramente se realiza un análisis del Data Center, para identificar los activos (información o servicios manejados por un sistema) de la red. La recolección de esta información se obtiene mediante encuestas y entrevistas a los usuarios responsables del Data Center, además se realizará una inspección física. Después de identificar los activos que componen el sistema, se definirá las dependencias entre ellos y se determinará el valor de cada uno, basado en los parámetros de confidencialidad, integridad, disponibilidad y autenticidad.

Posteriormente, se debe identificar las vulnerabilidades y amenazas relevantes que podrían afectar a los activos; se debe evaluar la probabilidad de que ocurra (riesgo) y estimar el daño que acusaría (impacto).

Finalmente, se debe identificar los activos críticos o los que poseen mayor nivel de riesgo y describir las salvaguardas efectivas para estos activos, las cuales, al dar su seguimiento permita mitigar el riesgo

Para el cumplimiento de estas etapas se utilizará la herramienta PILAR, que permite caracterizar y valorar los activos, caracterizar las amenazas y evaluar las salvaguardas.

Para concluir se desarrolla un plan de seguridad donde establecen políticas y procedimientos a seguir con las medidas de seguridad apropiadas, para evitar o mitigar las consecuencias no deseadas en los activos críticos basándose en las salvaguardas ya identificadas.

Capítulo 2

Fundamento Teórico

En este capítulo se detalla conceptos básicos sobre Seguridad de Información, análisis y gestión de riesgos, normativas y metodología para establecer las políticas; información que facilitará la comprensión de este proyecto.

2.1. Introducción

Cada día aumenta el uso del Internet y las actividades de muchas empresas dependen del buen funcionamiento de su sistema informático. Por tal razón, hay que tener control del acceso a estos sistemas, para poder brindar cierta seguridad a los componentes más importantes o valiosos de dicho sistema que maneja la información de una organización.

Lamentablemente ninguna organización está libre de ataques; de forma intencionada o no, hay intrusiones que se aprovechan de las vulnerabilidades existentes y ponen en peligro la información. Por lo cual, es necesario dotar a este sistema de ciertas medidas que brinden seguridad a nuestra información, no se puede tener un sistema 100% seguro, pero si uno adecuado.

Para conocer el estado actual de la seguridad que tiene el Data Center, es posible realizar un análisis y gestión de riesgos; mediante el cual se identifique las vulnerabilidades y amenazas existentes. Este diagnóstico permitirá tomar decisiones a largo y corto plazo que permitan mitigar ciertos riesgos a los que está expuesta dicha organización.

2.2. Seguridad de Información

La seguridad de la información se define como el conjunto de técnicas y actividades que adoptan las organizaciones para preservar la confidencialidad, integridad y disponibilidad de la información, así mismo se preocupa del resguardo y protección del sistema que lo procesa. (Garcia, 2011)

La seguridad de información de una empresa depende mucho de su organización y su personal, de que establezca reglas para que sólo el personal autorizado sea el que puede tener acceso a dicha información.

Es importante que las organizaciones tomen precauciones y manejen un adecuado sistema de seguridad, el cual ayude a mitigar los riesgos a los que está expuesto uno de sus activos más importantes, que es la información.

Por tal motivo, es necesario que las organizaciones elaboren planes de seguridad, creando medidas que no sólo resguarde la información, sino a sus recursos informáticos y en definitiva a sus usuarios.

2.2.1. Principios de la Seguridad

La seguridad de la información, se fundamenta en los principios básicos como los describe (Whitman & Mattord, 2011); los cuales son confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y no repudio, los mismos que se describen a continuación:

- **Confidencialidad**

Es la capacidad de un sistema informático de proporcionar la información solamente, al personal autorizado a acceder a ella. Esta característica debe proporcionar privacidad y proteger a dicho sistema, de invasiones, intrusiones y accesos, por parte de personas o programas no autorizados. (WORDPRESS, 2016)

Para asegurar en cierto grado la confidencialidad, se debe dotar de técnicas criptográficas para cifrar los datos que se consideren críticos.

- **Integridad de Datos**

La integridad de los datos es la protección que se debe dar a la información para que no sea modificada, duplicada o eliminada durante su transmisión o almacenamiento. Garantizando que la información sea la misma en todo momento, para ello es necesario técnicas criptográficas.

- **Disponibilidad**

Es la característica de la información, que le permite al usuario autorizado acceder a ella en el momento que requiera. La denegación o retardo del servicio, puede ser tomado como una violación a la disponibilidad.

- **Autenticidad**

Esta característica se encarga de asegurar la identidad de los entes que participan en una comunicación, es decir asegurar que la entidad es quien dice ser. La suplantación es el principal factor que pone en riesgo la autenticidad.

- **Trazabilidad**

Con este proceso se puede determinar las acciones que realizan los usuarios en un sistema informático, ya sea en un determinado tiempo o en tiempo real. (Jiménez, 2017)

El objetivo de esta característica es permitir que en todo momento se pueda determinar quién hizo qué y en qué momento, con la finalidad de poder conocer todos los incidentes y así poder analizarlos.

- **No repudio**

Este principio garantiza la participación de las partes en una comunicación. En toda comunicación, existe un emisor y un receptor, por lo que se puede distinguir dos tipos de no repudio:

- No repudio en origen: garantiza que la persona que envía el mensaje no puede negar que es el emisor del mismo, ya que el receptor tendrá pruebas del envío.
- No repudio en destino: El receptor no puede negar que recibió el mensaje, porque el emisor tiene pruebas de la recepción del mismo. Este servicio es muy importante en las transacciones comerciales por Internet, ya que incrementa la confianza entre las partes en las comunicaciones.

2.3. Análisis y Gestión de Riesgos

El análisis y gestión de riesgos, permite verificar la seguridad existente en una organización, identificar las causas de vulnerabilidades y proponer soluciones de control para minimizarlas.

Este es un proceso sistemático, ofrece actividades claves para resguardar la información y el sistema que la procesa. Permite seleccionar y establecer las medidas de seguridad apropiadas que ayudarán a controlar o eliminar los riesgos identificados dentro del sistema informático.

El diagnóstico permitirá en un futuro el diseño e implementación de un Sistema de Gestión de Seguridad de la Información - SGSI alineado al estándar ISO/IEC 27001, capaz de controlar las vulnerabilidades, amenazas y los riesgos de seguridad a que se ve expuesta la organización. (ISO 27000, 2017)

El análisis y gestión de riesgos es un proceso con el cual una organización puede identificar los riesgos a los que está expuesta, pero antes de iniciar con tal proceso se debe tener claro sus conceptos, los cuales se describen a continuación:

Según (Duque, 2010) "Análisis de riesgo es el proceso sistemático para estimar la magnitud de los riesgos al que está expuesta una Organización", mientras que "Gestión de riesgos es la selección e implementación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados".

Es importante en toda organización realizar un análisis y gestión de riesgos, el cual le permita conocer el estado de su red, sus vulnerabilidades y los riesgos a los que está expuesta la organización. Y a medida que la organización tenga claro a los riesgos que se enfrenta, podrá establecer políticas que le permitan tomar medidas preventivas y correctivas que garanticen un cierto grado de seguridad.

Toda organización en la actualidad tiene una alta dependencia de los sistemas informáticos, y están expuestas a diferentes riesgos. Esta situación se complica debido a que los controles adoptados por la mayoría de estas organizaciones aún no garantizan un estado de seguridad

aceptable. (CERTSUPERIOR, 2016) Y para que puedan continuar con sus actividades o negocios, se ven obligados a realizar un análisis y gestión de riegos, con el fin de conocer sus debilidades e implementar políticas qua ayuden a mitigarlos. Para llevar a cabo este proceso es necesaria la intervención de todo el personal, incluyendo a los directivos que deben avalar el proyecto y brindar el apoyo a todo el personal que esté involucrado en el manejo de los sistemas informáticos.

Existen muchas metodologías para realizar el análisis y gestión de riesgos de una organización, pero todas parten de un punto común: la identificación de activos de información, es decir todos aquellos recursos involucrados en la gestión de la información, que va desde datos y hardware, hasta documentos escritos y el recurso humano. (Tovar & María, 2015)

En el presente proyecto se muestra el proceso sistemático para realizar el análisis y gestión de riesgos; se evalúa el estado actual del Data Center de la FICA donde se identifica las vulnerabilidades, amenazas y riesgos, basándose en los criterios de confidencialidad, integridad y disponibilidad de la información, para luego establecer procedimientos y políticas que proporcionen una seguridad adecuada.

2.4. Metodologías para análisis y gestión de riesgos

Existen varias metodologías en el medio para la gestión de riesgos, entre ellas se tiene COBIT, ITIL y MAGERIT; que ofrecen buenas prácticas y herramientas para el seguimiento y la gestión de las actividades de las Tecnologías de la Información (TI). Según (Sánchez Zambrano, 2019) "La información se ha convertido en un activo vital para el éxito y continuidad de las actividades de cualquier organización. Por ende, el aseguramiento de dicha información y de los sistemas que lo procesan es un objetivo de primer nivel para la organización".

A continuación en la Tabla 1 se observa comparativo de los modelos COBIT, ITIL y MAGERIT basado en sus funciones, las áreas de cobertura, la organización que creo el modelo

y para que se implementa. Es importante concluir que un modelo no es mejor que otro; para que un modelo sea aplicable a una organización hay que evaluar el que mejor se ajuste a la organización.

Tabla 1

Comparativa entre COBIT, ITIL y MAGERIT

	COBIT	**ITIL**	**MAGERIT**
Funciones	Mapeo de procesos IT	Mapeo de la gestión de niveles de servicios de IT	Prepara a la organización para procesos de evaluación, certificación o acreditación.
Objetivos	Brindar buenas prácticas a través de un marco de trabajo de dominios y procesos, y presentar las actividades de una manera manejable y lógica.	Proporcionar a los administradores de sistemas de TI las mejores herramientas y documentos que les permitan mejorar la calidad de sus servicios.	Generar conciencia a los responsables de sistemas de información de la existencia de riesgos y la necesidad de solucionarlos.
Áreas	4 procesos y 34 Dominios	9 procesos	Se basa en la ISO/IEC 27002, 14 dominios, 35 objetivos de control y 114 controles
Creador	ISACA (Asociación de Auditoría y Control de	OGC (Oficina de comercio gubernamental)	Consejo Superior de Administración

	Sistemas de Información)		Electrónica del gobierno de España
¿Para qué se implementa?	Auditoría de sistemas de información	Gestión de niveles de servicio.	Planificación del proyecto análisis de riesgos, gestión de riesgos.
Software de apoyo	n.a.	n.a.	Herramienta PILAR

Las tres metodologías están orientadas a resguardar de una u otra maneras la seguridad de la información, pero Magerit proporciona un proceso sistemático para el análisis y gestión de riesgos, indicadores que se necesitan para la aplicación de este proyecto. De igual manera, se puede acotar que estas metodologías están orientadas a la elaboración de un SGSI[1].

2.5. Metodología Magerit

Magerit es la metodología de análisis y gestión de riesgos de los sistemas de información desarrollada por el Consejo Superior de Administración Electrónica del gobierno de España, para minimizar los riesgos de una organización. (Ministerio de Hacienda y Administraciones, 2016)

Es un método formal que sirve para investigar los riesgos a los que están expuestos los sistemas de información, para así poder recomendar las medidas apropiadas y proteger los activos que están en riesgo.

A continuación, se menciona las ventajas de esta metodología:

- Por sus años en el medio tiene madurez y es adaptable a cualquier tipo de organización.

[1] SGSI: Sistema de Gestión de la Seguridad de la Información.

- El análisis de riesgos puede ser del tipo cuantitativo o cualitativo.
- Cuenta con un inventario que permite identificar de una forma más fácil los recursos informáticos, activos y amenazas.
- Valora en base a la disponibilidad, confidencialidad, integridad, autenticación y trazabilidad, para un análisis integral del riesgo.

La aplicación de la metodología Magerit, pretende alcanzar los objetivos que se manifiestan a continuación (Ministerio de Hacienda y Administraciones, 2016):

- Concienciar al personal encargado del sistema informático que existen riesgos y la necesidad de reducirlos o mitigarlos a tiempo.
- Ofrecer un método sistemático, el que permita identificar los riesgos y medir de cierta manera la seguridad de la red.
- Proporcionar una metodología que ayude a descubrir los riesgos y la oportunidad de tenerlos bajo control.

Esta metodología se compone de tres libros que serán una guía para el análisis y gestión de riesgos, los cuales se detallan a continuación:

- **I Método.-** este libro detalla los pasos y las tareas para la estructura del proyecto de implementación de análisis y gestión de riesgo.
- **II Catálogo de elementos.-** en este libro se describe los paso para realizar un análisis del estado de riesgo y se propone un catálogo referente a: tipos de activos, dimensiones de valoración de los activos, criterios de valoración de los activos, amenazas típicas sobre los sistemas de información y salvaguardas a considerar para proteger sistemas de información.

- **III Guía de Técnicas.-** esta guía describe las tareas específicas que se pueden llevar acabo para la realización del proyecto de análisis y gestión de riesgos.

2.5.1. Metodología Análisis de Riesgo

El análisis de riesgos permite determinar qué tan seguro es su sistema e identificar los riesgos a los que está expuesto y poder gestionarlos.

Este proceso es una aproximación metódica para determinar el riesgo, y a continuación se describe los pasos que se deben llevar a cabo (Ministerio de Hacienda y Administraciones, 2016):

1. Determinar los activos relevantes para la Organización, su dependencia entre unos y otros
2. Determinar el valor que tiene según los objetivos de la organización.
3. Identificar a qué amenazas están expuestos los activos.
4. Determinar si existen salvaguardas y que tan eficientes son.
5. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
6. Estimar el riesgo, definido por la probabilidad de que una amenaza de materialice.

La Figura 1 muestra el proceso y los elementos que integran el análisis de riesgo, descrito anteriormente:

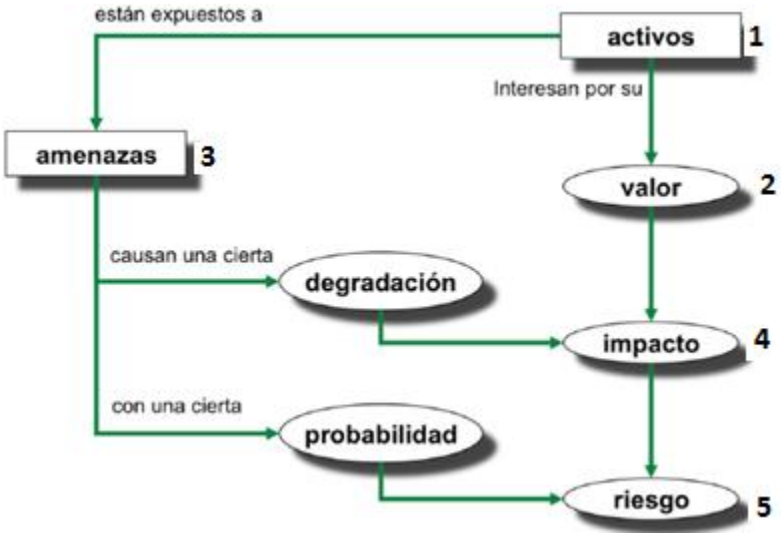


Figura 1 Metodología Magerit

Fuente: Ministerio de Hacienda y Administraciones, 2016

2.5.1.1.Activos Informáticos

El activo es un recurso del sistema de información, que es necesario, ya que éste forma parte de los procesos de funcionamiento de la organización.

"Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente, con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos" (CCN-STIC, 2016).

- **Dependencias**

Los activos dependen de otros activos como pueden ser los equipos, las comunicaciones, las instalaciones o el personal que trabajan con ellos. Las dependencias se establecen desde los activos superiores hasta llegar a los activos inferiores; pero las amenazas se materializan desde los activos inferiores hasta los superiores.

Por eso es tan importante identificar estas dependencias, ya que si un activo inferior está expuesto a alguna amenaza, puede verse perjudicado el activo superior.

- **Valoración**

Cada activo tiene su valor dentro de una organización, este depende de que tan importante y necesario sea el activo para la misma. Ya que, cuanto mayor es el valor del activo mayor es la necesidad de protegerlo.

El activo puede tener un valor propio o acumulado, generado por el valor de cada activo del que tiene dependencia.

Las valoraciones de los activos pueden ser cuantitativas o cualitativas. Las cuantitativas es determinar valores absolutos y cuestan mucho esfuerzo; y las cualitativas permiten posicionar el valor de cada activo en un orden relativo respecto de los demás. (Ministerio de Hacienda y Administraciones, 2016)

En este proyecto se valora los activos de forma cualitativa siguiendo las recomendaciones de la metodología Magerit. En la Tabla 2 se muestra una escala de valores, determinando el análisis que se puede dar a cada activo dependiendo de su importancia. Es recomendable utilizar una escala común para todas las dimensiones a evaluar, lo cual permite comparar riesgos.

Tabla 2

Criterios de valoración para los activos

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 menor
0	**Despreciable**	Irrelevante a efectos prácticos

Fuente: (Ministerio de Hacienda y Administraciones, 2016)

- **Dimensiones**

Un activo se dimensiona según los siguientes parámetros: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Por lo cual se debe responder básicamente a las siguientes preguntas, respectivamente, estas respuestas permiten asignar un valor en base a la Tabla 2.

- ¿Qué daño causaría que lo conociera quien no debe?
- ¿Qué perjuicio causaría que estuviera dañado o corrupto?
- ¿Qué perjuicio causaría no tenerlo o no poder utilizarlo?
- ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
- ¿Qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?
- ¿Qué daño causaría no saber quién accede, a qué datos y qué hace con ellos?

2.5.1.2.Amenazas

Las amenazas son consideradas como eventos que pueden causar un incidente en la organización, pudiendo causar daños materiales o perdidas inmateriales en sus activos. Las amenazas afectan directamente a las propiedades de la información: integridad, disponibilidad, confidencialidad y autenticidad.

Se considera amenaza a "cualquier causa potencial, ya sea intencional o fortuita, de un daño a un recurso de información y por ende a los activos de información que dicho recurso soporta" (Matalobos Veiga, 2012)

- **Identificación de amenazas**

Según (Ministerio de Hacienda y Administraciones, 2016) los tipos de amenazas que pueden afectar a los activos se listas a continuación:

De origen natural.- Procesos o fenómenos naturales como terremotos, inundaciones, incendios, etc; que pueden transformarse en un evento perjudicial y causar daños en el sistema de información.

Del entorno (de origen industrial).- Estos son desastres industriales (contaminación, fallos eléctricos,..) a los que están expuestos los sistemas de información.

Defectos de las aplicaciones.- Estas amenazas surgen por los problemas que puede dar el equipamiento del sistema de información, ya sea por errores en su implantación o diseño; frecuentemente se denominan vulnerabilidades técnicas.

Causadas por las personas de forma accidental.- Las personas que tiene acceso al sistema de información pueden de forma no intencionada, poner en riesgo la información ya sea por error o por omisión.

Causadas por las personas de forma deliberada.- Las personas que tienen acceso al sistema de información, pueden hacer uso de este privilegio para acceder a la información con intención de beneficiarse indebidamente, causar daño o perjuicio a la organización.

No todos los activos pueden verse afectados por todas las amenazas, sino que hay q establecer la relación entre las amenazas que pueden causar daño a un activo.

- **Valoración de las amenazas**

Si un activo esta frente a una amenaza, no quiere decir que este pueda ser afectado en todas sus dimensiones, ni en la misma cantidad. Cuando se ha logrado identificar la amenaza a la que está expuesto un activo, es necesario valorar su influencia en dos factores; primero es la degradación, en donde se analiza que tan perjudicado resultaría el activo en caso de que un incidente ocurriera y segundo es la probabilidad, donde se determina que tan probable o improbable es que se materialice dicha amenaza. Los criterios para la valoración de la degradación se muestra en la Tabla 3 y la probabilidad de ocurrencia se muestran en la

Tabla 4.

Tabla 3

Degradación del Valor

		DETALLE
MA	81% - 100%	Muy Alta
A	61% - 80%	Alta
M	41% - 60%	Media
B	21% - 40%	Baja
MB	0 - 20%	Muy Baja

Fuente: Ministerio de Hacienda y Administraciones, 2016

Tabla 4

Probabilidad de ocurrencia

		DETALLE
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)

Fuente: Ministerio de Hacienda y Administraciones, 2016

2.5.1.3.Determinación del impacto potencial

Impacto se considera al daño causado sobre un activo, como consecuencia de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y

el porcentaje de degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema de información. (Ministerio de Hacienda y Administraciones, 2016)

Las consecuencias indirectas que pueden causar el impacto son: pérdidas económicas, pérdidas de inversiones en el mercado o que los posibles clientes tengan una imagen negativa de la empresa.

Para calcular el valor del impacto se debe aplicar la Ecuación 1:

$$\text{Impacto} = \text{Valor del activo} * \text{Degradación del Valor} \qquad \textit{Ec.1}$$

2.5.1.4.Determinación del riesgo potencial

El riesgo es considerado como la posibilidad de que una amenaza se materialice sobre uno o más activos de una organización, aprovechando las vulnerabilidades, lo cual produzca un impacto, dando como resultado pérdidas. El riesgo crece con el impacto y con la probabilidad de ocurrencia. (Ministerio de Hacienda y Administraciones, 2016)

Valoración de Riesgos

Para valorar los riesgos, como primer punto es identificar los activos, segundo identificar cada amenaza sobre cada activo y por último es necesario estimar la vulnerabilidad, que es la probabilidad de que una amenaza se materialice.

La metodología Magerit divide al riesgo en cuatro zonas:

- **Bajo:** el nivel de riesgo es bajo, y por lo tanto no es necesario emplear salvaguardas adicionales.
- **Medio**: el nivel de riesgo es medio y se deberá poner en consideración si se deben implementar salvaguardas para evitarlos.
- **Alto**: El nivel de riesgos es alto y en esta etapa es obligatorio implementar salvaguardas necesarias para mitigar riesgos.
- **Crítico**: el nivel de riesgo crítico es un estado preocupante, y es necesario implementar salvaguardas de manera inmediata para minimizarlos.

Para determinar el riesgo se utiliza la Ecuación 2:

$$\text{Riesgo} = \text{Probabilidad de Amenaza} * \text{Magnitud del Daño (Impacto)} \qquad \textit{Ec. 2}$$

Tanto la probabilidad como la magnitud pueden tomar los siguientes valores representativos para estimar el valor del riesgo, que se muestra la Tabla 5.

Tabla 5

Valores representativos para estimar el riesgo

Valor representativo	**Probabilidad de la Amenaza**	**Magnitud del Daño**
5 - Catastrófico	100	10
4 - Crítico	10	8-9
3 - Alto	1	6-7
2 - Medio	1/10	4-5
1 - Bajo	1/100	0-3

Los valores que se muestran en la Tabla 5 respecto a las variantes de probabilidad de la amenaza y magnitud del daño, son los definitivos en la metodología Magerit, pero para mayor facilidad y comprensión del cálculo del riesgo, se recomienda usar los valores determinados en la primera columna de la tabla mencionada.

Al momento de calcular el riesgo es imperativo generar una matriz de riesgos como se muestra en la Tabla 6, donde se puede entender según el color, la zona de riesgo que representa, según la metodología Magerit.

Tabla 6

Matriz de riesgo

PROBABILIDAD		IMPACTO				
		1	2	3	4	5
Muy Frecuente (a diario)	5	Alto	Alto	Crítico	Crítico	Crítico
Frecuente (mensualmente)	4	Medio	Alto	Alto	Crítico	Crítico
Normal (una vez al año)	3	Bajo	Medio	Alto	Crítico	Crítico
Poco frecuente (cada varios años)	2	Bajo	Bajo	Medio	Alto	Crítico
Muy poco frecuente (siglos)	1	Bajo	Bajo	Medio	Alto	Alto

Riesgo Residual

Es aquel riesgo que subsiste, después de haber implementado controles o salvaguardas. Para determinar este riesgo se toma en consideración el valor del activo, la exposición de los recursos de información a la amenaza y la eficiencia de la salvaguarda planificada o implementada para reducir la frecuencia o el impacto de la amenaza.

2.5.1.5.Salvaguardas

Las salvaguardas son medidas o procedimientos tecnológicos que ayudan a reducir el riesgo de un sistema. Hay amenazas que se pueden manejar o controlar simplemente con una organización adecuada, otras requieren elementos técnicos (programas o equipos), otras seguridades físicas y por último, está la política de personal. (Ministerio de Hacienda y Administraciones, 2016)

Para seleccionar una salvaguarda apropiada es necesario tener en cuenta los siguientes aspectos: tipos de activos a proteger, dimensiones de seguridad que requieren protección, amenazas de las que se debe proteger y saber si existen salvaguardas alternativas.

Con las elección de las salvaguardas apropiadas se pretende reducir la probabilidad de que una amenaza se materialice o a su vez limitar el daño que cause una amenaza en caso de llegar a materializarse.

2.5.1.6.Vulnerabilidades

Se denomina vulnerabilidad a la debilidad (agujero, falla o error en la seguridad del sistema de información) de un sistema, que la amenaza puede aprovechar para materializarse. Magerit mide la vulnerabilidad por la frecuencia cuantitativa de la materialización de la amenaza sobre el activo.

Existen diferentes vulnerabilidades a la que puede estar expuesto un sistema, a continuación se menciona las principales según (Ministerio de Hacienda y Administraciones, 2016):

- Vulnerabilidades físicas como por ejemplo: incendios, terremotos, inundaciones etc.
- Las deficiencias en el diseño de los sistemas.
- Debilidades en los protocolos utilizados por el sistema.
- Las debilidades en los códigos ejecutados por el sistema.
- Software malicioso como son los virus.
- Vulnerabilidades humanas con o sin mala intención.

2.5.2. Proceso de Gestión de Riesgos

Después de haber obtenido los resultados del análisis de riesgos, se habrá obtenido información que permita tomar decisiones sobre los activos que se quiere proteger, teniendo conocimiento de las amenazas y el riesgo al que se está enfrentando.

En la Figura 2 se muestra las posibles decisiones que se pueden tomar tras haber estudiado los riesgos, pudiendo tomar la alternativa que más convenga a la organización. El riesgo puede ser aceptado y monitoreado periódicamente, estudiado o tratado.

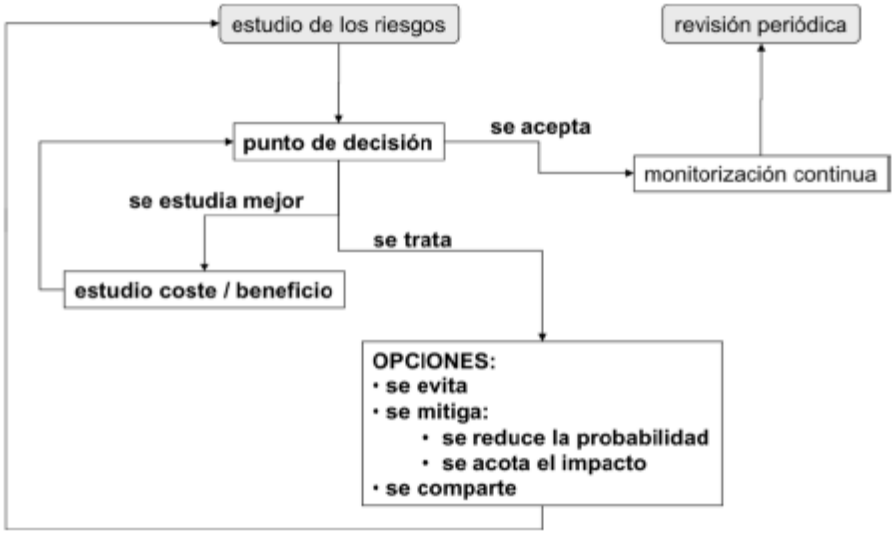


Figura 2 Proceso de gestión de riesgos

Fuente: Ministerio de Hacienda y Administraciones, 2016

2.5.2.1.Determinar los criterios de aceptación del riesgo

Este proceso depende de la organización, esta determina el nivel de impacto y riesgo aceptable, es decir, debe aceptar las responsabilidades de las insuficiencias. Esta decisión puede ser política o gerencial, no necesariamente técnica. Estos niveles de aceptación se pueden establecer por activo o por agregación de activos (en un determinado departamento, en un determinado servicio, en una determinada dimensión). Cualquier nivel de impacto y/o riesgo es aceptable si lo conoce y acepta formalmente la organización. (Ministerio de Hacienda y Administraciones, 2016)

2.5.2.2.Tratamiento

El tratamiento que se dé, a uno u otro riesgo dependerá de la organización, ya que bajo los criterios de los administradores de la red, se podrá identificar que riesgos deberán ser tratados, dependiendo de las consideraciones u objetivos que tenga la organización. Hay diferentes formas de tratar al riesgo y se mencionan a continuación (Ministerio de Hacienda y Administraciones, 2016):

Eliminación

El proceso de eliminación implica prescindir de ciertos elementos de la red, pero que esto no altere los objetivos de la organización. Existen dos opciones de como ejecutar este proceso:

- Eliminar cierto activo y emplear otro en su lugar.
- Reordenar la arquitectura del sistema, para de esta forma cambiar el valor acumulado en ciertos activos.

Mitigación

La mitigación del riesgo se refiere a una de dos opciones:

- Reducir la degradación causada por una amenaza.
- Reducir la probabilidad de que una amenaza se materialice.

En las dos opciones la solución es mejorar el conjunto de salvaguardas. En algunas ocasiones subir el nivel de las salvaguardas implica el despliegue de más equipos, lo que esto se convierte en un nuevo activo, y se deberá realizar una nuevo análisis de riesgo para cerciorarse que el riesgos sea menor que del sistema original.

Compartición

Este proceso consiste en transferir el riesgo de forma total o parcial. En ocasiones la empresa no tiene la capacidad de tratamiento y precisa la contratación de un tercero con capacidad para reducir y gestionar el riesgo.

Financiación

En este proceso se requiere que la organización debe estar preparada financieramente para cuando haya que responder por las consecuencias de una amenaza materializada.

2.5.3. Plan de Seguridad

El plan de seguridad contiene una serie de proyectos donde se materializa las decisiones adoptadas para el tratamiento de los riesgos. Para el desarrollo de este plan es necesario tener en claro que es un SGSI (Sistema de Gestión de Seguridad de la Información), siendo este un conjunto de políticas de administración de la información que permite reducir las amenazas hasta que estas sean asumibles por la institución, de tal manera que si llegara a ocurrir un incidente el daño sea mínimo y así la continuidad de las actividades de la institución estarían aseguradas.

En el SGSI se contempla el diseño, implementación y mantenimiento de un conjunto de procesos que permiten la gestión eficiente de la accesibilidad de la información, logrando asegurar en cierto grado la confidencialidad, integridad y disponibilidad de los activos de información y así mismo, minimizando los riesgos de la seguridad de la información. (ISO 27000, 2005)

A continuación se enuncian algunos beneficios de un SGSI:

- Establecer una metodología de gestión de seguridad clara y estructurada.
- Reducir el riesgo de pérdida, robo o corrupción de la información.
- Acceder a la información por parte de los usuarios a través de medidas de seguridad.
- Asegurar que los riesgos y controles sean continuamente revisados.

La familia de normas ISO/IEC 27000 adopta un modelo conforme se observa en la Figura 3 de mejora continua para la implantación de un SGSI, denominado PDCA (Plan-Do-Check-Act) y en español PHVA (Planificar, Hacer, Verificar y Actuar).

- **Planificar:** establecer las actividades que se llevarán a cabo para el cumplimiento de los objetivos propuestos.

- **Hacer:** en este proceso se plasma las actividades que propongan la mejora, en base al proceso anterior.
- **Verificar:** mediante el uso de herramientas, monitorizar y evaluar la efectividad del cumplimiento del plan de seguridad.
- **Actuar:** mantener el proceso que se realiza mediante el plan de seguridad y mejorar constantemente a medida de lo posible.

Figura 3 Modelo PDCA

Fuente: NTE INEN-ISO 27001, 2011

Alcance y limites

El plan de seguridad de la información se enfoca en reducir los riesgos encontrados dentro de la institución, enfocado en proteger los activos críticos; sin embargo la implementación no se encuentra dentro del alcance de este proyecto de titulación.

2.5.4. Plan de Acción

Un Plan de Acción es una presentación resumida de las tareas que se debe realizar por ciertas personas, en un tiempo determinado. El propósito del Plan de Acción es proponer un

documento que sirva como guía, a la hora de llevar a cabo un proyecto. El plan establece quiénes serán los responsables que se encargarán de su cumplimiento en tiempo y forma.

En concreto podemos determinar que todo plan de acción debe conformarse por los siguientes apartados: los objetivos que se desea alcanzar, acciones estratégicas a seguir, tiempos establecidos y también quién se encargará de ejercer como responsable.

2.6. Herramienta PILAR

La herramienta PILAR (Procedimiento Informático Lógico para el Análisis de Riesgos) soporta el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit. Y permite realizar calificaciones de seguridad respecto a la norma ISO 27002.

Con esta herramienta se analizan los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Además para tratar el riesgo se propone: salvaguardas (o contramedidas), normas de seguridad, procedimientos de seguridad y analiza el riesgo residual a lo largo de diversas etapas de tratamiento.

Esta herramienta soporta las fases del método Magerit:

- Caracterización de los activos: identificación, clasificación, dependencias y valoración.
- Caracterización de las amenazas.
- Evaluación de las salvaguardas.
- Evaluación del impacto y el riesgo.

PILAR presenta los resultados en varias formas, ya sea en informes RTF, gráficas o tablas que se pueden agregar a una hoja de cálculo, logrando elaborar diferentes tipos de informes y presentaciones de los resultados.

2.6.1. Diagrama de utilización de herramienta PILAR

PILAR es una herramienta creada específicamente bajo los lineamientos de la metodología Magerit, en la Figura 4 se muestra el funcionamiento de la herramienta PILAR, en donde se determina cada proceso por el que pasa un activo, el cual también es recomendado por la metodología Magerit y se describe a continuación:

- Identificar el activo, este activo debe ser clasificado dentro del grupo correspondiente.
- Establecer las dependencias entre activos.
- Valorar los activos es decir seleccionar el nivel según el criterio de que tan grave sea que una amenaza se materialice.
- Identificación de amenazas, asigna amenazas automáticamente de la biblioteca del programa según las características de cada activo.
- Valoración de amenaza por cada activo, el programa calcula la probabilidad de que una amenaza se materialice.
- Impacto y riesgo, el programa genera automáticamente estos parámetros.
- Tratamiento del riesgo, el programa recomienda un listado de salvaguardas.
- Impacto y riesgo residual, el programa genera automáticamente.

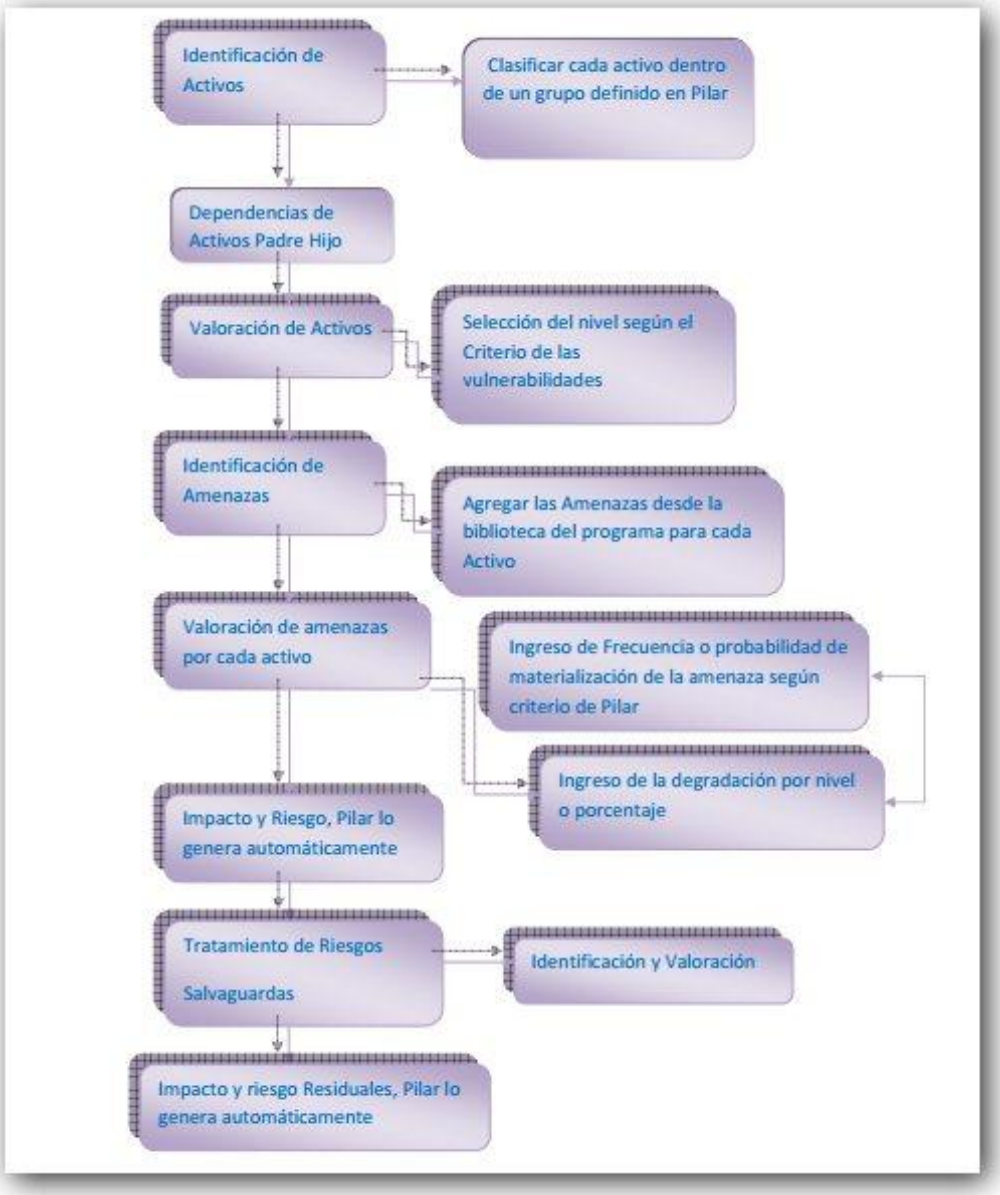


Figura 4 Diagrama de utilización de la herramienta PILAR
Fuente: Martinez Garcis, 2012

2.7. ISO/IEC 27002

Como parte de la elaboración del Plan de Seguridad se propone establecer políticas que se basan en los objetivos de control y controles de la norma ISO/IEC 27002; la versión 2005 es la que se aplica en este proyecto.

ISO/IEC 27002 es una norma para la seguridad de la información que ha publicado la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional.

Esta norma establece los controles para abordar las mejores prácticas en la gestión de la seguridad de la información, pero hay que tener en cuenta que no todos los controles pueden ser aplicables a todos los sistemas de gestión, debido a que los requerimientos de seguridad son únicos y diferentes en cada organización.

La norma ISO/IEC 27002 se encuentra enfocada a todo tipo de empresas, independientemente del tamaño, tipo o naturaleza y se encuentra organizado en base a 14 dominios, 35 objetivos de control y 114 controles. Ver Anexo 1**.**

Capítulo 3

Situación actual

En este capítulo se describe la situación actual, detallando los equipos y servicios integrados en el Data Center, con sus características y responsables. Esta información permite conocer el funcionamiento del Data Center, las políticas existentes y hasta qué punto se da cumplimiento a las mismas.

3.1. Análisis estado actual Data Center

En la Facultad de Ingeniería en Ciencias Aplicadas (FICA) se encuentra ubicado un Data Center totalmente implementado, el mismo que fue concebido con la idea de alojar equipos de telecomunicaciones de la facultad, en condiciones ambientales estables y ciertos niveles de seguridad; con la finalidad de crear un laboratorio de investigación tanto para estudiantes como docentes de las carreras ofertadas.

El Data Center está ubicado en la planta baja de la Facultad de Ingeniería en Ciencias Aplicadas, dentro de la oficina de la Carrera de Ingeniería en Telecomunicaciones (CITEL). En la Figura 5 se muestra el diagrama de infraestructura del Data Center. Donde sus dimensiones físicas son 2,85 m de longitud por 3 m de ancho, por lo tanto un área total de 8,55 m2 (Narváez, 2016).

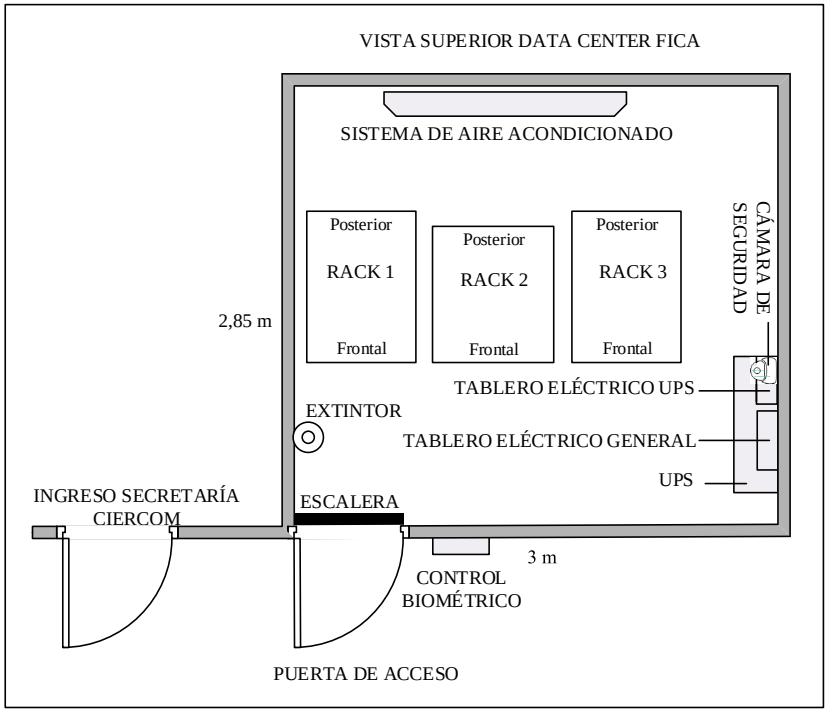


Figura 5 Infraestructura Data Center FICA

Fuente: Data Center FICA

El Data Center se compone de los sistemas elementales que se describen a continuación: Sistema Eléctrico, Sistema de Control de Acceso, Sistema de Aire Acondicionado, Sistema de Seguridad y Sistema de Telecomunicaciones.

- **Sistema Eléctrico**

Este sistema se encarga del suministro eléctrico de todo el Data Center, la acometida eléctrica es independiente tomada del trasformador eléctrico ubicado frente al Gimnasio de la Universidad, la cual llega por debajo de la tierra a la caja de revisión de concreto ubicada en la parte externa de la facultad FICA, posterior a esto, tiene una conexión al tablero eléctrico general en la parte interna del Data Center. El tablero eléctrico que se puede ver en la Figura 6, es la parte principal de la instalación eléctrica, aquí llega la conexión de la acometida comercial y en el mismo se encuentra conectado el sistema UPS, el sistema de control de acceso y aire acondicionado. (Narváez, C., 2016)

Figura 6 Sistema Eléctrico

El sistema UPS identificado en la Figura 7, funciona en caso de que exista un fallo en el sistema eléctrico comercial, alimentando todo el equipamiento TIC y puerta de seguridad. Al igual protege a los circuitos eléctricos de cambios bruscos y violentos.

Figura 7 Sistema UPS

- **Sistema de Control de Acceso**

El acceso al Data Center es restringido, por ende se implementó un sistema de control de acceso que se maneja a través de un mecanismo biométrico como se puede ver en la Figura 8.

Además, consta de una puerta de seguridad metálica, resistente a rayones y golpes, con un diseño hermético para evitar las fugas de aire refrigerado, barra anti-pánico y cerradura electromagnética.

Figura 8 Sistema de control de acceso

- **Sistema de Aire Acondicionado**

Cuenta con un sistema de aire acondicionado como se puede ver Figura 9, considerado como sistema de refrigeración tipo “Split” o conocido como “conford”, debido a que el Data Center es de dimensiones relativamente pequeñas y cuenta con una cantidad de equipos moderado, este sistema es suficiente para mantener este espacio en condiciones ambientales aceptables. (Camues, 2017)

Figura 9 Sistema de aire acondicionado

- **Sistema de Seguridad**

Se cuenta con una cámara de vigilancia como se puede ver en la Figura 10, la cual está ubicada en el interior del Data Center enfocando a la puerta de ingreso. El acceso a ella es vía web en modo monitoreo y no de almacenamiento.

Figura 10 Sistema de Seguridad

- **Sistema de Telecomunicaciones**

El Data Center FICA aloja equipamiento de red, que funciona como red redundante del anillo de fibra de la Universidad Técnica del Norte. Estos equipos y cables están ubicados en el Rack 1. En el Data Center FICA se alojan equipos de red los cuales están ubicados como se muestra en la Figura 11. Siendo la distribución de equipos de la siguiente manera. En el Rack 1 se encuentra un switch capa tres que sirve como equipo de borde y conexión del Data Center con el edificio central y el internet por medio de dos cables de fibra óptica; Rack 2 en donde se ubican los servidores que forman la infraestructura virtual Proxmox (PV1, PV2, PV3 y PV4) para virtualización de equipos, el servidor Radius, tres servidores pertenecientes a CISIC[2] y un switch 3com; Rack 3 aloja un switch 3com y un router Mikrotik que se encarga de la red inalámbrica con tecnología propia, además un switch QPcom y 4 servidores para fines administrativos y educativos que brindan servicio tanto a docentes como estudiantes, siendo estos: Opina, Reactivos, Biométrico y Revista Universitaria.

[2] CISIC: Carrera de Ingeniería en Sistemas Computacionales.

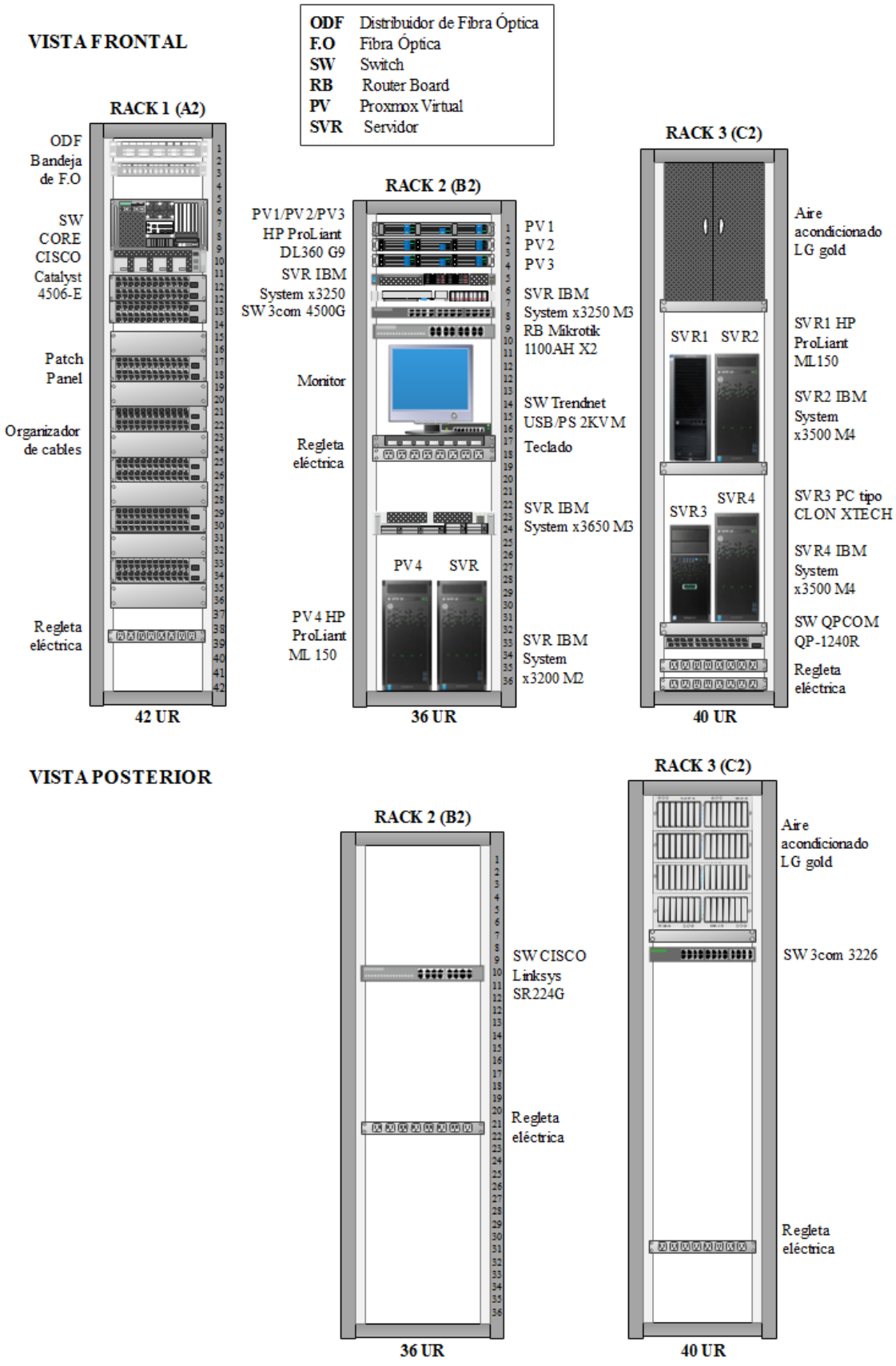


Figura 11 Ubicación Física equipos Data Center
Fuente: Data Center FICA

Topología Física

La topología física de la red del Data Center se puede observar en la Figura 12, en donde el acceso a internet y servicios es proporcionado por el enlace de fibra óptica desde el DDTI[3] hasta el switch de core Catalyst.

La red interna FICA está dividida en tres segmentos físico de red.

El primer segmento distribuido desde el puerto 23 del switch de core Catalyst este interconecta al switch 3Com, el cual provee conexión a cuatro servidores denominados Opina, Reactivos, Biométrico, Reactivos y Revista Universitaria.

El segundo segmento distribuido desde el puerto 27 del switch de core Catalyst este interconecta al switch LinkSys, el cual provee conectividad a los tres servidores que administra la carrera de sistemas de la facultad.

Y el tercer segmento de la red, provee conectividad a la red inalámbrica de la FICA y también a la estructura virtual Proxmox. Desde el puerto 30 de switch de core Catalyst se proporciona un enlace hacia el router Mikrotik, el que se encarga del enrutar el tráfico; luego interconecta al swicth QPcom a través de switch 3Com, desde el cual se provee conectividad a todos los access point ubicados en la FICA. Por otro lado la infraestructura virtual Proxmox se conecta a través del switch 3Com, esta infraestructura está formada por cuatro servidores que se denominan PV1, PV2, PV3 y PV4; de igual forma en este segmento de red se encuentra conectado el Servidor Radius.

[3] DDTI: Dirección de Desarrollo Tecnológico e Informático

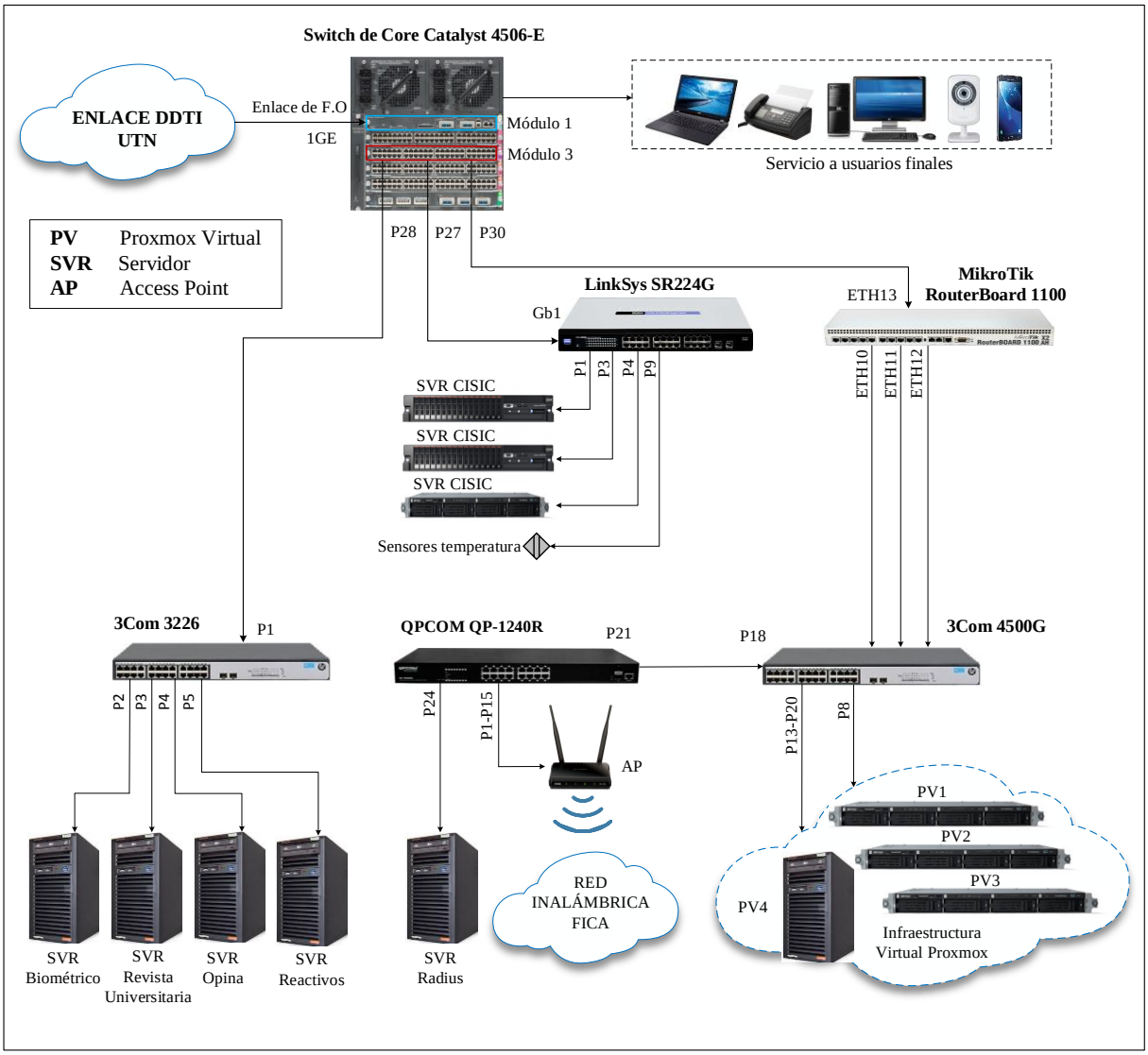


Figura 12 Topología física equipos Data Center

Fuente: Data Center FICA

Descripción equipos de la red

El Data Center FICA aloja doce servidores y seis equipos de red, los cuales se describen a continuación en la Tabla 7, información que fue recolectada mediante fichas técnicas evidenciadas en el Anexo 5.

Tabla 7

Equipos de red alojados en el Data Center FICA

EQUIPO	MARCA/MODELO	FUNCIÓN	No. SERIE	CARACTERÍSTICAS
SERVIDORES	IBM System x3500 M4	Revista Universitaria	7383AC1-KQ6M81T	RAM: 7,6 GB Procesador: Intel Xeon ® CPU: E5-2630 2,30 GHz x 12 HDisk: 610 GB OS: CentOS 6.5
	IBM System x3500 M4	Reactivos	7383AC1-KQ6M81V	RAM: 7,6 GB Procesador: Intel Xeon ® CPU E5-2630 2,30 GHz x 12 HDisk: 135 GB OS: CentOS 6.5
	PC tipo “Clon” X Tech	Administración Biométricos FICA	H81M-S1	RAM: 4 GB Procesador: Core (TM) i3-4150 CPU: 3.5 GHz HDisk: 610 GB OS: Windows 7 Profesional
	HP ProLiant ML150	Servicio de encuestas y evaluación OPINA	QAAUD014H39NC2	RAM: 4.8 GB Procesador: Intel Xeon ® CPU: E54405 GHz x 4 HDisk:150 GB OS: Ubuntu 12.10
	HP ProLiant DL360 Gen9	Proxmox (PV1)	MXQ51704F7	RAM: 32 GB Procesador: Intel Xeon ® CPU: E5-2620 V3

				HDisk: 450 GB OS: Ubuntu Server 14.043 LTS
	HP ProLiant DL360 Gen9	Proxmox (PV2)	MXQ51500L9	RAM: 32 GB Procesador: Intel Xeon ® CPU: E5-2620 V3 HDisk: 450 GB OS: Ubuntu Server 14.043 LTS
	HP ProLiant DL360 Gen9	Proxmox (PV3)	MXQ51704F9	RAM: 32 GB Procesador: Intel Xeon ® CPU: E5-2620 V3 HDisk: 450 GB OS: Ubuntu Server 14.043 LTS
SERVIDORES	HP ProLiant ML150	Proxmox (PV4)	QAAUD014H39 NMO	RAM: 1 GB Procesador: Intel Xeon® CPU: E5405 2.0GH x 4 HDisk: 160 GB OS: Ubuntu Server 14.043 LTS
	IBM System x3200 M2	Radius	4368E1U-KQGVGWB	RAM: 2GB Procesador: Dual-core Xeon CPU: E3110 3.0 HDisk: 1TB OS: CentOS 6.5
	IBM System x3250 M3	CISIC (GeoPortal)	KQ51C82	RAM: 7,6 GB Procesador: Intel Xeon ® CPU E5-2630 2,30 GHz x 12 HDisk: 135 GB OS: CentOS 6.5

	IBM System x3250	CISIC (Servidor Pruebas)	KQCMXW0	RAM: 4.8 GB Procesador: Intel Xeon ® CPU: E54405 GHz x 4 HDisk:150 GB OS: Ubuntu 12.10
	IBM System x3650M3	Servidor CISIC	KQ14RFK	RAM: 7,6 GB Procesador: Intel Xeon ® CPU E5-2630 2,30 GHz x 12 HDisk: 135 GB OS: CentOS 6.5
	CISCO Catalyst 4506-E	Enlace Principal Distribución de Red de la Facultad	FOX115167P1	Puertos: 48 x3 Características de Capa 3 administrable
SWITCHES Y ROUTER	CISCO Linksys SR224G	Distribución de red	REP20FB00241	Puertos: 24
	3COM 4500G	Distribución de red	YEYFC4PE1D200	Puertos: 24
	RB Mikrotik 1100AH X2	Router de red inalámbrica	574005AFCF00/627	Puertos: 24
	3COM 3226	Distribución de red	0104/73MF4XD03C0A0	Puertos: 24
	QPCOM QP-1240R	Distribución de conexiones AP-red inalámbrica FICA	121005919	24 puertos Fast Ethernet 10/100/1000 Mbps

Fuente: Data Center FICA

Topología Lógica

La topología lógica de la red interna del Data Center está representada en la Figura 13. La red está constituida por un router MikroTik y dos switches administrables (switch core Catalyst y switch 3Com 4500G), el swtich de core Catalyst es administrado externamente, pero para la red representa un equipo de frontera y el que provee acceso a internet a la red interna, el switch 3com 4500G y el router MikroTik son administrados internamente y a partir de los cuales se estructura la red. Además, existen tres switches que son: Lynksys, el 3com 3226 y QPcom que son dispositivos de capa 2, y son los encargados de brindar la conexión a los demás equipos de red como: servidores y access point, respectivamente.

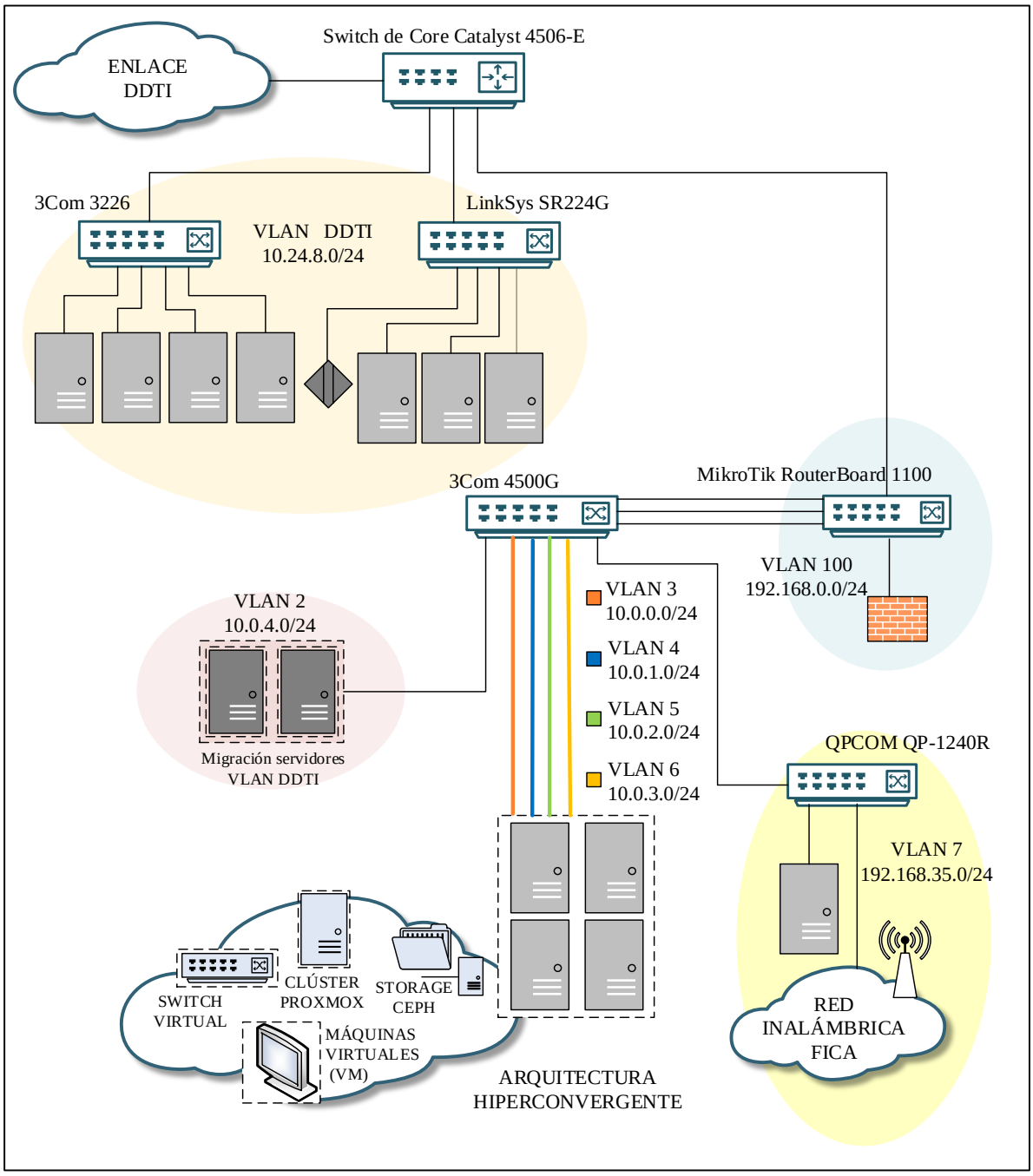


Figura 13 Topología Lógica del Data Center
Fuente: Data Center FICA

En el switch administrable 3com 4500G, tienen configurado siete VLAN´s para organizar de mejor manera la red, siendo asignadas de la siguiente manera: VLAN 2: ENLACE_RED_ANTIGUA, VLAN 3: VLAN_SERV_PROXMOX, VLAN 4: VLAN_ILO_SERV_PROXMOX, VLAN 5: VLAN_SERV_VIRTUAL VLAN 6 STORAGE_CEHP, VLAN 7: VLAN_WIFI_ADMIN y VLAN 100: TO_MIKROTIK.

En la Tabla 8 se muestran la asignación de las direcciones IP´s utilizadas en la red interna constituida en el Data Center de la FICA.

Tabla 8

Direccionamiento IP red Data Center

	VLAN	EQUIPO	SUBRED	IP	GATEWAY	MÁSCARA
3com 226 Linksy	VLAN DDTI	OPINA	10.24.8.0	10.24.8.X	10.24.8.254	255.255.255.0
		Revista Universitaria		10.24.8.X		
		Reactivos		10.24.8.X		
		Biométrico		10.24.8.X		
		CISIC 1		10.24.8.X		
		CISIC 2		10.24.8.X		
		CISIC 3		10.24.8.X		
		Sensores		10.24.8.X		
3COM 4500G	**2**	Migración Servidores VLAN DDTI	10.0.4.0	10.0.4.X	10.0.4.254	255.255.255.0
	3	PV1	10.0.0.0	10.0.0.1	10.0.0.254	255.255.255.0
		PV2		10.0.0.2		
		PV3		10.0.0.3		
		PV4		10.0.0.4		
	4	iLO PV1	10.0.1.0	10.0.1.1	10.0.1.254	255.255.255.0
		iLO PV2		10.0.1.2		
		iLO PV3		10.0.1.3		
	5	VM (Máq. Virtuales)	10.0.2.0	10.0.2.X	10.0.2.254	255.255.255.0
	6	CEHP PV1	10.0.3.0	10.0.3.1	10.0.3.254	255.255.255.0
		CEHP PV2		10.0.3.2		
		CEHP PV3		10.0.3.3		
		CEHP PV4		10.0.3.4		
	7	QPcom	192.168.35.0	192.168.35.X	192.168.35.1	255.255.255.0
		Radius		192.168.35.X		
		APs		192.168.35.X		
	100	MikroTik	192.168.0.0	192.168.0.X	192.168.0.254	255.255.255.0

Fuente: Data Center FICA

Servidores

El Data Center FICA tiene implementado servidores de aplicación, los cuales brinda servicios a los usuarios con acceso a la red inalámbrica y usuarios autorizados. Los servidores existentes se describen a continuación:

- **Servidor Proxmox**

  Proxmox es una plataforma de virtualización open source, conformado por cuatro servidores; permite el despliegue y la gestión de máquinas virtuales. Es un servidor que permite la migración de servidores físicos sin tiempo de inactividad, copias de seguridad de programas y brinda servicio de alta disponibilidad a la red.

- **Servidor Radius**

  Radius (Remote Authentication Dial-In User Service) es el servidor que se encarga de verificar la autenticidad de un usuario, para darle acceso a la red. Utiliza un protocolo cliente-servidor, donde el usuario mediante credenciales otorgadas se conecta al servidor.

- **Servidor Opina**

  El servidor OPINA permite modelar encuestas desde cualquier punto con acceso a Internet. Los destinatarios del servicio de creación de encuestas OPINA son el personal docente y estudiantes de la facultad FICA.

- **Servidor de Reactivos**

  Este servidor es un gestor de contenidos, orientado al entorno educativo, con la finalidad de descargar/visualizar temarios propuestos por el administrador y poder realizar diversas actividades interactivas.

- **Servidor Revista Universitaria**

  Este servidor trabaja bajo la plataforma OJS (Open Journal Systems) siendo este un Sistema de Administración y publicación de revistas y documentos periódicos (Seriadas)

en Internet. Este sistema permite un manejo eficiente y unificado del proceso editorial, con esto se busca acelerar el acceso en la difusión de contenidos e investigación producido por la Universidad.

- **Servidor de Control de Acceso Biométrico**

El servidor biométrico maneja una base de datos que almacena información personal de los docentes, entre ella la huella dactilar como elemento de identificación y de registro de horarios de ingreso y salida, así mismo valida la autenticación para ingreso a laboratorios, aulas y oficinas.

3.2. Distribución de responsables de los equipos del Data Center

En la investigación realizada se puede destacar que el Data Center cuenta con una estructura organizacional descentralizada, por lo cual existe una persona a cargo denominada administrador de red, y cada servidor es administrada por un responsable o encargado, previamente asignado.

Los equipos se encuentran asignados de manera independiente por cada docente a cargo del proyecto como se muestra en la Tabla 9.

Tabla 9

Responsables de los equipos del Data Center

EQUIPO	MARCA/MODELO	UBICACIÓN	FUNCIÓN/USO	RESPONSABLE/USUARIO
SERVIDORES	IBM System x3500 M4	Rack 3	Revista Universitaria	MSc. Daisy Imbaquingo
	IBM System x3500 M4	Rack 3	Reactivos	Ing Santiago Meneses
	PC xtech tipo Clon	Rack 3	Administración biométricos FICA	MSc. Ludmila Starodub
	HP Proliant ML150 G5	Rack 3	Servicio de encuestas y evaluación OPINA	MSc. Fabián Cuzme

	HP Proliant DL360 G9	Rack 2	Proxmox (PV1)	MSc. Hernán Domínguez
	HP Proliant DL360 Gen9	Rack 2	Proxmox (PV2)	MSc. Hernán Domínguez
	HP Proliant DL360 Gen9	Rack 2	Proxmox (PV3)	MSc. Hernán Domínguez
	HP Proliant ML150	Rack 2	Proxmox (PV4)	MSc. Hernán Domínguez
	IBM System x3200 M2	Rack 2	Radius	MSc. Hernán Domínguez
	IBM System x3250 M3	Rack 2	Servidor GeoPortal CISIC	MSc. Pablo Landeta
	IBM System x3250	Rack 2	Servidor Pruebas CISIC	MSc. Pablo Landeta
	IBM System x3650 M3	Rack 2	Servidor CISIC	MSc. Mauricio Rea
EQUIPOS DE RED: SWITCHES Y ROUTER	Switch CISCO Catalyst 4506-E	Rack 1	Enlace Principal Distribución de Red de la Facultad	Ing. Santiago Meneses
	Switch CISCO Linksys SR224G	Rack 2	Distribución de red	MSc. Edgar Jaramillo
	Switch 3COM 4500G	Rack 2	Distribución de red	MSc. Edgar Jaramillo
	Router Board Mikrotik 1100	Rack 2	Router de red	MSc. Edgar Jaramillo
	Switch 3COM 3226	Rack 3	Distribución de red	MSc. Edgar Jaramillo
	Switch QPCOM QP-1240R	Rack 3	Distribución de conexiones AP – red inalámbrica FICA	MSc. Edgar Jaramillo
COORDINADOR DE ACTIVIDADES ADMINISTRACIÓN Y GESTIÓN DE RED				MSc. Hernán Domínguez

Fuente: Data Center FICA

3.3. Normativa de Seguridad

En un trabajo de investigación previo se realizó un Modelo de seguridad de la información estableciendo políticas de seguridad para el Data Center de la FICA (Perugachi, 2018), las cuales serán tomadas como punto de partida para la elaboración del presente proyecto. Dichas políticas no han sido socializadas, aplicadas ni actualizadas impidiendo su utilización; además que estas fueron elaboradas para una infraestructura que actualmente ha cambiado.

3.4. Salvaguardas Existentes

Mediante una inspección física realizada al Data Center, se puede determinar la existencia de las siguientes salvaguardas:

- Para el acceso físico al Data Center, se cuenta con un mecanismo de control de acceso biométrico, impidiendo el ingreso a personal no autorizado.
- Existe un sistema de alimentación ininterrumpida, que funciona en caso de fallos o desconexión del sistema eléctrico principal, el cual se encarga de mantener operativos los activos que integran el Data Center.
- Cuenta con un sistema de control de temperatura, el cual da una alerta en caso de llegar a grados de temperatura no adecuados, al igual que un sistema de alerta en caso de fallos eléctricos.
- En la parte lógica de la red del Data Center, se encuentra implementado un servidor Radius, el cual proporciona las credenciales para el respectivo acceso a la red.

3.5. Identificación de vulnerabilidades

Con el fin de recolectar información con respecto a la seguridad que se maneja e identificar las falencias o vulnerabilidades que se presentan en el Data Center, se realizó una entrevista con preguntas cerradas al técnico encargado, la cual se puede verificar en el Anexo 2. Cabe indicar que dicha entrevista se basó en los indicadores más representativos de la norma ISO/IEC 27002. Llegando al siguiente análisis:

- Existen políticas de seguridad como se menciona en el apartado 3.3 de este documento, pero no fueron debidamente socializadas, por ende, los usuarios del Data Center desconocen de su existencia y por tal razón no fueron aplicadas.
- No existen roles que determinen la funciones del personal dentro del Data Center, habido inexistencia de personal encargado exclusivo de la seguridad de la información.
- No hay un correcto etiquetado de los activos (activos esenciales, hardware, software y equipos auxiliares), a consecuencia no existe un inventario debidamente documentado.
- No existe procedimientos para la manipulación de los activos y su respectivo mantenimiento.
- No se documenta los cambios y procedimientos realizados dentro del Data Center.
- No existen procedimientos para el ingreso al Data Center FICA.
- No existe herramientas que alerten en caso de incidentes en la seguridad de la información, ni el personal correspondiente para atender estas alertas.
- No existe plan de continuidad del Data Center, el cual permita recuperar y restaurar las funciones críticas parcial o totalmente interrumpidas.

Luego de haber identificado estas vulnerabilidades, es necesario realizar un análisis del riesgo donde se determine el nivel del riesgo al que está expuesto el sistema de información que se aloja en el Data Center, para seguidamente realizar el tratamiento del respectivo riesgo al que se está enfrentando.

Capítulo 4

Análisis y Gestión de Riesgos mediante la Metodología Magerit v3.0

En este capítulo se documenta el análisis y gestión de riesgos bajo el concepto de la metodología Magerit 3.0, la misma que sugiere el uso de la herramienta informática PILAR. Se establece los activos más significativos que posee el Data Center, como resultado de la entrevista al personal directamente relacionado con esta área. También se detalla las amenazas al que están expuestos los activos más importantes y se define las salvaguardas apropiadas para brindar seguridad a dichos activos.

Para este proceso se determina la realización de un análisis cualitativo de los activos que se encuentran en el Data Center FICA.

El presente capítulo se divide en tres procesos que son la planificación, el análisis de riesgos y la gestión de riesgos, como se muestra en la Figura 14.

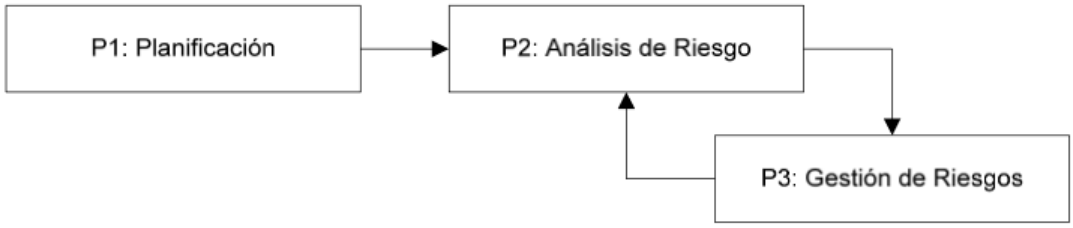


Figura 14 Proceso de Análisis de Riesgo
Fuente: Ministerio de Hacienda y Administraciones, 2016

4.1. Planificación

Como objetivo principal de este análisis es detectar las vulnerabilidades a las que se encuentra expuesta la información del Data Center FICA, en el apartado 3.5 de este documento se enuncia los resultados obtenidos y considerados como vulnerabilidades de este sistema de información.

Con la ayuda de la metodología se genera un plan de seguridad para mejorar la disponibilidad, integridad, confidencialidad y autenticidad de la seguridad de la información del Data Center FICA.

4.2. Análisis de riesgos

Para llevar a cabo el proceso de análisis de riesgo se hace uso de la herramienta PILAR versión 7.2.3 para Windows, que se basa en la metodología Magerit. Para el uso de esta herramienta se obtuvo una licencia de evaluación. En el Anexo 3 se presenta el proceso de instalación y en el Anexo 4 se encuentra el manual de uso de esta herramienta informática.

En la Figura 15 se muestra el panel principal del proyecto siendo este configurado como confidencial.

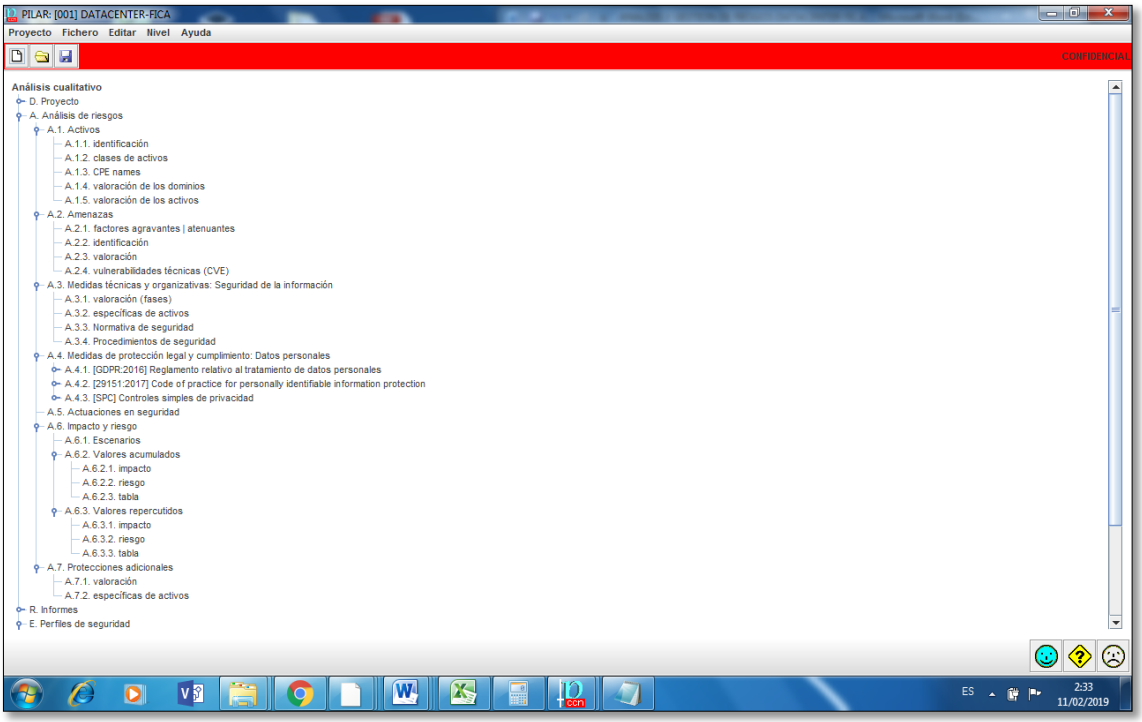


Figura 15 Panel Principal de Proyecto
Fuente: Herramienta PILAR

4.2.1. Se elabora Identificación de los activos de información

Los activos que formarán parte del análisis y gestión de riesgos han sido seleccionados en base a la importancia que tienen para la facultad. De acuerdo a la metodología Magerit, cada

activo de información debe tener asignado un código identificativo, en la Figura 16 se muestra un ejemplo del código utilizado. Este código está estructurado de la siguiente manera:

- Tipo de activo: estas dos primeras letras describen el tipo de activo al que pertenece (Ejemplo: ES esencial, HW hardware, SW software y EA elemento auxiliar).
- Ubicación: siglas que definen el lugar en el que está el activo (Ejemplo: FICA Facultad de Ingeniería en Ciencias Aplicadas).
- Número de activo: este fragmento muestra la numeración del total de los activos.
- Siglas que identifican el activo: son siglas que representan al nombre del activo, para que sea fácil de reconocer (Ejemplo: RU revista universitaria, SRR servidor radius, PV1 proxmox virtual 1, PV2 proxmox virtual 2, etc).

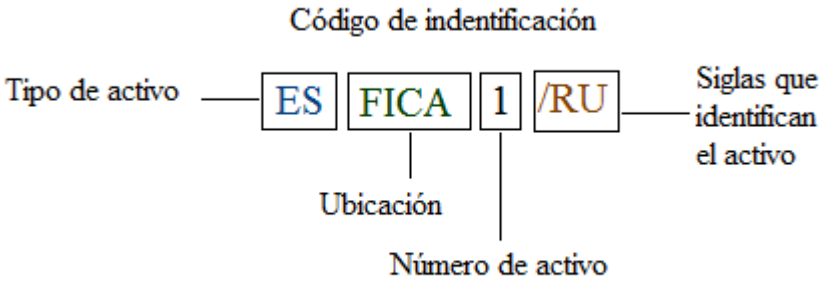


Figura 16 Código de identificación del activo

En la Tabla 10 se listan los activos a ser evaluados en la herramienta PILAR, los cuales han sido previamente clasificados como lo recomienda la metodología Magerit. Se asigna un código para cada activo como se muestra en la Figura 16 y un nombre que represente al activo.

Tabla 10

Activos Data Center FICA

ACTIVOS DEL DATACENTER FICA		
	Esenciales	
Código	**Nombre**	**Detalle**
ESFICA1/RU	RU	IBM Systemx3500 M4 Revista Universitaria
ESFICA2/SRR	SRR	Servidor Radius
	Equipos Informáticos (Hardware)	
HWFICA1/PV1	HPPV1	HP Proliant DL360 G9 (Proxmox PV1)
HWFICA2/PV2	HPPV2	HP Proliant DL360 G9 (Proxmox PV2)
HWFICA3/PV3	HPPV3	HP Proliant DL360 G9 (Proxmox PV3)
HWFICA4/PV4	HPPV4	HP Proliant ML150 (Proxmox PV4)
HWFICA5/SS	IBMSS	IBM System x3650 M3 (Sin Servicio)
HWFICA6/CS1	IBMCS1	IBM System x3250 M3 (CISIC)
HWFICA7/CS2	IBMCS2	IBM System x3250 (CISIC)
HWFICA8/SWC	CORE	Switch de Core Catalyst 4506-E
HWFICA9/RTM	ROUTER	RouterBoard 1100AHX2 Mikrotik
HWFICA10/SWD1	SWD1	Switch de Distribución 3Com 4500G PROXMOX
HWFICA11/SWQP	SWQP	Switch de distribución inalámbrica QPCOM
HWFICA12/SWD2	SWD2	Switch de distribución CISCO Linksys SR224G
HWFICA13/SWD3	SWD3	Switch de Distribución 3Com 3226 SERVIDORES
	Aplicaciones Informáticas (Software)	
SWFICA1/P	SRP	Proxmox
SWFICA2/O	SRO	Opina
SWFICA3/M	SRM	Reactivos
SWFICA4/B	SRB	Biométrico
	Elementos Auxiliar	
EAFICA1/SE	SE	Sistema Eléctrico
EAFICA2/AA	AA	Aire Acondicionado
EAFICA3/UPS	UPS	UPS
EAFICA4/CS	CS	Cámara de Seguridad
EAFICA5/CA	CA	Control de Acceso
EAFICA6/BB	BB	Backbone
EAFICA7/CU	CE	Cableado Estructurado

A continuación se ingresa cada activo en la herramienta PILAR (ver manual de uso Anexo 4), como se sugiere en la Tabla 10. En la Figura 17 se muestra los activos ingresados, con los cuales se trabajará durante todo este proceso.

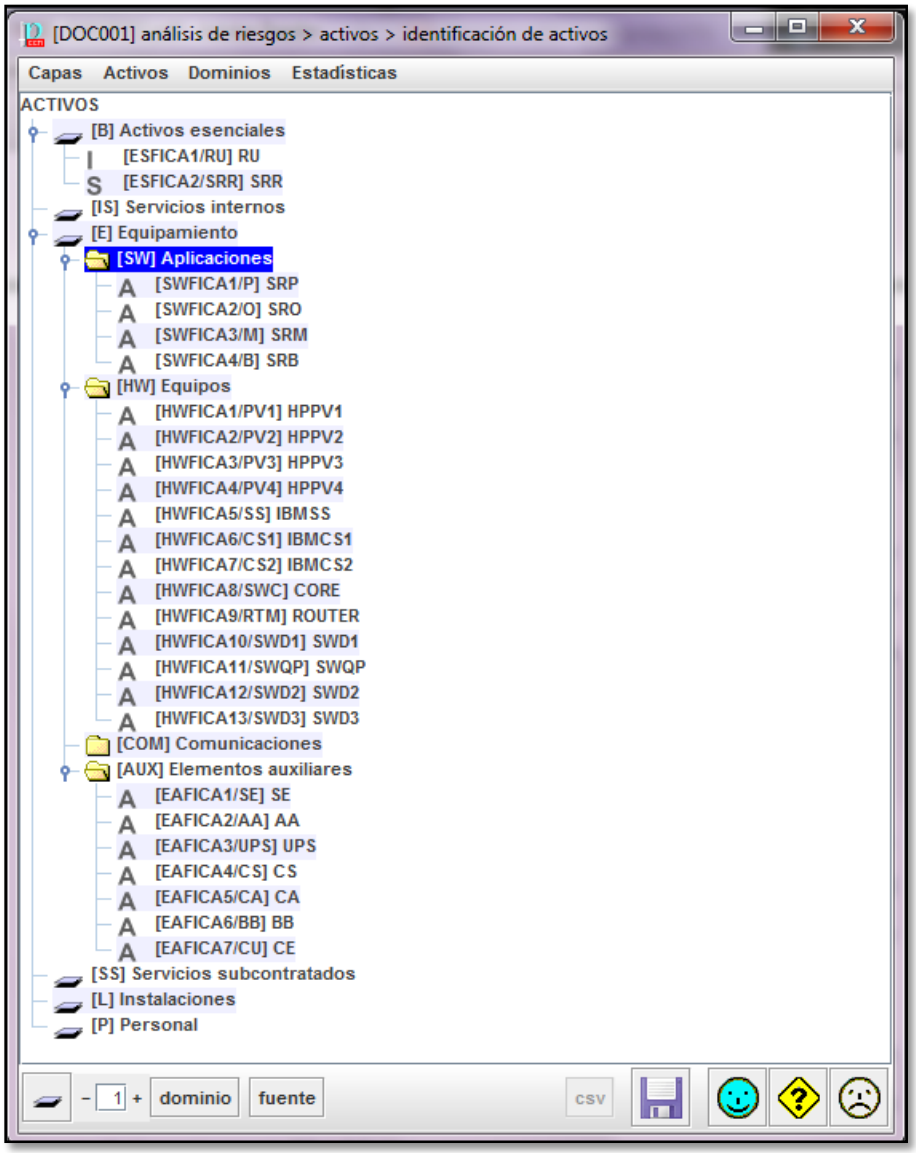


Figura 17 Identificación de activos

4.2.2. Dependencia de activos

Existen activos que dependen unos de otros, pudiendo ser unos más significativos; esto quiere decir que, si un activo inferior se ve afectado por un incidente de seguridad, el activo superior también se verá afectado; por ende, se deberá tomar en cuenta estas dependencias al momento de dar la valoración a los activos.

En la Figura 18 se muestra las dependencias de los activos, en donde el servidor Radius y el servidor de la Revista Universitaria son fundamentales y estos a su vez dependen de los

equipos de red como son los switch y routers, de la misma manera estos dependen de los elementos auxiliares. Como activos inferiores, se consideran a los elementos auxiliares y equipos de red; y como activos superiores se consideran a los servidores.

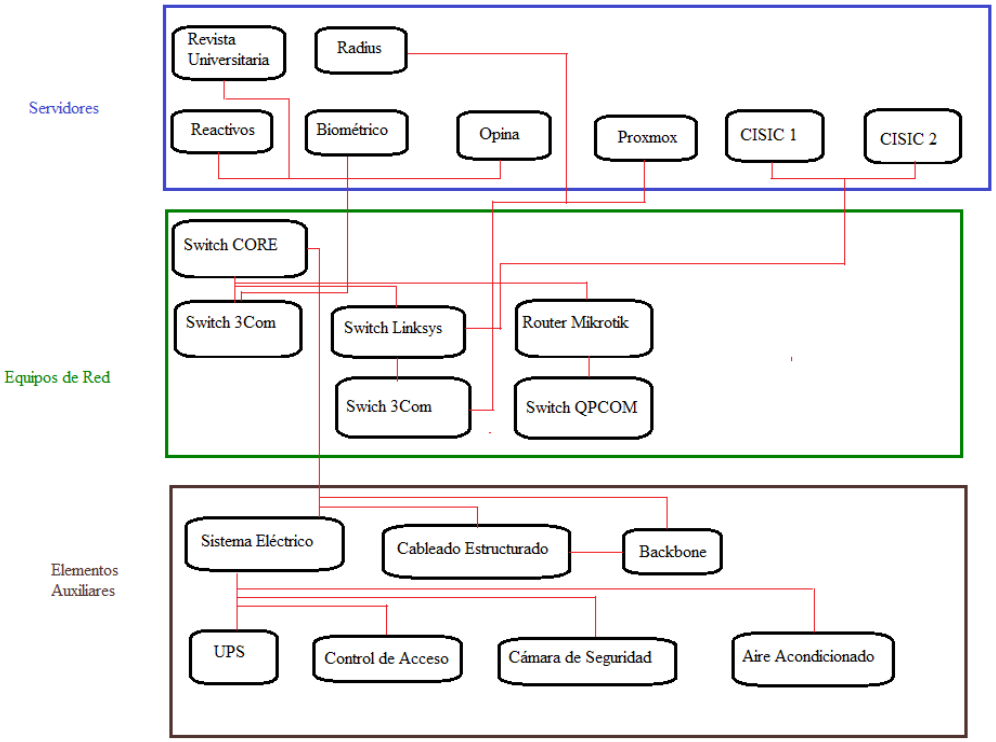


Figura 18 Dependencia de activos

4.2.3. Clasificación de los activos

Para clasificar un activo dentro de una categoría se toma en consideración la información que maneja cada uno de ellos, un activo puede pertenecer a varias categorías de tipos de activos; en la Tabla 11 se muestra la clasificación de los activos de información en base a sus propias características y a los diferentes tipos descritos en el "Catálogo de elementos" de la metodología Magerit. (Ministerio de Hacienda y Administraciones, 2016); el código que se representa en la columna "Tipo de activo" refleja la posición jerárquica y la característica específica de cada activo como lo sugiere la metodología y como se muestra en la herramienta PILAR, en la Figura 19 se puede ver el ejemplo de clasificación o tipificación de un activo.

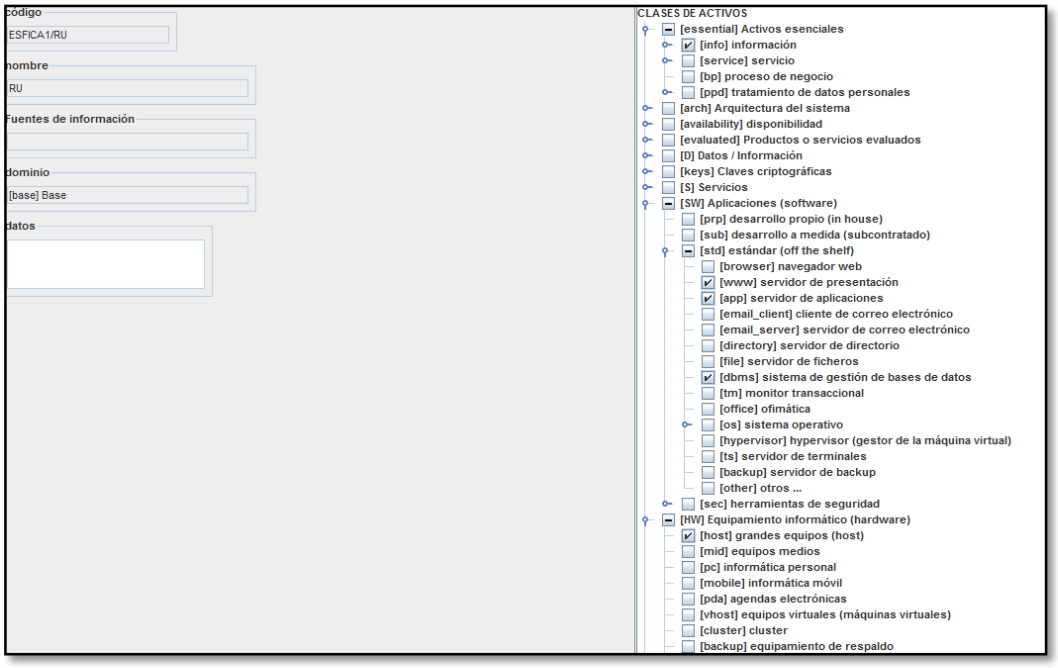


Figura 19 Clasificación del activo Revista Universitaria

A continuación en la Tabla 11 se resume la clasificación de todos los activos considerados en este proyecto.

Tabla 11

Caracterización activos Data Center

Nombre y código	Tipo de activo
Servidor Revista Universitaria [ESFICA1/RU]	[essential] [info]información [SW] [std] [www] servidor de presentación [SW] [std] [app] servidor de aplicaciones [SW] [std] [dbms]sistema de gestión de base de datos [HW] [host]grandes equipos
Servidor Radius [ESFICA2/SRR]	[essential] [service]servicio [D] [files] ficheros de datos [D] [conf] datos de configuración [D] [int] datos de gestión interna

	[D] [password] credenciales
	[D] [acl] datos de control de acceso
	[D] [log] registro de actividad
	[keys][com] protección de las comunicaciones
	[S] [prov] [int]interno (usuarios y medios de la propia organización)
	[HW] [host] grandes equipos
Servidor Proxmox PV1 [HWFICA1/PV1]	[HW] [host]grandes equipos
	[HW] [backup] equipamiento de respaldo
Servidor Proxmox PV2 [HWFICA2/PV2]	[HW] [host]grandes equipos
	[HW] [backup] equipamiento de respaldo
Servidor Proxmox PV3 [HWFICA3/PV3]	[HW] [host]grandes equipos
	[HW] [backup] equipamiento de respaldo
Servidor Proxmox PV4 [HWFICA4/PV4]	[HW] [host]grandes equipos
	[HW] [backup] equipamiento de respaldo
Servidor Sin Servicio [HWFICA5/SS]	[HW] [host]grandes equipos
Servidor CISIC Geoportal [HWFICA6/CS1]	[D]Datos / información
	[S] [prov] [ext] a usuarios externos
	[S] [prov] [int] usuarios internos
	[S] [prov] [file] almacenamiento de ficheros
	[SW] [std] [www] servidor de presentación
	[SW] [std] [app] servidor de aplicaciones
	[SW] [std] [dbms] sistema de gestión de base de datos
	[HW] [host]grandes equipos
Servidor CISIC Pruebas [HWFICA7/CS2]	[D]Datos / información
	[S] [prov] [ext] a usuarios externos

	[S] [prov] [int] usuarios internos
	[S] [prov] [www] world wide web
	[SW] [std] [www] servidor de presentación
	[SW] [std] [app] servidor de aplicaciones
	[SW] [std] [dbms] sistema de gestión de base de datos
	[HW] [host]grandes equipos
Switch CORE [HWFICA8/SWC]	[HW] [network][router] encaminador
Router Mikrotik [HWFICA9/RTM]	[HW] [network][router] encaminador
Switch Distribución 1 [HWFICA10/SWD1]	[HW] [network][switch] conmutador
Switch QPCom [HWFICA11/SWQP]	[HW] [network][switch] conmutador
Switch Distribución 2 [HWFICA12/SWD2]	[HW] [network][switch] conmutador
Switch Distribución 3 [HWFICA13/SWD3]	[HW] [network][switch] conmutador
Servidor Proxmox [SWFICA1/P]	[S] Servicios
	[SW] Aplicaciones (software)
	[HW] [host]grandes equipos
Servidor Opina [SWFICA2/O]	[D] [files] ficheros de datos
	[D] [log] registro de actividad
	[S] [prov] [ext] a usuarios externos
	[S] [prov] [int] usuarios internos
	[S] [prov] [file] almacenamiento de ficheros
	[SW] [std] [www] servidor de presentación
	[SW] [std] [app] servidor de aplicaciones
	[HW] [host]grandes equipos
Servidor Reactivos	[D] [files] ficheros de datos
[SWFICA3/M]	[D] [log] registro de actividad
	[D] [backup]copias de respaldo

	[D] [acl] datos de control de acceso
	[S] [prov] [int] usuarios internos
	[S] [prov] [www] world wide web
	[S] [prov] [ftp]transferencia de ficheros
	[SW] [std] [www] servidor de presentación
	[SW] [std] [app] servidor de aplicaciones
	[HW] [host] grandes equipos
Servidor Biométrio [SWFICA4/B]	[D] [log] registro de actividad
	[D] [password] credenciales
	[D] [acl] datos de control de acceso
	[S] [prov] [int] usuarios internos
	[S] [prov] [idm] gestión de identidades
	[SW] [std] [dbms] sistema de gestión de base de datos
	[HW] [host]grandes equipos
Sistema Eléctrico [EAFICA1/SE]	[AUX][power] fuentes de alimentación
	[AUX][supply] suministros esenciales
Aire Acondicionado [EAFICA2/AA]	[AUX][ac] equipos de climatización
Sistema de Alimentación Ininterrumpida [EAFICA3/UPS]	[AUX][ups] sistema de alimentación ininterrumpida
Cámara de Seguridad [EAFICA4/CS]	[AUX][other] otros
Control de Acceso [EAFICA5/CA]	[AUX][other] otros
Backbone [EAFICA6/BB]	[AUX][cabling][fiber] fibra óptica
Cableado Estructurado [EAFICA7/CU]	[AUX][cabling]cableado de datos

4.2.4. Valoración de activos

Para la valoración de los activos, la metodología Magerirt recomienda un valor en la escala del cero al diez como se refiere en la Tabla 2, donde el cero significa que el activo no tiene mucha importancia y que su pérdida o daño no afectará a las actividades de la facultad; pero lo contrario sucedería si la valoración es diez, implica que la pérdida o daño de ese activo tendría graves consecuencias para la facultad.

La valoración de cada activo se basa en la importancia que tiene este para la facultad, para lo cual se evalúa las cuatro propiedades de la seguridad de la información como se estableció en el alcance de este proyecto, siendo estas: confidencialidad, integridad, disponibilidad y autenticidad.

Para poder asignar un valor a la propiedad de disponibilidad en un activo es necesarios responder la siguiente pregunta ¿Qué importancia tendría que el activo no estuviera disponible?; en el caso de la propiedad de integridad es necesario responder a la pregunta ¿Qué importancia tendría que los datos fueran modificados fuera de control?; en la propiedad de confidencialidad se debe responder a la pregunta ¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas? y referente a la propiedad de autenticidad se debe responder a la pregunta ¿Qué importancia tendría que quien accede al servicio no sea realmente quien cree?; las respuestas a estas preguntas debe ser asignada empleando un rango de valores de 0 a 10 en base a las tablas puntualizadas en el Anexo 6**,** según la propiedad a evaluar.

El análisis y valoración de estas cuatro propiedades de la seguridad de la información, se estableció en una mesa de trabajo asistida por el encargado del Data Center y el responsable de este proyecto, como se puede ver en el Anexo 6.

En la Figura 20 se muestra la valoración de las propiedades de la información por cada activo; los criterios de valoración buscan ser lo más homogéneo posible entre todos los tipos

de activos, por tal razón los criterios establecidos son basados en los criterios descritos en el libro de “Catálogos de elementos” de la metodología Magerit.

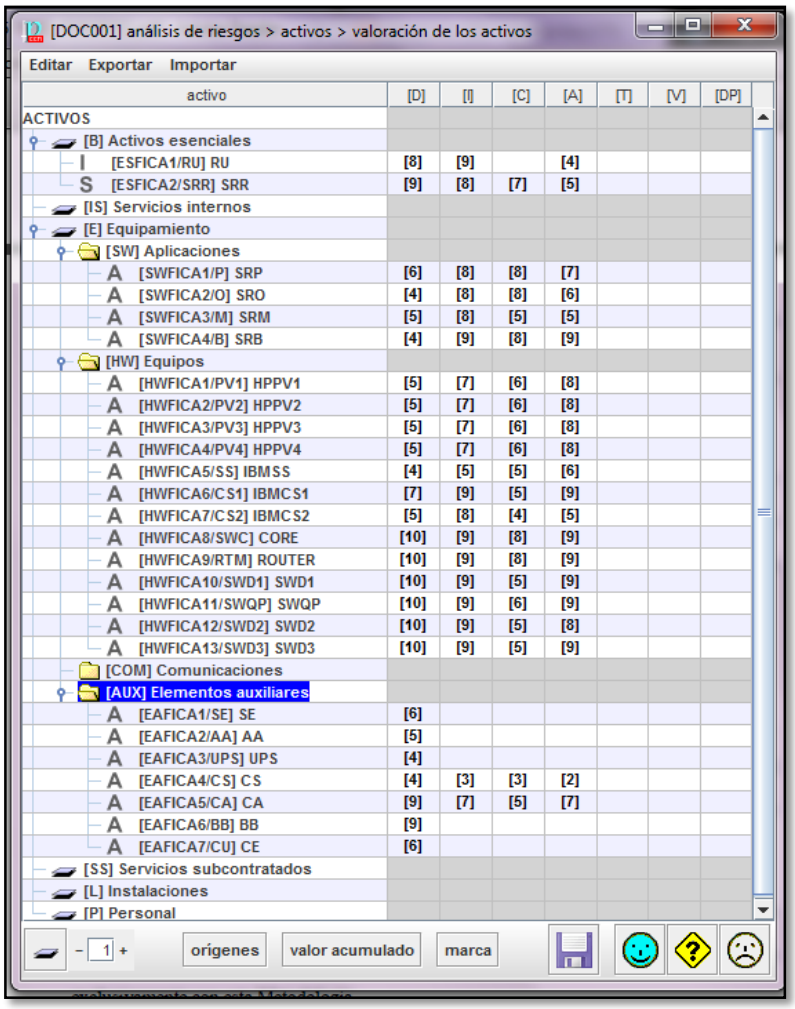


Figura 20 Valoración de activos

4.2.5. Identificación de Amenazas

La selección de amenazas de los activos se realiza en función del tipo o tipos de activos en los que se ha clasificado a cada uno de los elementos inversos en el análisis de riesgo. PILAR facilita esta tarea, ya que cada amenaza sólo puede afectar a un determinado tipo de activo, por lo tanto, en este proyecto se utiliza la información proporcionada por esta herramienta; utilizando su biblioteca de amenazas, las que se asocian a cada uno de los activos de manera automática. Las amenazas que se pueden encontrar en un sistema de información están contempladas en la metodología Magerit.

En el Anexo 7 se puede ver de forma detallada las amenazas que se presentan por cada activo. En la Figura 21 se puede apreciar el listado que PILAR proporciona de posibles amenazas para el activo tomado de ejemplo, que es un activo clasificado como esencial con código [ESFICA1/RU] que es el Servidor Radius.

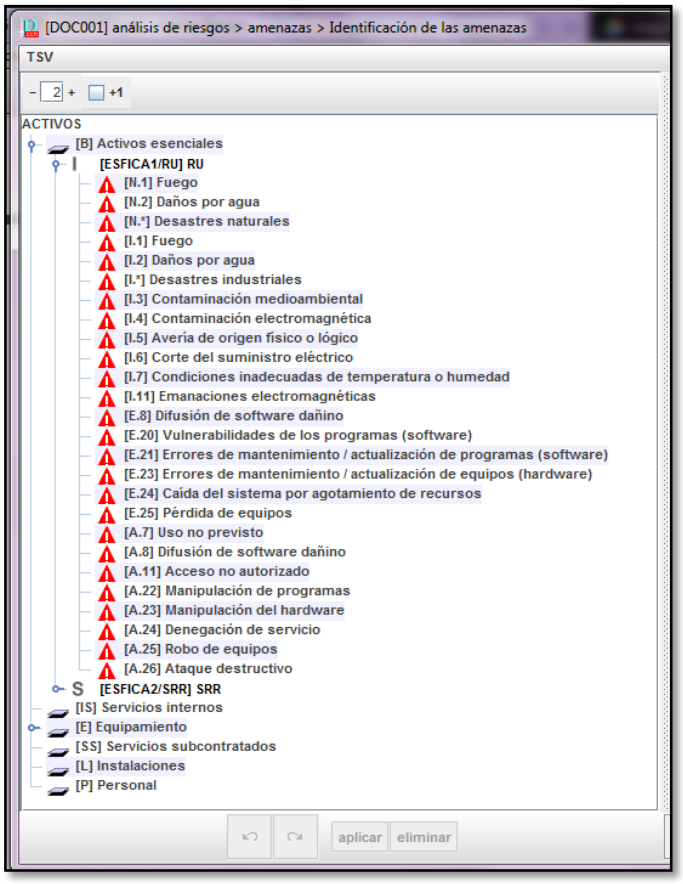


Figura 21 Identificación de amenazas del activo esencial ESFICA1/RU

4.2.6. Valoración de amenazas

PILAR proporciona de igual manera de forma automática el valor de las amenazas, definiendo la frecuencia o probabilidad de posible materialización de las mismas y la degradación por niveles o porcentajes de las cuatro dimensiones que están siendo evaluadas, como se muestra en la Figura 22 tomando como ejemplo los valores de las amenazas del activo con código [ESFICA1/RU].

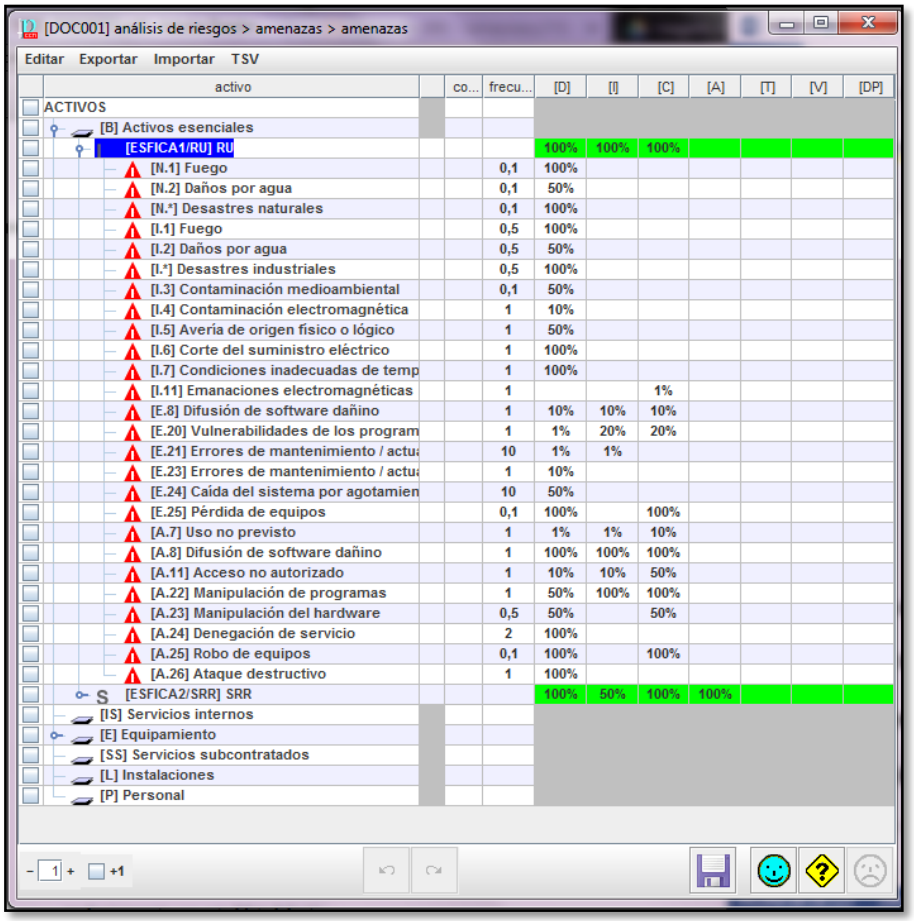


Figura 22 Valoración de amenazas del activo esencial ESFICA1/RU

Determinar el grado de degradación y la frecuencia de ocurrencia de cada amenaza sobre cada activo, tiene el fin de saber el impacto y riesgo potencial de dicha amenaza sobre el activo. La frecuencia de ocurrencia se evalúa de acuerdo a los valores que se establecen en la Tabla 4 y el grado de degradación que se establecen en la Tabla 3. En el Anexo 7 se presentan los resultados del análisis de riesgos, donde se detallan las amenazas que afectan a cada activo con su valor de probabilidad de ocurrencia y el valor de degradación.

4.2.7. Identificación y Valoración de Salvaguardas

Después de haber realizado el análisis de riesgo la misma herramienta PILAR sugiere una lista de buenas prácticas que se muestra en la Figura 23, que son necesarias para gestionar la seguridad del Data Center FICA. Además, la herramienta PILAR designa un valor a la salvaguarda, siendo este valor interpretado de la siguiente manera:

- Salvaguardas valoradas en [8], tiene que ser implementadas o tratadas de forma inmediata, tiene prioridad máxima en este caso.
- Salvaguardas valoras en [6-7], tiene que ser implementadas o tratadas de forma inmediata, ya que tiene un nivel de criticidad alto.
- Salvaguardas valoradas en [4-5], tiene que ser implementadas o tratadas, a mediano plazo, ya que tiene un nivel de criticidad medio.
- Salvaguardas valoradas en [2-3], tiene que ser implementadas o tratadas, a mediano plazo, ya que tiene un nivel de criticidad bajo.

Figura 23 Identificación y Valoración de Salvaguardas

La herramienta PILAR sugiere un listado de medidas a tomar para minimizar los riesgos presentes en los activos de información. Pudiendo ser tomados como punto de partida para la elaboración o actualización de las políticas que son parte del Plan de Seguridad.

En el Anexo 8, se detalla el tratamiento del riesgo, en donde se seleccionan los controles o salvaguardas para cada grupo de activo, después de analizar a la amenaza a la que está expuesto, la vulnerabilidad y el riesgo al que puede enfrentarse.

4.2.8. Estimación del Impacto

El impacto es el daño que se origina sobre el activo derivado de la materialización de las amenazas. En la Figura 24 se representan estos valores, sacando las siguientes conclusiones respecto a la magnitud del impacto:

- Los activos marcados de color rojo representan un nivel de impacto crítico en la dimensión de disponibilidad, pudiendo verse severamente afectadas las funciones del Data Center. Estos activos son los equipos de red (routers, switchs).
- Los activos marcados de color rosa representan un nivel de impacto muy alto en las dimensiones de disponibilidad, confidencialidad, integridad y autenticidad. Con la posibilidad de causar perdida de funcionalidad del Data Center, divulgación no autorizada de la información, que la información sea alterada sin control ni autorización y que accedan usuarios no permitidos.
- Los activos marcados de color amarillo representan un nivel de impacto alto, siendo de igual forma susceptibles a la materialización de amenazas, acusando daños en las cuatro dimensiones de la seguridad de la información.

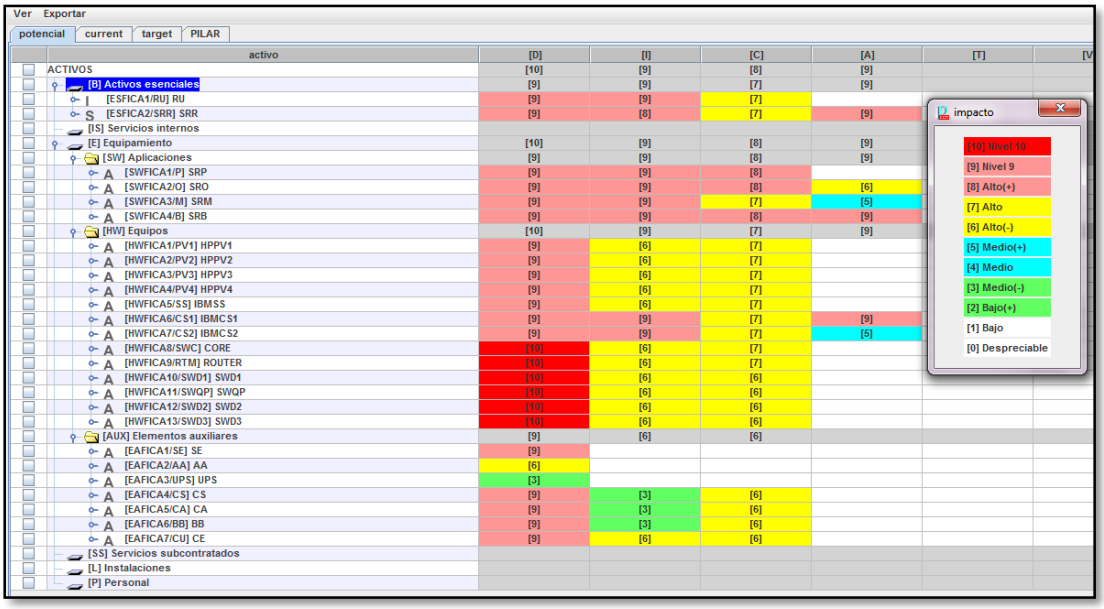


Figura 24 Valor del impacto potencial por activo

Además, la herramienta PILAR proporciona los resultados del impacto luego de implementar las salvaguardas apropiadas, mostrando los valores conforme se observa en la Figura 25, donde notablemente se puede observar que estos valores disminuyen.

activo	[D]	[I]	[C]	[A]
ACTIVOS	[6]	[4]	[4]	[5]
[B] Activos esenciales	[5]	[4]	[3]	[5]
[ESFICA1/RU] RU	[5]	[4]	[3]	
[ESFICA2/SRR] SRR	[5]	[4]	[3]	[5]
[IS] Servicios internos				
[E] Equipamiento	[6]	[4]	[4]	[2]
[SW] Aplicaciones	[5]	[4]	[4]	[2]
[SWFICA1/P] SRP	[5]	[4]	[4]	
[SWFICA2/O] SRO	[5]	[4]	[4]	[2]
[SWFICA3/M] SRM	[5]	[4]	[3]	[1]
[SWFICA4/B] SRB	[5]	[4]	[4]	[1]
[HW] Equipos	[6]	[4]	[3]	[1]
[HWFICA1/PV1] HPPV1	[5]	[1]	[3]	
[HWFICA2/PV2] HPPV2	[5]	[1]	[3]	
[HWFICA3/PV3] HPPV3	[5]	[1]	[3]	
[HWFICA4/PV4] HPPV4	[5]	[1]	[3]	
[HWFICA5/SS] IBMSS	[5]	[1]	[3]	
[HWFICA6/CS1] IBMCS1	[5]	[4]	[3]	[1]
[HWFICA7/CS2] IBMCS2	[5]	[4]	[3]	[1]
[HWFICA8/SWC] CORE	[6]	[1]	[3]	
[HWFICA9/RTM] ROUTER	[6]	[1]	[3]	
[HWFICA10/SWD1] SWD1	[6]	[1]	[2]	
[HWFICA11/SWQP] SWQP	[6]	[1]	[2]	
[HWFICA12/SWD2] SWD2	[6]	[1]	[2]	
[HWFICA13/SWD3] SWD3	[6]	[1]	[2]	
[AUX] Elementos auxiliares	[5]	[2]	[2]	
[EAFICA1/SE] SE	[5]			
[EAFICA2/AA] AA	[2]			
[EAFICA3/UPS] UPS	[0]			
[EAFICA4/CS] CS	[5]	[0]	[2]	
[EAFICA5/CA] CA	[5]	[0]	[2]	
[EAFICA6/BB] BB	[5]	[0]	[2]	
[EAFICA7/CU] CE	[5]	[2]	[2]	
[SS] Servicios subcontratados				
[L] Instalaciones				
[P] Personal				

Figura 25 Estimación de impacto después de implementar salvaguardas.

En el Anexo 9 se muestra una comparativa del impacto existente y el impacto que existe después de implementar salvaguardas, pudiendo aseverar que posterior a la implementación de las buenas prácticas de seguridad, sugeridas por la herramienta PILAR el impacto disminuye en un 42 % aproximado.

4.2.9. Estimación del Riesgo

El cálculo del valor del riesgo, la herramienta PILAR proporciona de manera automática, pero en el apartado 2.5.1.4, se explica la manera de interpretar este valor.

La estimación del riesgo en PILAR, resulta de la relación entre la probabilidad de que el riesgo ocurra, con el impacto causado producto de la ocurrencia del riesgo.

En la Figura 26 se muestra el riesgo al que se enfrenta cada activo, los colores indican el nivel de criticidad, así mismo como se muestra en la matriz de riesgo en la Tabla 6, pudiendo observar que el nivel de riesgo del sistema que está siendo evaluado es crítico, siendo necesario implementar salvaguardas de manera inmediata para minimizar el riesgo.

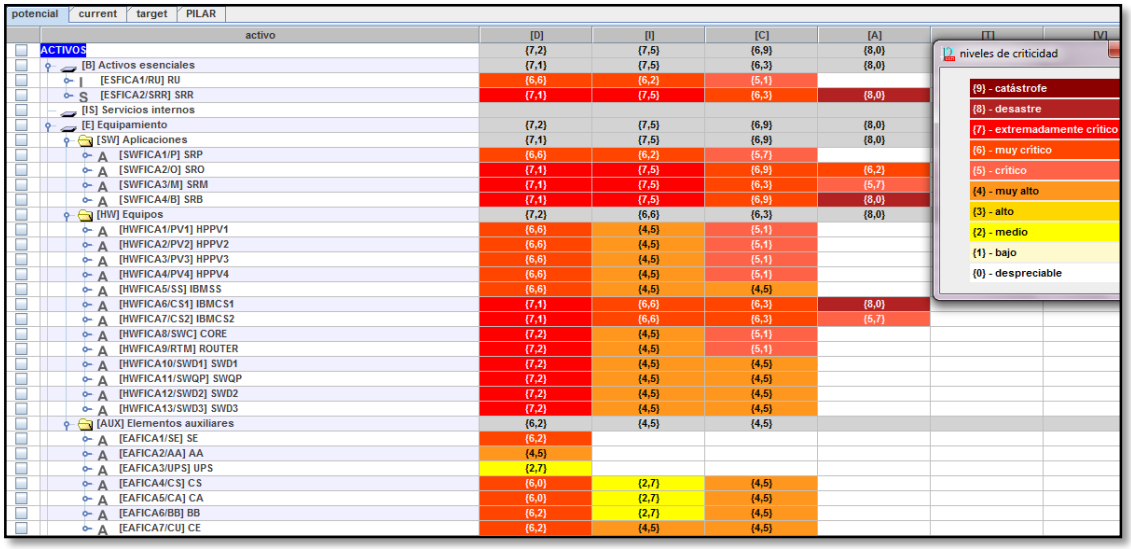
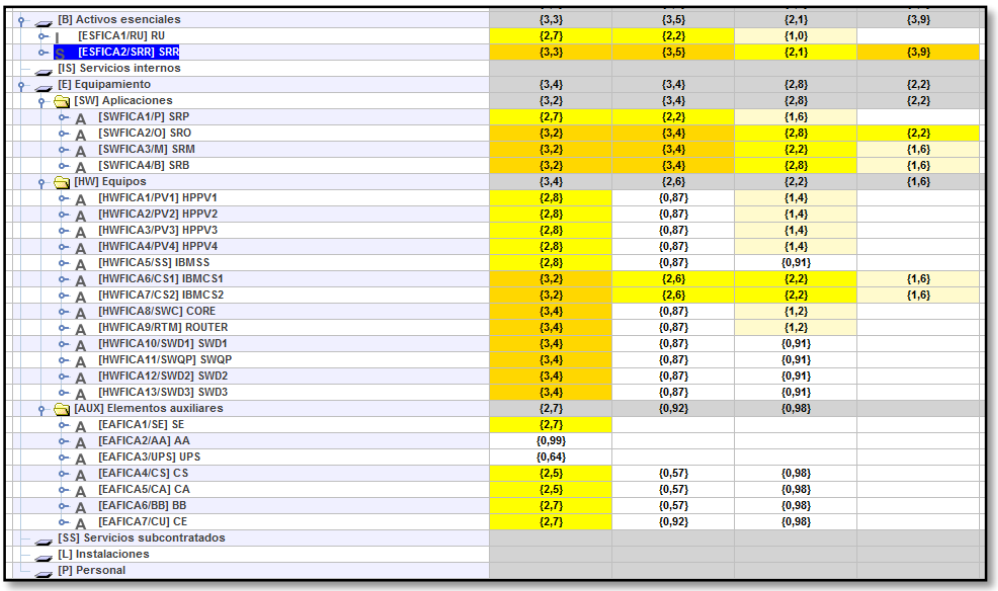


Figura 26 Riesgo potencial por activo

La herramienta PILAR proporciona los resultados del riesgo residual, que es riesgo que se mantiene a pesar de la implementación o planificación de las salvaguardas. En la Figura 27 se

muestran los valores del riesgo, aunque estos son de niveles menores y tienen salvaguardas, no se ha podido eliminar el riesgo en su totalidad.



[B] Activos esenciales	{3,3}	{3,5}	{2,1}	{3,9}
[ESFICA1/RU] RU	{2,7}	{2,2}	{1,0}	
[ESFICA2/SRR] SRR	{3,3}	{3,5}	{2,1}	{3,9}
[IS] Servicios internos				
[E] Equipamiento	{3,4}	{3,4}	{2,8}	{2,2}
[SW] Aplicaciones	{3,2}	{3,4}	{2,8}	{2,2}
[SWFICA1/P] SRP	{2,7}	{2,2}	{1,6}	
[SWFICA2/O] SRO	{3,2}	{3,4}	{2,8}	{2,2}
[SWFICA3/M] SRM	{3,2}	{3,4}	{2,2}	{1,6}
[SWFICA4/B] SRB	{3,2}	{3,4}	{2,8}	{1,6}
[HW] Equipos	{3,4}	{2,6}	{2,2}	{1,6}
[HWFICA1/PV1] HPPV1	{2,8}	{0,87}	{1,4}	
[HWFICA2/PV2] HPPV2	{2,8}	{0,87}	{1,4}	
[HWFICA3/PV3] HPPV3	{2,8}	{0,87}	{1,4}	
[HWFICA4/PV4] HPPV4	{2,8}	{0,87}	{1,4}	
[HWFICA5/SS] IBMSS	{2,8}	{0,87}	{0,91}	
[HWFICA6/CS1] IBMCS1	{3,2}	{2,6}	{2,2}	{1,6}
[HWFICA7/CS2] IBMCS2	{3,2}	{2,6}	{2,2}	{1,6}
[HWFICA8/SWC] CORE	{3,4}	{0,87}	{1,2}	
[HWFICA9/RTM] ROUTER	{3,4}	{0,87}	{1,2}	
[HWFICA10/SWD1] SWD1	{3,4}	{0,87}	{0,91}	
[HWFICA11/SWQP] SWQP	{3,4}	{0,87}	{0,91}	
[HWFICA12/SWD2] SWD2	{3,4}	{0,87}	{0,91}	
[HWFICA13/SWD3] SWD3	{3,4}	{0,87}	{0,91}	
[AUX] Elementos auxiliares	{2,7}	{0,92}	{0,98}	
[EAFICA1/SE] SE	{2,7}			
[EAFICA2/AA] AA	{0,99}			
[EAFICA3/UPS] UPS	{0,64}			
[EAFICA4/CS] CS	{2,5}	{0,57}	{0,98}	
[EAFICA5/CA] CA	{2,5}	{0,57}	{0,98}	
[EAFICA6/BB] BB	{2,7}	{0,57}	{0,98}	
[EAFICA7/CU] CE	{2,7}	{0,92}	{0,98}	
[SS] Servicios subcontratados				
[L] Instalaciones				
[P] Personal				

Figura 27 Riesgo Residual

En el Anexo 9 se muestra una comparativa entre el riesgo potencial y el residual, pudiendo afirmar que el riesgo disminuye en un 38.66%, luego de la implementación de las salvaguardas establecidas.

4.2.10. Interpretación de Resultados

Después de haber realizado el proceso de análisis de riesgos, la herramienta PILAR refleja en la Figura 28 los activos que están expuestos a mayor nivel de riesgo. Pudiendo decir que el Servidor Radius y Sevidor de la Revista Universitaria son los activos más críticos, seguidamente tenemos con igual alto riesgos a las Servidores Opina, Reactivos, y Biométrico. Cabe recalcar que los equipos de conectividad igual tienen un riesgo elevado, por tal razón se debe gestionar dichos riesgos.

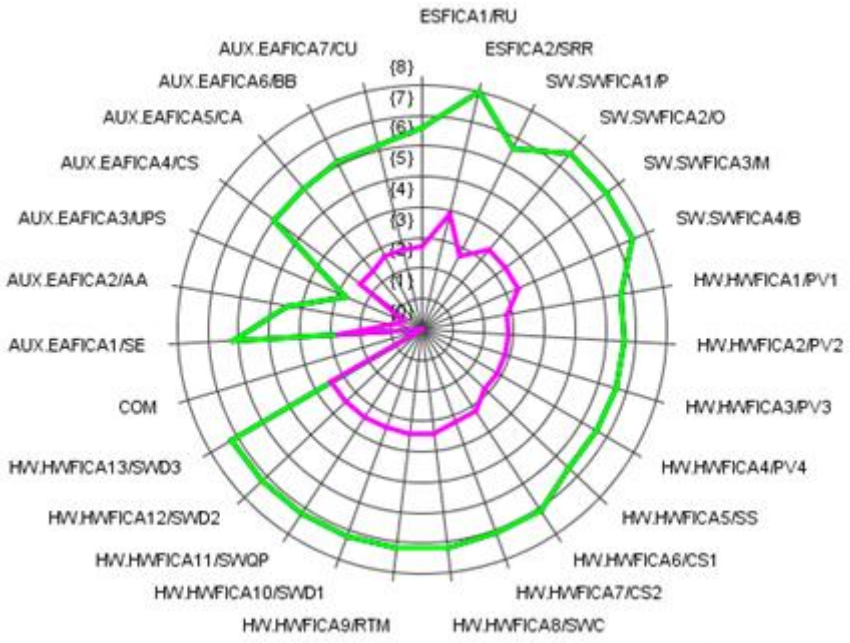


Figura 28 Nivel de riesgo por activo

4.3. Gestión de Riesgo

La gestión del riesgo es la planeación para manejar la amenaza a la que se está enfrentado, a través de una secuencia de actividades que incluyen identificación de la amenaza, análisis de vulnerabilidades y evaluación del riesgo, para luego establecer las estrategias para su tratamiento, las estrategias incluyen eliminar, mitigar, compartir o financiar, con la finalidad de reducir el impacto negativo del riesgo, determinando los controles o salvaguardas sugeridas por PILAR en el apartado 4.2.7. Este proceso está plasmado en el Anexo 8, documento donde se detalla el informe del tratamiento del riesgo, el cual servirá como base para la actualización de las políticas que son parte del Plan de Seguridad y están descritas en el Anexo 10.

Capítulo 5

Desarrollo de Planes para mejorar la Seguridad de la Información

Después de haber realizado el análisis de riesgos y haber identificado los activos críticos, podemos plantear salvaguardas que serán parte del Plan de Seguridad. El Plan de Seguridad de la Información proporciona directrices necesarias para gestionar de manera correcta la seguridad de la información, este documento servirá como guía para gestionar adecuadamente los activos, así como también proporcionará una serie de pautas para priorizar la gestión de los riesgos de la seguridad de la información. Además, se plantea un Plan de Acción, que su cumplimiento dará como resultado, mejoras en la seguridad de información.

5.1. Plan de Seguridad

En el documento que se elabora a continuación, se detalla las actividades que se deben realizar en el Data Center, para disminuir los riesgos identificados y mejorar la seguridad de la información. Cabe recalcar que el presente proyecto de titulación está centrado en la fase de planificación, es decir la implementación, verificación y mejoramiento del plan queda a total criterio de los encargados del Data Center.

5.2. Plan de Acción

Este documento detalla la gestión de los diferentes proyectos que se establecieron en el Plan de Seguridad, con la finalidad de coordinar y comprometer al personal a cargo del Data Center; ya que, con el apoyo de las autoridades respectivas se puede conseguir el objetivo propuesto.

Facultad de Ingeniería en Ciencias Aplicadas
FICA

PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA EL DATA CENTER FICA

2019

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA EL DATA CENTER

Versión	1.0
Elaborado por:	Sra. Vanessa Marilyn Jácome Chávez
	MSc. Jaime Michilena
Revisado por:	
Aprobado por:	

I. INTRODUCCIÓN

La información es el activo más importante para todo tipo de instituciones el cual permite el progreso y evolución de las actividades propias del negocio, como también permitir la mejora y eficiencia en la prestación de servicios.

El aseguramiento de la información como también de los activos que la procesan, almacenan, transportan o modifican; motivan a las empresas o instituciones a utilizar diversos tipos de recursos como normativas de seguridad, metodologías y estándares.

El entorno tecnológico actual en el que todos se encuentran permanentemente conectados, conlleva a exponer a los sistemas a diversos tipos de amenazas y ataques, como también a incidentes de seguridad originados al interior de la institución, sea por error o falta de conocimiento de administradores, como usuarios de los servicios y sistemas.

El presente Plan de Seguridad permite desarrollar actividades de Seguridad de la Información del Data Center de la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la

Universidad Técnica del Norte, su análisis previo y posterior desarrollo con la finalidad de ser utilizado como una planificación para la implementación del Sistema de Gestión de Seguridad de la Información.

II. MODELO DE OPERACIÓN

El desarrollo del presente Plan de Seguridad sigue el modelo PDCA (Plan-Do-Check-Act) Planificar, Hacer, Verificar y Actuar (Mejora Continua) con la finalidad de estructurar la Planificación de la Seguridad de la Información.

Planificar:

La fase de planificación determina la situación de la institución sobre los procesos en materia de seguridad de la información, mediante la ejecución de varias actividades utilizadas para posteriores análisis. Las actividades involucran listar o actualizar los activos de información del Data Center de la FICA mediante las directrices determinadas por la Metodología Magerit, identificación de las amenazas y vulnerabilidades para la elaboración del Análisis de Riesgos.

El Análisis de Riesgos de los activos detecta la forma como se lleva a cabo los procesos internos de seguridad, de tal forma que permita establecer el Tratamiento de los Riesgos.

Hacer:

Elaboración y redacción de la documentación del SGSI, conlleva a la elaboración, actualización o modificación de la Política de Seguridad de la Información, con ello permite la justificación necesaria en la elaboración de las Normativas, Procedimientos y Estándares que forman parte del SGSI.

Como resultado de la fase de planificación se obtiene la lista de la documentación a ser elaborada como parte del Sistema de Gestión de Seguridad de la Información.

Verificar:

Son los mecanismos de verificación del cumplimiento estipulado en la Política de Seguridad de la Información y demás documentación del SGSI. La principal característica de la fase de verificación es establecer lineamientos de control y recolección de información que permita la toma de decisiones en mejoras al SGSI.

Actuar – Mejora Continua:

Analizar y establecer mejoras o correcciones de una parte o de toda la documentación del SGSI con la finalidad de corregir procesos débiles o insuficientes, elaborar nuevas políticas de seguridad en función de nuevas tecnologías o cambios que afecten a los servicios o activos de información o de ser el caso ratificar la documentación existente.

FASE 1: PLANIFICAR

Objetivo: Determinar la situación actual de la Seguridad de la Información de los activos de información, mediante la aplicación de la metodología Magerit para realizar el análisis y gestión de riesgos.

DOCUMENTACIÓN	ACTIVIDADES
Inventario de activos de información	En cumplimiento con lo dictaminado en la Metodología Magerit se debe realizar el inventario actualizado de los activos de información de seguridad de la información del Data Center de la FICA. (Ver Tabla 7)
Tipificación de los activos	Establecer el tipo de activo por cada uno de los activos e información en base al grado de criticidad de las propiedades de la información (Confidencialidad, Integridad,

	Disponibilidad y Autenticidad), en base a lo dispuesto en la metodología Magert. (Ver apartado 4.2.3)
Identificación de amenazas	Por cada tipo de activo de información identificar las posibles amenazas a los que pueden estar expuestos cada activo de información. (Ver Anexo 7)
Análisis de Riesgos	Elaborar el informe de análisis de riesgos por grupos de activos especificando la magnitud de las variables de la seguridad de la información como también la frecuencia estimada de ocurrencia. (Ver Anexo 7)
Tratamiento de Riesgos	En base a la Metodología Magerit determinar el o los tipos de tratamiento de riesgo que pueden ser aplicados por cada amenaza. (Ver Anexo 8)

FASE II: HACER

Objetivo: Realizar la documentación del Sistema de Gestión de Seguridad de la Información.

DOCUMENTACIÓN	ACTIVIDADES
Elaborar/Actualizar/Modificar la Política de Seguridad de la Información	Actualizar la Política de Seguridad de la Información la cual deberá ser aprobada por las autoridades correspondientes y difundida en la institución. (Ver Anexo 10)
Normativa de roles y responsabilidades de la Seguridad de la Información	Desarrollar e implementar la normativa referente al establecimiento de roles y responsabilidades de los activos de información en caso

	de existir algún incidente de seguridad u otras actividades operativas.
Normativa de Seguridad Física y Ambiental	Desarrollar e implementar la normativa de control y gestión sobre la seguridad física de los activos de información como del ambiente del Data Center.
Normativa de Control de Acceso	Desarrollar e implementar la normativa de control de acceso para personal interno como terceras partes acerca del acceso al interior del Data Center, especificando acciones a realizar, tiempo de intervención y equipamiento a intervenir.
Normativa del Sistema de Energía Eléctrica	Desarrollar e implementar la normativa de supervisión, monitorización y mantenimiento de los sistemas de energía eléctrica que brindan servicios a los equipos instalados en el Data Center.
Normativa de Buenas Prácticas de Gestión de Cambios	Desarrollar e implementar la normativa sobre las acciones que deben realizar los administradores o propietarios de los activos de información al existir cambios de cualquier índole.
Normativa de Gestión de Incidentes de Seguridad de la Información	Desarrollar e implementar la normativa de gestión, monitoreo y control ante la ocurrencia de eventos e incidentes de seguridad de la información.
Procedimiento para Identificación y Evaluación de Riesgos de los Activos de Información	Desarrollar e implementar el procedimiento metodológico de identificación y evaluación de riesgos de seguridad de la información. Donde permita identificar las vulnerabilidades y amenazas.

Procedimiento de Control de Acceso al Data Center	Desarrollar e implementar el procedimiento de control de acceso al Data Center de la FICA
Procedimiento de Mantenimiento de Equipos del Data Center	Desarrollar e implementar el procedimiento de mantenimiento de los equipos instalados en el Data Center.
Procedimiento de Ingreso y Salida de Equipos del Data Center	Desarrollar e implementar el procedimiento de control y supervisión de equipos que por cualquier circunstancia tengan que ingresar o salir de las instalaciones del Data Center.
Procedimiento de Generación de Copias de Respaldo	Desarrollar e implementar el procedimiento de elaboración de respaldos de la información y datos de configuración.
Estándar de Etiquetado de Activos de Información	Definir los lineamientos o el formato de la etiqueta de los activos de información.
Estándar de Creación de Contraseñas de Usuarios y Administradores de Sistemas	Definir los lineamientos o el formato de las credenciales de acceso a los sistemas de información.
Plan de Contingencia de TI	Definir el Plan de Contingencia de Tecnologías de la Información.

FASE 3: VERIFICAR

Objetivo: Evaluar el desempeño y eficiencia del SGSI, a través de instrumentos que permitan determinar la efectividad de la implantación del SGSI.

DOCUMENTACIÓN	ACTIVIDADES
Ejecutar Auditoria de la Seguridad de la Información.	Ejecución de auditorías del modelo de seguridad y temas normativos y de cumplimiento de seguridad de la información aplicables al Data Center. Monitoreo continuo de los controles de seguridad. Analizar la posibilidad de adquirir herramientas para monitorear las aplicaciones, redes, códigos maliciosos, entre otros. Verificar el cumplimiento de políticas de seguridad del Data Center.
Nota: Se debe efectuar una actualización y difusión periódica de todas las normativas y procedimientos.	

FASE 4: PLAN DE CONTINUIDAD

Objetivo: Consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el SGSI.

DOCUMENTACIÓN	ACTIVIDADES
Diseñar Plan de Mejoras	Diseñar un plan de mejoras continuas de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas para el SGSI. Actualizar el Manual de Políticas de Seguridad de la Información cuando ocurran cambios significativos. Capacitar al personal que maneje la seguridad de la información, así como al personal técnico relacionado con el Data Center.

Facultad de Ingeniería en Ciencias Aplicadas
FICA

PLAN DE ACCIÓN PARA EL DATA CENTER FICA

2019

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

PLAN DE ACCIÓN PARA EL DATA CENTER

Versión 1.0

Elaborado por: Sra. Vanessa Marilyn Jácome Chávez
MSc. Jaime Michilena

Revisado por:

Aprobado por:

I. OBJETIVO Y ALCANCE

El Data Center de la FICA, es un espacio que cuenta con equipos de red y servidores, que deben ser administrados bajo ciertos parámetros, para tener un sistema organizado y seguro. Por tal razón, se despliega este Plan de Acción con el cual se pretende tener un ambiente controlado lo que permita mejorar la seguridad de información, donde se establece responsables y tiempos estimados para su cumplimiento.

II. RESPONSABLES

N°	CARGO	FUNCIÓN
1	Administrador del Data Center	Verifica que la documentación técnica correspondiente al Data Center este correcta. Coordina actividades en el Data Center.
2	Técnico encargado Data Center	Proporcionar documentación técnica clara, precisa y actualizada. Y está encargado de las actividades operativas que se realicen en el Data Center.
3	Custodio del Activo	Personal responsable de un activo y actividades relacionadas con su funcionamiento.

III. DESCRIPCIÓN DE ACTIVIDADES

OBJETIVOS	ACCIONES ESTRATÉGICAS	INDICADORES	RESPONSABLE	PLAZOS
Establecer controles para garantizar la seguridad de la información en el Data Center de la FICA.	Se elabora el documento de las Políticas de Seguridad de Información en base a los dominios establecidos en la norma ISO/IEC 27002. Se debe modificar este documento cada vez que existan cambios significativos dentro del Data Center.	Elaborar/Actualizar/Modificar la Política de Seguridad de la Información	Administrador Data Center	
Tener control total de la operatividad del Data Center y de cada activo, y en caso de existir problemas saber a quién corresponde solucionarlos.	Se elabora un documento donde se definan responsables del Data Center y de cada uno de los activos; y así definir los roles de cada uno de ellos, estableciendo un modelo jerárquico de funciones.	Normativa de Roles y Responsabilidades de la Seguridad de la Información	Administrador Data Center	15 días

Evitar daños e interferencias que puedan producirse en el Data Center.	Se elabora un documento donde se establezcan parámetros y controles para asegurar el área física y ambiental del Data Center.	Normativa de Seguridad Física y Ambiental	Administrador Data Center / Técnico encargado	15 días
Evitar el acceso al Data Center y a los activos, de manera no autorizada.	Se elabora un documento donde se establezcan medidas de seguridad para acceder al Data Center y a los activos que ahí se alojan.	Normativa de Control de Acceso	Administrador Data Center / Técnico encargado	15 días
Mantener en buen estado, el sistema de energía eléctrica.	Se elabora un documento donde se establezca parámetros para realizar la debida supervisión, monitorización y mantenimiento del sistema eléctrico.	Normativa del Sistema de Energía Eléctrica.	Administrador Data Center / Técnico encargado	15 días
Asegurar que los cambios sean aprobados, implementados y revisados de manera controlada.	Se elabora un documento donde se establezcan buenas prácticas para realizar cualquier cambio dentro del Data Center.	Normativa de Buenas Prácticas de Gestión de Cambios	Administrador Data Center / Técnico encargado	15 días

Actuar de una manera oportuna y organizada ante la presencia de incidentes.	Se elabora un documento donde se establezcan roles y responsables, para gestionar los incidentes que se presenten.	Normativa de Gestión de Incidentes de Seguridad de la Información	Administrador Data Center / Técnico encargado	15 días
Agilitar el proceso de identificación de amenazas y vulnerabilidades, para poder asumir el riesgo de manera oportuna.	Se elabora un documento donde se establezcan los procedimientos a seguir para detectar amenazas y vulnerabilidades, para poder determinar el riesgo al que se enfrenta el sistema.	Procedimiento para Identificación y Evaluación de Riesgos de los Activos de Información	Técnico encargado / Custodios de Activos	5 días
Controlar el acceso al Data Center, evitar el acceso no autorizado y posibles eventualidades negativas que afecten a la infraestructura tecnológica.	Se elabora un documento donde se establezca el proceso y permisos para acceder al Data Center.	Procedimiento de Control de Acceso al Centro de Datos	Administrador Data Center / Técnico encargado	5 días

Optimizar el rendimiento y adecuado funcionamiento de la infraestructura tecnológica.	Se elabora un documento que defina las actividades para realizar un mantenimiento preventivo y correctivo de los activos que se alojan dentro del Data Center.	Procedimiento de Mantenimiento de Equipos del Centro de Datos	Técnico encargado / Custodios de Activos	5 días
Mantener un registro de los cambios en la infraestructura del Data Center y liberación de responsabilidades de los equipos o activos.	Se elabora un documento que proporcione directrices claras para el ingreso o salida de activo de manera adecuada en el Data Center, sin que afecte el buen funcionamiento.	Procedimiento de Ingreso y Salida de Equipos del Centro de Datos	Técnico encargado / Custodios de Activos	5 días
Tener respaldo de la información importante y manejarlos de una manera segura.	Se elabora un documento que detalle el proceso a seguir para elaborar copias de respaldos de la información y datos de configuración, de una manera segura.	Procedimiento de Generación de Copias de Respaldo	Técnico encargado / Custodios de Activos	5 días

Mantener un lugar de trabajo organizado y bien etiquetado.	Se elabora un documento donde se defina los lineamientos de formatos adecuados para etiquetar los activos y elementos del Data Center, para que la localización de equipos o elementos sea rápida y precisa, facilitando al mismo tiempo la búsqueda para su mantenimiento o en caso de averías.	Estándar de Etiquetado de Activos de Información	Administrador Data Center / Técnico encargado	5 días
Mantener un sistema de acceso seguro a los equipos del Data Center.	Se elabora un documento donde se determine parámetros para establecer contraseñas.	Estándar de Creación de Contraseñas de Usuarios y Administradores de los Sistemas.	Administrador Data Center / Técnico encargado.	5 días

Garantizar que se pueda recuperar la infraestructura tecnológica que soporta los servicios del Data Center.	Se elabora un documento donde se detallen procesos a seguir para garantizar que, en caso de fallos se pueda recuperar la infraestructura o servicios.	Plan de Contingencia de TI	Administrador Data Center / Técnico encargado/ Custodios de Activos	1 mes

Conclusiones

- La norma ISO/IEC 27002 brinda listado de dominios, donde recomienda buenas prácticas de seguridad que pueden ser adaptadas al Data Center de la Facultad de Ingeniería y Ciencias Aplicadas, en base a esta norma se pudo realizar una entrevista la cual permitió valorar la situación actual del Data Center respecto a la seguridad de información; además en base a esta norma se redactan las políticas a considerar en este trabajo de titulación, las cuales ayuden a fortalecer y mejorar la seguridad de la información de cada activo.
- La metodología Magerit proporciona un proceso sistemático para el análisis y gestión de riesgo, lo cual fue de mucha ayuda al momento de desarrollar este proyecto, ya que este modelo sistematizado información que facilita el proceso del análisis y gestión de riesgos de la institución, pudiendo realizar este proyecto de una forma estructurada y clara, la cual facilita el entendimiento de este documento.
- La metodología Magerit sugiere el uso de la herramienta PILAR, siendo esta una herramienta de gran ayuda en el análisis y gestión de riesgos; dado el caso de existir cambios significativos en el Data Center y de ser necesario realizar una nueva evaluación de los riesgos, esta herramienta permite editar el archivo generado en previos análisis, pudiendo sacar nuevos resultados.
- Mediante el análisis del riesgo se pudo determinar los activos y las amenazas más importantes que se presentan en el Data Center, lo cual dio paso a la gestión de los mismos; pudiendo establecer el tratamiento que se le puede dar a cada riesgo y establecer controles que lo disminuyan.
- A lo largo del desarrollo de este proceso se pudo observar que no solo los activos como servidores son de gran importancia, sino también los elementos que componen o son parte de su conectividad, como los activos de hardware (equipos de red) y

activos auxiliares (cableado estructurado, sistema eléctrico, sistema de aire acondicionado, UPS, sistema de seguridad); los mismo que se tomaron en cuenta para poder brindar una seguridad robusta y estructurada.

- El Plan de Seguridad proporciona las pautas para implantar un SGSI, que en asuntos de seguridad es a donde se quiere llegar. Ya que brinda un proceso metódico, el cual permite tratar a los riesgos de una forma organizada, aumentando la posibilidad de controlarlos.
- Se plantea un Plan de Acción, el cual debe ser cumplido a cabalidad ya que este permitirá mejorar la seguridad al menos en un 40% aproximadamente, pero esto requiere del compromiso y colaboración de todo el personal relacionado con el Data Center.

Recomendaciones

- Ningún plan de seguridad va a garantizar el 100% de la seguridad de un sistema, pero se debe realizar el mayor esfuerzo con el cumplimiento de políticas y procedimientos establecidos para intentar lograr la mayor seguridad posible; y se necesita el compromiso y cooperación de los responsables del Data Center, para el cumplimiento de este plan.
- Se recomienda socializar las políticas y procedimientos a todos los usuarios y responsables de activos, ya que así podrán manejar la información de una manera más prolija, protegiendo en gran parte la información.
- PILAR es una herramienta que facilita el proceso de análisis y gestión de riesgos, en este proyecto se utilizó con licencia modo de evaluación, por tal razón tuvo algunos limitantes; se recomienda adquirir este software bajo un licencia comercial, lo cual facilitaría y agilitaría el proceso de evaluación de riesgos del sistema de información que maneja el Data Center, ya que este está expuesto a cambios constantes.
- El trabajo en equipo hace que las actividades y labores sean más fácil de realizar y en menor tiempo, pero cuando se trata de existencia de riesgos es necesario, asignar una persona que esté a cargo y sea responsable de la seguridad de la información y que la misma sea la encargada de hacer cumplir las políticas y procesos para resguardar la información.
- Es necesario actualizar las políticas en caso de que existan cambios significativos en el Data Center, así mismo es necesario designar periodos para la revisión del Plan de Seguridad y nombrar un responsable para este, para que le pueda dar seguimiento y cumplimiento al mismo. Se recomienda realizar las actualizaciones de las políticas al menos una vez al año.

- Es necesario fomentar una cultura de seguridad de la información a nivel de cada usuario del Data Center, considerando requerimientos básicos como usar contraseñas para acceso a equipos, para que este no pueda ser accedido por cualquier persona.
- Para que un Plan de Seguridad funcione es necesario tener el apoyo de las autoridades y usuarios que están relacionados con el Data Center; para de esta manera tener éxito tanto en la buena planificación y ejecución del plan.
- Como bien se mencionó el alcance de este trabajo de titulación está dirigido al cumplimiento de la primera Fase del Plan de Seguridad, pero se recomienda el pronto cumplimiento y desarrollo de las siguientes fases, ya que, el cumplimiento del mismo fortalecerá la seguridad de la información en el Data Center FICA.

Bibliografía

Amutio Gomez, M. A. (2012). MAGERIT-version 3.0 Metodología de analisis y gestión de riesgos de los sistemas de información Libro I-Metodo. En M. A. Amutio Gomez, *MAGERIT-version 3.0 Metodología de analisis y gestión de riesgos de los sistemas de información Libro I-Metodo* (pág. 175). Madrid: Ministerio de Hacienda y Administraciones Públicas.

CCN-STIC. (2016). *Guía de Seguridad.* Obtenido de http://www.dit.upm.es/~pepe/401/index.html#!1283

CERTSUPERIOR. (2016). *Seguridad en Redes*. Obtenido de https://www.certsuperior.com/SeguridadenRedes.aspx

Duque, B. (2010). *Metodologias de Gestión de Riesgos*. Obtenido de https://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+deGesti%C3%B2n+de+Riesgos.pdf

Ferrero Recasens, E. (2006). *Análsis y gestión de riesgos del servicio IMAT del sistema de información de I.C.A.I.* Universidad Pontificia Comillas, Madrid. Recuperado el 1 de Marzo de 2019, de https://docplayer.es/1625163-Analisis-y-gestion-de-riesgos-del-servicio-imat-del-sistema-de-informacion-de-i-c-a-i.html

Garcia, M. A. (2011). *Seguridad y Alta Disponibilidad*. Obtenido de https://mgarciafelipe.files.wordpress.com/2011/10/ud-1-adopcic3b3n-de-pautas-de-seguridad-informc3a1tica-miguelangelgarcia1.pdf

ISO 27000. (2017). *Sistema de Gestión de la Seguridad de la Información*. Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

ISO/IEC 27000. (2005). Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

Jiménez, J. (2017). *Conceptos en seguridad de los sistemas de información: confidencialidad, integridad, disponibilidad y trazabilidad*. Obtenido de https://oposcaib.wikispaces.com/file/view/38+-+Conceptes+en+seguretat+dels+sistemes+d%27informaci%C3%B3.+Confidencialitat%2C+integritat%2C+disponibilitat+i+tra%C3%A7abilitat.pdf

Martinez Garcis, R. (2012). Obtenido de https://docs.google.com/document/d/15TYUClkxF_WYA1kTqCJa6bwQaCLlaEkwAQ-8EvFO7js/edit?pli=1

Matalobos Veiga, J. (2012). *Analisis de Riesgo de la Seguridad de la Información.* Obtenido de http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

Ministerio de Administraciones Públicas de España. (2005). "MAGERIT Versión 2, Metodología de Análisis y Gestión de Riesgos de los sistemas de información". Obtenido de http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184

Ministerio de Hacienda y Administraciones. (Octubre de 2016). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Obtenido de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Narváez, C. (2016). Diseño de una Data Center TIER I basado en el estandar TIA942 para la Facultad de Ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte. *http://repositorio.utn.edu.ec/handle/123456789/5346.* Universidad Tecnica del Norte, Ibarra.

Palet, J. (14 de Marzo de 2011). *Desarrollo Web* . Obtenido de http://www.desarrolloweb.com/articulos/protocolo-ipv6-entrevista-jordi-palet.html

Perugachi, C. (2018). *Repositorios UTN.* Recuperado el Febrero de 2019, de http://repositorio.utn.edu.ec/browse?type=author&value=Perugachi+Espinosa%2C+Cristian+Alfonso

Tovar, C., & María, N. (2015). *Administración del Riesgo en Informática*. Obtenido de https://es.slideshare.net/carolinatovar7/admn-del-riesgo-en-informtica

UNE 71504:2008. (2008). *Metodología de análisis y gestión de riesgos para los sistemas de información.*

Whitman, M., & Mattord, H. (2011). *Principles of Information Security.* USA: Cengage Learning. Obtenido de https://books.google.es/books?hl=es&lr=&id=L3LtJAxcsmMC&oi=fnd&pg=PR9&d

q=Security+information+confidentiality&ots=6WC1NUjRoT&sig=NliBpW-eC0vZhhQUrqlhqjjJYdU#v=onepage&q=Security%20information%20confidentiality&f=false

WORDPRESS. (2016). *Seguridad de la Información*. Obtenido de https://seguridadinformatica648.wordpress.com/

Anexo 1: ISO/IEC 27002:2005. Dominios (11), Objetivos de control (39) y Controles (133)

5. POLÍTICA DE SEGURIDAD.

5.1 Política de seguridad de la información.

5.1.1 Documento de política de seguridad de la información.

5.1.2 Revisión de la política de seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

6.1 Organización interna.

6.1.1 Compromiso de la Dirección con la seguridad de la información.

6.1.2 Coordinación de la seguridad de la información.

6.1.3 Asignación de responsabilidades relativas a la seguridad de la información.

6.1.4 Proceso de autorización de recursos para el tratamiento de la información.

6.1.5 Acuerdos de confidencialidad.

6.1.6 Contacto con las autoridades.

6.1.7 Contacto con grupos de especial interés.

6.1.8 Revisión independiente de la seguridad de la información.

6.2 Terceros.

6.2.1 Identificación de los riesgos derivados del acceso de terceros.

6.2.2 Tratamiento de la seguridad en la relación con los clientes.

6.2.3 Tratamiento de la seguridad en contratos con terceros.

7. GESTIÓN DE ACTIVOS.

7.1 Responsabilidad sobre los activos.

7.1.1 Inventario de activos.

7.1.2 Propiedad de los activos.

7.1.3 Uso aceptable de los activos.

7.2 Clasificación de la información.

7.2.1 Directrices de clasificación.

7.2.2 Etiquetado y manipulado de la información.

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

8.1 Antes del empleo.

8.1.1 Funciones y responsabilidades.

8.1.2 Investigación de antecedentes.

8.1.3 Términos y condiciones de contratación.

8.2 Durante el empleo.

8.2.1 Responsabilidades de la Dirección.

8.2.2 Concienciación, formación y capacitación en seguridad de la información.

8.2.3 Proceso disciplinario.

8.3 Cese del empleo o cambio de puesto de trabajo.

8.3.1 Responsabilidad del cese o cambio.

8.3.2 Devolución de activos.

8.3.3 Retirada de los derechos de acceso.

9. SEGURIDAD FÍSICA Y DEL ENTORNO.

9.1 Áreas seguras.

9.1.1 Perímetro de seguridad física.

9.1.2 Controles físicos de entrada.

9.1.3 Seguridad de oficinas, despachos e instalaciones.

9.1.4 Protección contra las amenazas externas y de origen ambiental.

9.1.5 Trabajo en áreas seguras.

9.1.6 Áreas de acceso público y de carga y descarga.

9.2 Seguridad de los equipos.

9.2.1 Emplazamiento y protección de equipos.

9.2.2 Instalaciones de suministro.

9.2.3 Seguridad del cableado.

9.2.4 Mantenimiento de los equipos.

9.2.5 Seguridad de los equipos fuera de las instalaciones.

9.2.6 Reutilización o retirada segura de equipos.

9.2.7 Retirada de materiales propiedad de la empresa.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.

10.1 Responsabilidades y procedimientos de operación.

10.1.2 Gestión de cambios.

10.1.3 Segregación de tareas.

10.1.4 Separación de los recursos de desarrollo, prueba y operación.

10.2 Gestión de la provisión de servicios por terceros.

10.2.1 Provisión de servicios.

10.2.2 Supervisión y revisión de los servicios prestados por terceros.

10.2.3 Gestión del cambio en los servicios prestados por terceros.

10.3 Planificación y aceptación del sistema.

10.3.1 Gestión de capacidades.

10.3.2 Aceptación del sistema.

10.4 Protección contra el código malicioso y descargable.

10.4.1 Controles contra el código malicioso.

10.4.2 Controles contra el código descargado en el cliente.

10.5 Copias de seguridad.

10.5.1 Copias de seguridad de la información.

10.6 Gestión de la seguridad de las redes.

10.6.1 Controles de red.

10.6.2 Seguridad de los servicios de red.

10.7 Manipulación de los soportes.

10.7.1 Gestión de soportes extraíbles.

10.7.2 Retirada de soportes.

10.7.3 Procedimientos de manipulación de la información.

10.7.4 Seguridad de la documentación del sistema.

10.8 Intercambio de información.

10.8.1 Políticas y procedimientos de intercambio de información.

10.8.2 Acuerdos de intercambio.

10.8.3 Soportes físicos en tránsito.

10.8.4 Mensajería electrónica.

10.8.5 Sistemas de información empresariales.

10.9 Servicios de comercio electrónico.

10.9.1 Comercio electrónico.

10.9.2 Transacciones en línea.

10.9.3 Información públicamente disponible.

10.10 Supervisión.

10.10.1 Registros de auditoría.

10.10.2 Supervisión del uso del sistema.

10.10.3 Protección de la información de los registros.

10.10.4 Registros de administración y operación.

10.10.5 Registro de fallos.

10.10.6 Sincronización del reloj.

11. CONTROL DE ACCESO.

11.1 Requisitos de negocio para el control de acceso.

11.1.1 Política de control de acceso.

11.2 Gestión de acceso de usuario.

11.2.1 Registro de usuario.

11.2.2 Gestión de privilegios.

11.2.3 Gestión de contraseñas de usuario.

11.2.4 Revisión de los derechos de acceso de usuario.

11.3 Responsabilidades de usuario.

11.3.1 Uso de contraseñas.

11.3.2 Equipo de usuario desatendido.

11.3.3 Política de puesto de trabajo despejado y pantalla limpia.

11.4 Control de acceso a la red.

11.4.1 Política de uso de los servicios en red.

11.4.2 Autenticación de usuario para conexiones externas.

11.4.3 Identificación de los equipos en las redes.

11.4.4 Protección de los puertos de diagnóstico y configuración remotos.

11.4.5 Segregación de las redes.

11.4.6 Control de la conexión a la red.

11.4.7 Control de encaminamiento (routing) de red.

11.5 Control de acceso al sistema operativo.

11.5.1 Procedimientos seguros de inicio de sesión.

11.5.2 Identificación y autenticación de usuario.

11.5.3 Sistema de gestión de contraseñas.

11.5.4 Uso de los recursos del sistema.

11.5.5 Desconexión automática de sesión.

11.5.6 Limitación del tiempo de conexión.

11.6 Control de acceso a las aplicaciones y a la información.

11.6.1 Restricción del acceso a la información.

11.6.2 Aislamiento de sistemas sensibles.

11.7 Ordenadores portátiles y teletrabajo.

11.7.1 Ordenadores portátiles y comunicaciones móviles.

11.7.2 Teletrabajo.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.

12.1 Requisitos de seguridad de los sistemas de información.

12.1.1 Análisis y especificación de los requisitos de seguridad.

12.2 Tratamiento correcto de las aplicaciones.

12.2.1 Validación de los datos de entrada.

12.2.2 Control del procesamiento interno.

12.2.3 Integridad de los mensajes.

12.2.4 Validación de los datos de salida.

12.3 Controles criptográficos.

12.3.1 Política de uso de los controles criptográficos.

12.3.2 Gestión de claves.

12.4 Seguridad de los archivos de sistema.

12.4.1 Control del software en explotación.

12.4.2 Protección de los datos de prueba del sistema.

12.4.3 Control de acceso al código fuente de los programas.

12.5 Seguridad en los procesos de desarrollo y soporte.

12.5.1 Procedimientos de control de cambios.

12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.

12.5.3 Restricciones a los cambios en los paquetes de software.

12.5.4 Fugas de información.

12.5.5 Externalización del desarrollo de software.

12.6 Gestión de la vulnerabilidad técnica.

12.6.1 Control de las vulnerabilidades técnicas.

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

13.1 Notificación de eventos y puntos débiles de seguridad de la información.

13.1.1 Notificación de los eventos de seguridad de la información.

13.1.2 Notificación de puntos débiles de seguridad.

13.2 Gestión de incidentes y mejoras de seguridad de la información.

13.2.1 Responsabilidades y procedimientos.

13.2.2 Aprendizaje de los incidentes de seguridad de la información.

13.2.3 Recopilación de evidencias.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.

14.1.2 Continuidad del negocio y evaluación de riesgos.

14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.

14.1.4 Marco de referencia para la planificación de la cont. del negocio.

14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.

15. CUMPLIMIENTO.

15.1 Cumplimiento de los requisitos legales.

15.1.1 Identificación de la legislación aplicable.

15.1.2 Derechos de propiedad intelectual (DPI).

15.1.3 Protección de los documentos de la organización.

15.1.4 Protección de datos y privacidad de la información de carácter personal.

15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.

15.1.6 Regulación de los controles criptográficos.

15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.

15.2.1 Cumplimiento de las políticas y normas de seguridad.

15.2.2 Comprobación del cumplimiento técnico.

15.3 Consideraciones sobre las auditorías de los sistemas de información.

15.3.1 Controles de auditoría de los sistemas de información.

15.3.2 Protección de las herramientas de auditoría de los sistemas de información.

Anexo 2: Entrevista

UNIVERSIDAD TECNICA DEL NORTE

PROYECTO DE TESIS

PLAN DE SEGURIDAD PARA LA GESTIÓN DE RIESGOS EN EL DATACENTER DE LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS CON LA METODOLOGÍA MAGERIT V3.0

Objetivo: Esta entrevista va dirigida a las personas encargadas y responsables del Data Center de la Facultad, con la finalidad de obtener información sobre el manejo de la seguridad dentro del mismo y además de identificar la información que se maneja en cada uno de los activos más importantes para la institución.

Nombre y Apellido: Ing. Santiago Meneses

Cargo que desempeña: Técnico/Docente encargado Data Center

INDICADORES/PREGUNTAS	SI	NO	DESCONOCE	COMENTARIO
POLITICAS DE SEGURIDAD				
1. ¿Conoce o sabe Ud. de la existencia de políticas de seguridad de la información?			x	
2. Si existen políticas ¿conoce si son de conocimiento de todo el personal?		x		
3. Si existen políticas ¿se aplican estas políticas?		x		
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN				
4. ¿Hay un compromiso de las autoridades con respecto a la seguridad de la información?		x		
5. ¿Se tiene bien definida las personas responsables relativas a la seguridad de la información?		x		

GESTIÓN DE ACTIVOS.					
6.	¿Se cuenta con un inventario de activos debidamente documentado y actualizado?		x		
7.	¿Se cuenta con procedimientos para la manipulación de los activos?		x		
8.	¿El etiquetado en el Data Center existente es el apropiado?		x		
9.	¿Qué activos dentro del Data Center considera Ud. de vital importancia o críticos?				Todos los servidores de vital importancia son el radius, el de la revista universitaria; ya que son los que definen el propósito del Data Center. Además cabe recalcar que los equipos de red como switch y router son tan importantes como los servidores, ya que sin su correcto funcionamiento, hay falencias en toda la red.
10.	¿Se tienen debidamente clasificada la información?		x		
SEGURIDAD LIGADA A LOS RECURSOS HUMANOS					
11.	¿Si existe un nuevo responsable de un determinado activo, es informado debidamente de sus responsabilidades?	x			
12.	¿Se toma medidas de seguridad cuando existe cambio de encargados de determinado activo?	x			Se cambia credenciales para el acceso.
SEGURIDAD FÍSICA Y DEL ENTORNO					
13.	¿Existe control físico de entrada al Data Center?	x			Se tiene control de acceso biométrico
14.	Existe sistemas que alerten amenazas como fuego, calor extremo, humedad, etc?		x		

15.	¿Se realiza mantenimiento de los equipos?		x		
16.	¿El cableado estructurado está en buenas condiciones?	x			
GESTIÓN DE COMUNICACIONES Y OPERACIONES					
17.	¿Se documenta los procedimientos operativos que realizan los usuarios dentro del Data Center?		x		
18.	¿Se documentan los cambios que se realizan en los diferentes activos?		x		
19.	¿Existen copias de seguridad de la información?	x			
20.	¿Se cuenta con controles contra software malicioso?		x		
CONTROL DE ACCESO.					
21.	¿Se realiza procedimientos para dar acceso al Data Center?		x		
22.	¿Para el acceso remoto se tienen establecidos mecanismos de autenticación de usuario a la red interna del Data Center?	x			
23.	¿Se cuenta con una política o procedimiento con respecto al uso, protección y ciclo de vida de las claves criptográficas?		x		
GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN					
24.	¿El Data Center cuenta con un procedimiento formal para reportes de incidentes?		x		
25.	¿Cuenta con alguna herramienta que reporte y registro de incidente?		x		
26.	¿Al tener algún reporte de incidente de seguridad, se cuenta con un plan de respuesta?		x		
GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO					
27.	¿El Data Center cuenta con planes de continuidad de las operaciones?		x		
28.	¿Se realiza pruebas, mantenimiento y evaluación constante de los planes de		x		

continuidad de las operaciones?				
CUMPLIMIENTO				
29. ¿Se cuenta con controles del cumplimiento de las políticas de seguridad de la información?		x		

Ing. Santiago Meneses
Firma Responsable

¡GRACIAS POR SU TIEMPO BRINDADO!

Resultados Entrevista

En base a la entrevista realizada se puede concluir como se muestra en la figura que en relación a la seguridad de información, en un 76% se desconoce la existencia de políticas y procedimientos, en un 21% existe la certeza que se manejan o aplican ciertos controles y en un 3% no existen o no se aplican. Por tal razón se puede aseverar lo siguiente:

Figura 1 Resultados entrevista

- Con respecto al indicador *políticas de seguridad* se puede decir, que a pesar de la existencia de políticas de seguridad como se menciona en el apartado 3.3; él encargado asegura no conocerlas, por ende, jamás han sido aplicadas y mucho menos actualizadas.
- En relación a los *aspectos organizativos de la seguridad de la información*, se puede decir que no se cuenta con personal encargado exclusivamente de la seguridad de la información y se asevera que las autoridades no han establecido compromiso con respecto a este tema.
- En el indicador *gestión de activos*, se exterioriza que no existe un inventario de activos debidamente documentado. De igual manera se puede decir, que no existe un etiquetado apropiado, ni se establecen procedimientos para su apropiada manipulación. Además, se puede acotar que como activos importantes se considera a los servidores Radius y Revista Universitaria, que son los activos que funcionan a razón de los objetivos de la facultad. También se puede decir que tienen vital

importancia los equipos de red como los switches y router, ya que del correcto funcionamiento de estos, dependerá el correcto funcionamiento del resto de equipos o activos.

- Con respecto a la *seguridad ligada a los recursos humanos*, se puede decir que se toman las medidas necesarias para dar un grado de seguridad a la información. Dado el caso que exista nuevo responsable de determinado activo, se informa de las responsabilidades que tienen ante mencionado activo y se realiza el cambio de credenciales para el respectivo acceso.
- En la *seguridad física y del entorno*, se puede decir que existe un control adecuado, ya que cuenta con un sistema de control de acceso biométrico para el Data Center. Además, se puede acotar con respecto a este indicador, que existe un cableado estructurado en buen estado, aunque no se realiza mantenimientos a los equipos y adicional no se cuentan con sistemas que alertan frente amenazas externas.
- En relación a la *gestión de comunicaciones y operaciones*, se puede decir que no se documentan los cambios, procedimientos que realizan en los activos o dentro del Data Center.
- Con respecto al *control de acceso*, no se realizan procedimientos donde se documente los permisos para el ingreso al Data Center, además se puede decir que para acceso remoto se cuenta con mecanismos de autenticación, sin ningún procedimiento o política referente.
- En el dominio de *gestión de incidentes en la seguridad de la información*, no existen procedimientos, herramientas ni personal a cargo de este tema.
- En relación a la *gestión de la continuidad del negocio*, no existen planes de continuidad.
- No existe *cumplimiento* de políticas de seguridad de la información.

Anexo 3: Manual de Instalación PILAR

Entorno Windows

La herramienta de Análisis y Gestión de Riesgo se la puede instalar mediante modo Administrador o modo Usuarios.

Pilar en entorno Windows, el primer paso para la instalación en dirigirse a un navegador y buscar la página principal de la herramienta donde se puede ver las diferentes versiones que existen. Pilar descargas: https://www.ar-tools.com/

Veremos en la parte izquierda las siguientes versiones los cuales sirven:

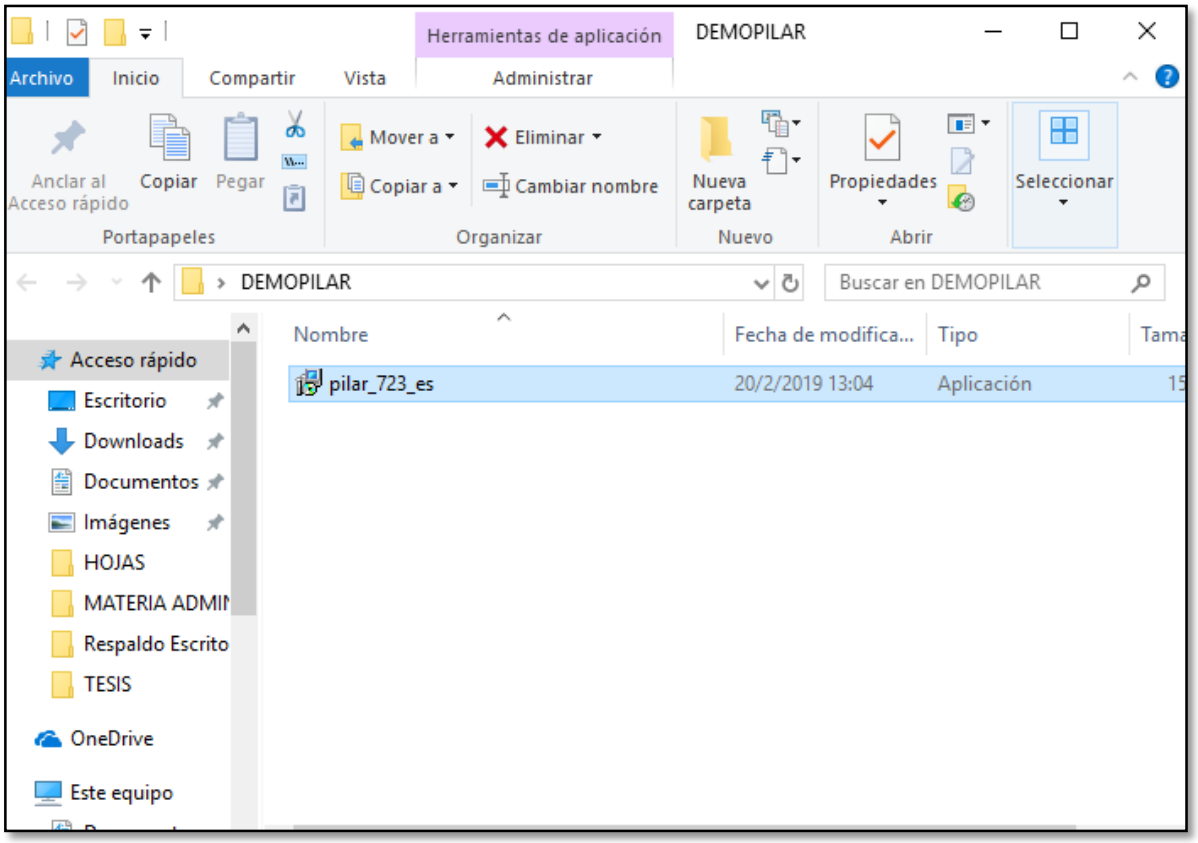
PILAR: versión íntegra de la herramienta.

PILAR Basic: versión sencilla para Pymes y Administración Local.

μPILAR: versión de PILAR reducida, destinada a la realización de análisis de riesgos muy rápidos.

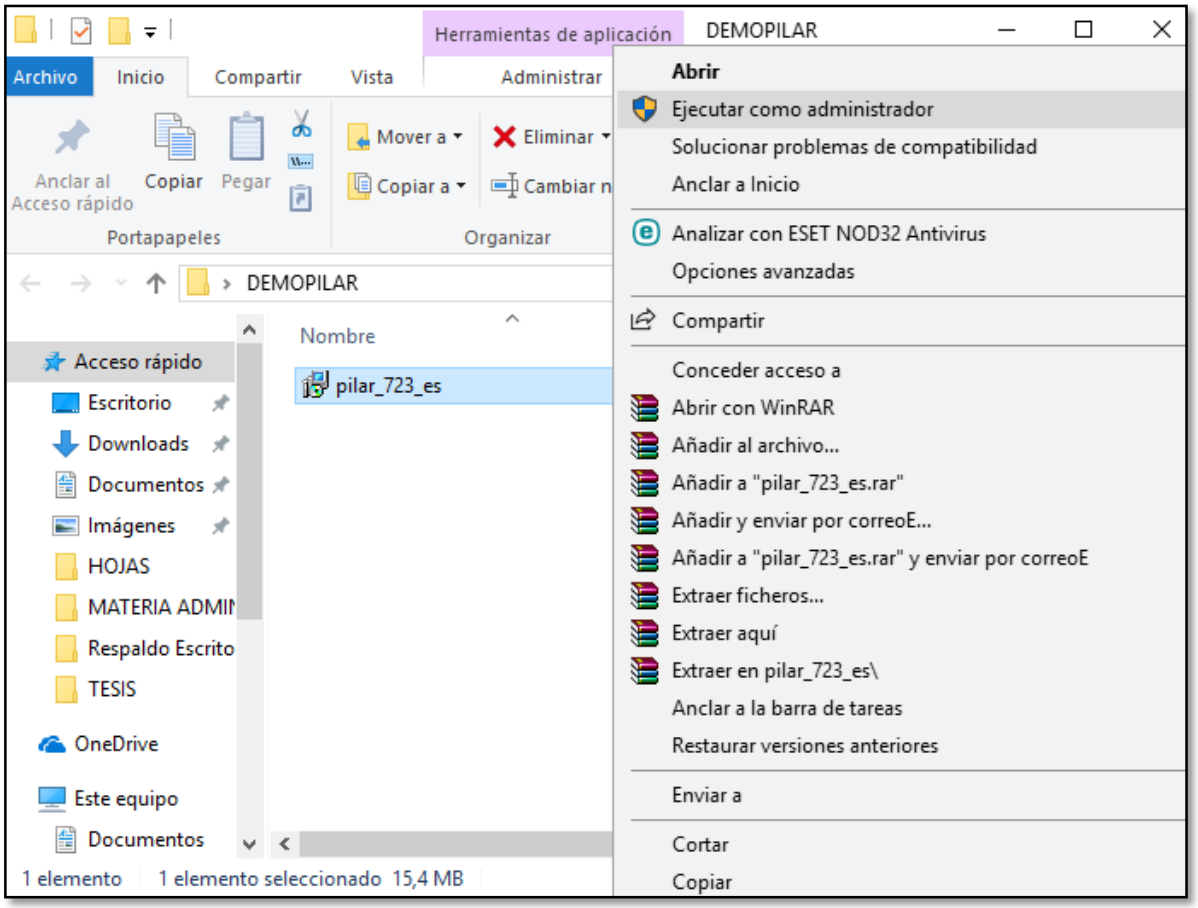
RMAT (Risk Management Additional Tools) Personalización de herramientas.

Para el manual la instalación se usó la versión Básica.



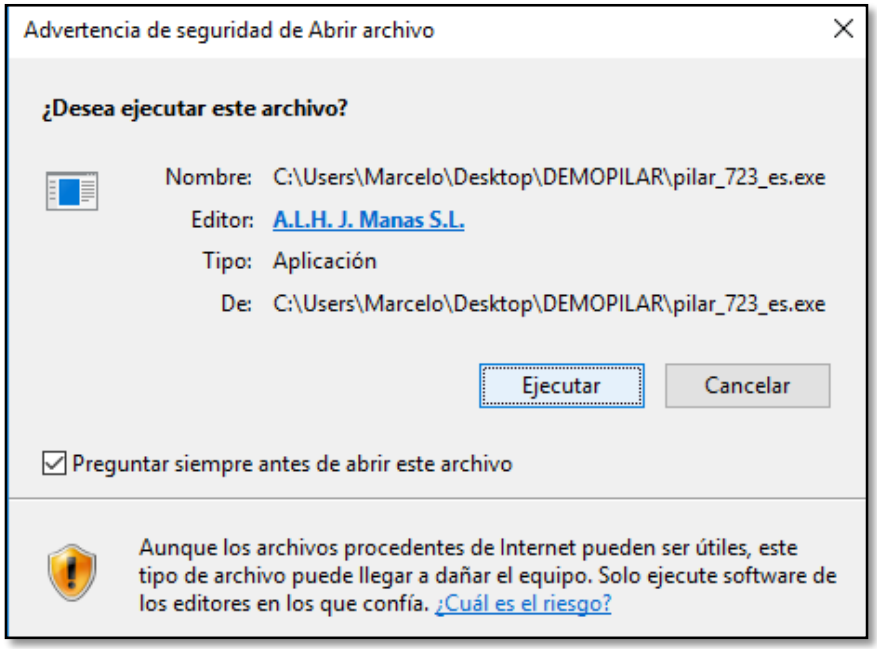
Instalación

Una vez descargada la versión que se quiere instalar, se la selecciona y mediante click derecho seleccionamos la opción **Ejecutar como Administrador**.



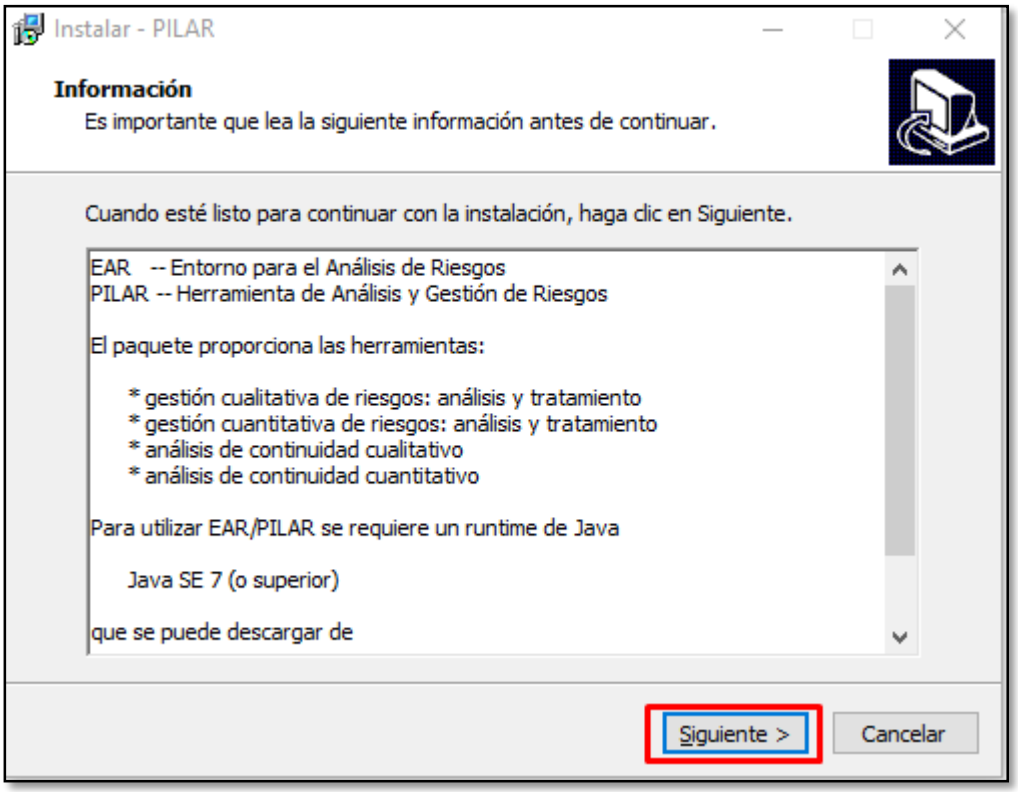
Ejecución

No indica el inicio de ejecución del archivo y hacemos clic en **Ejecutar.**



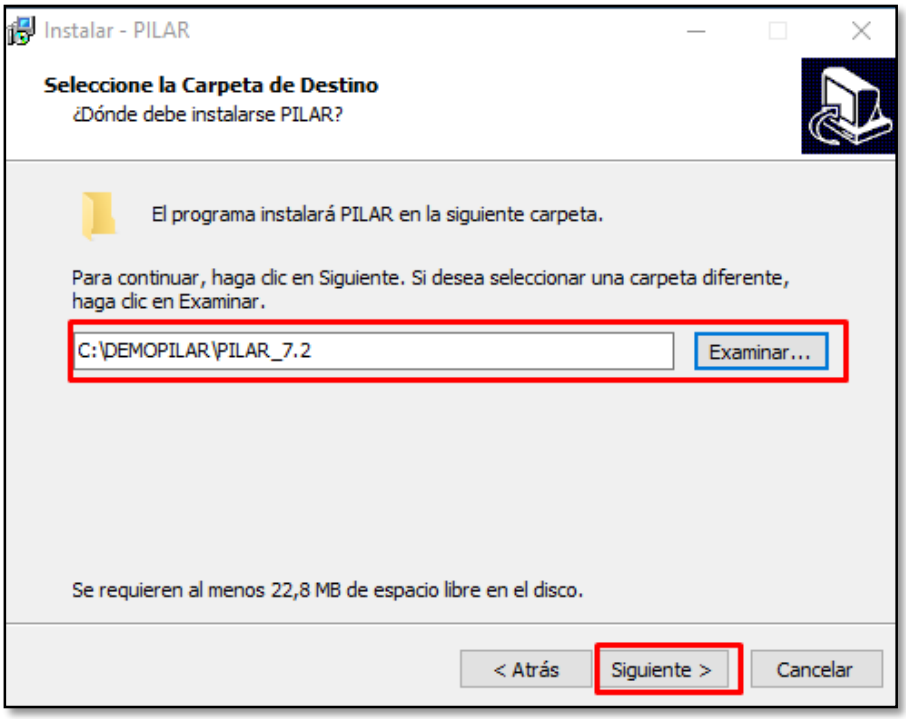
Información

Indica antes de su instalación los paquetes que presta la herramienta, para la utilización de la herramienta se requiere tener corriendo Java, el cual habitualmente ya se tiene instalado en el sistema, lo cual se hace clic izquierdo en **Siguiente.**



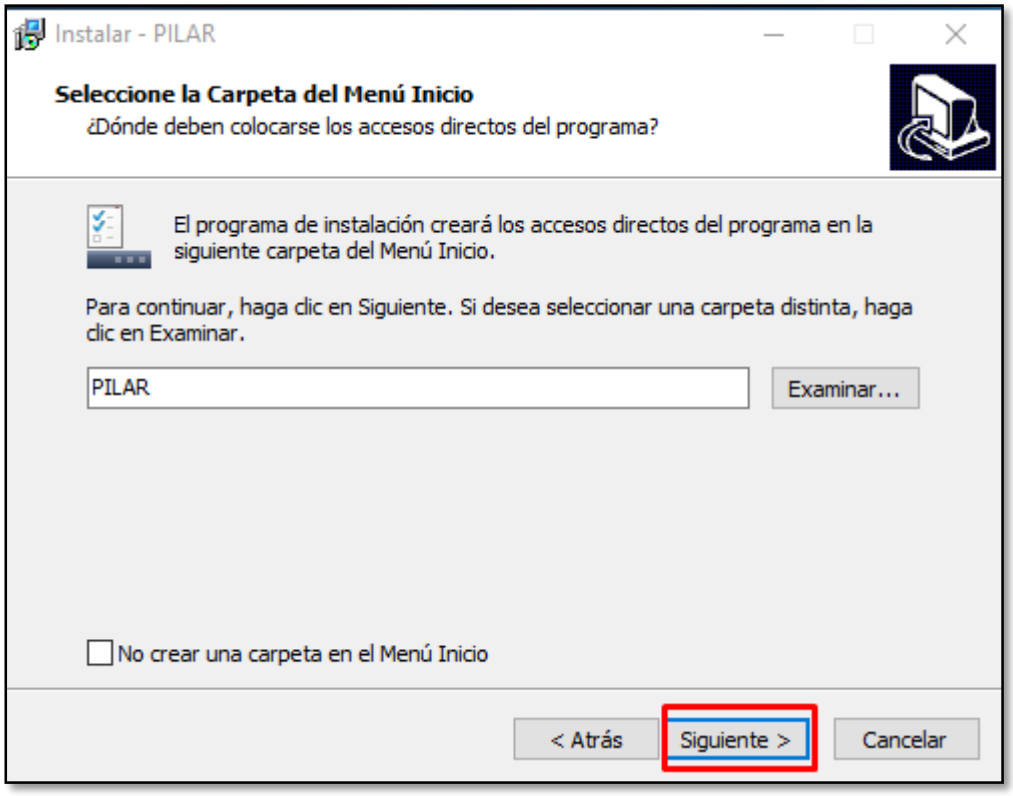
Carpeta Destino

Luego nos informa del lugar donde se instalar Pilar, el espacio mínimo de memoria para hacerlo. Realizamos clic izquierdo en **Siguiente** o seleccionamos la carpeta o dirección donde se requiera.



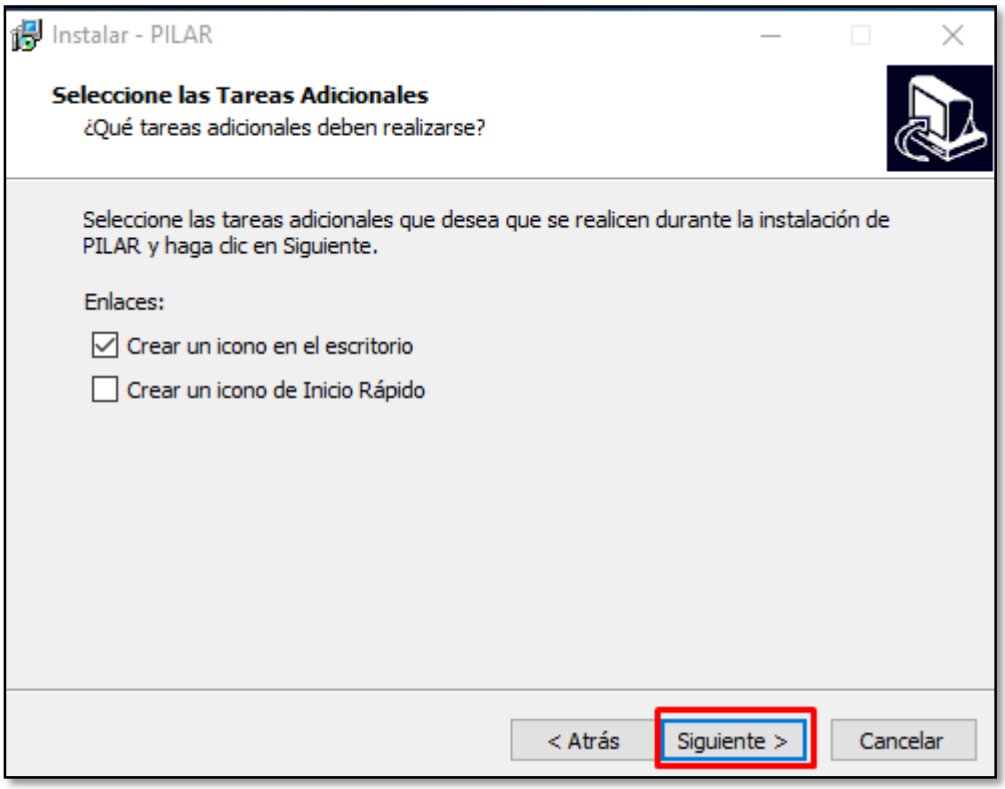
Menú

Luego informa sobre la creación de accesos directos, realizamos clic izquierdo en el botón **Siguiente.**



Tareas Adicionales

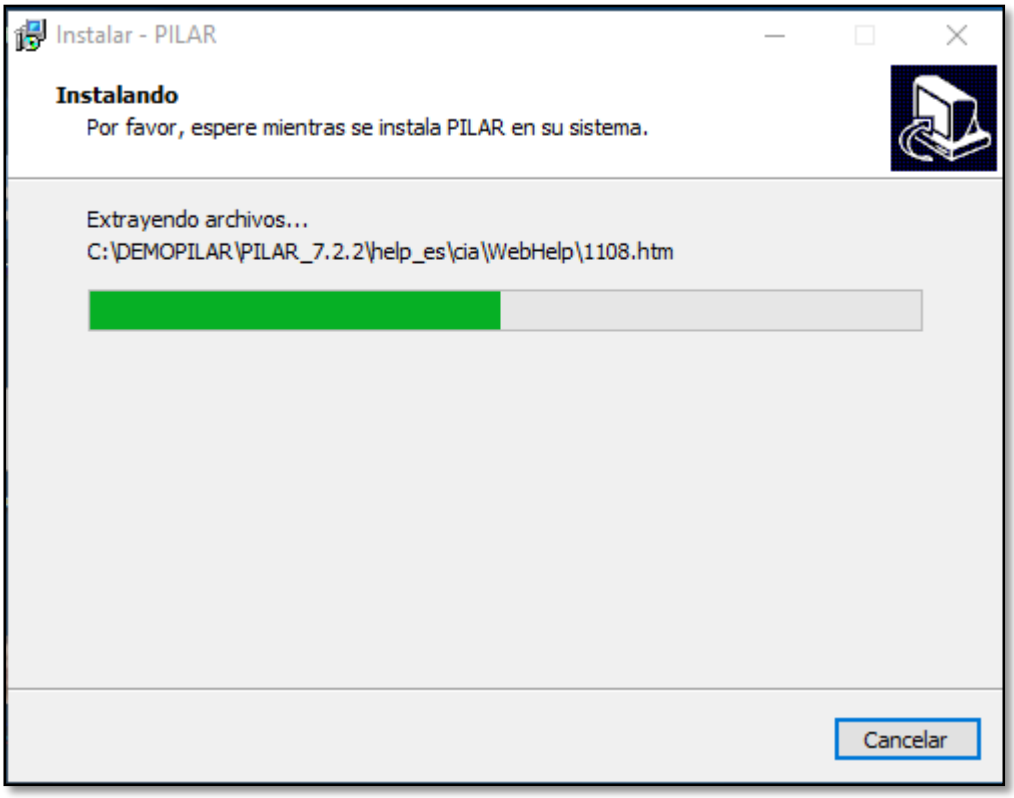
Indica las tareas adicionales que realizan durante la instalación de Pilar, la cual es crear iconos en el escritorio o de inicio rápido. Realizamos clic izquierdo en **Siguiente.**



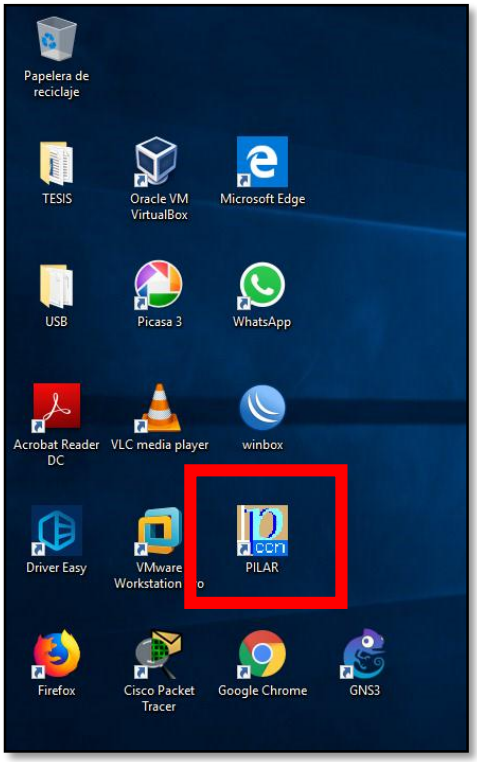
Instalar

Una vez terminado de realizar los pasos anteriores, la herramienta nos indica la carpeta destino, carpeta menú inicio y tareas adicionales. Realizamos clic izquierdo en **Instalar.**

Esperamos mientras se instala la herramienta PILAR.



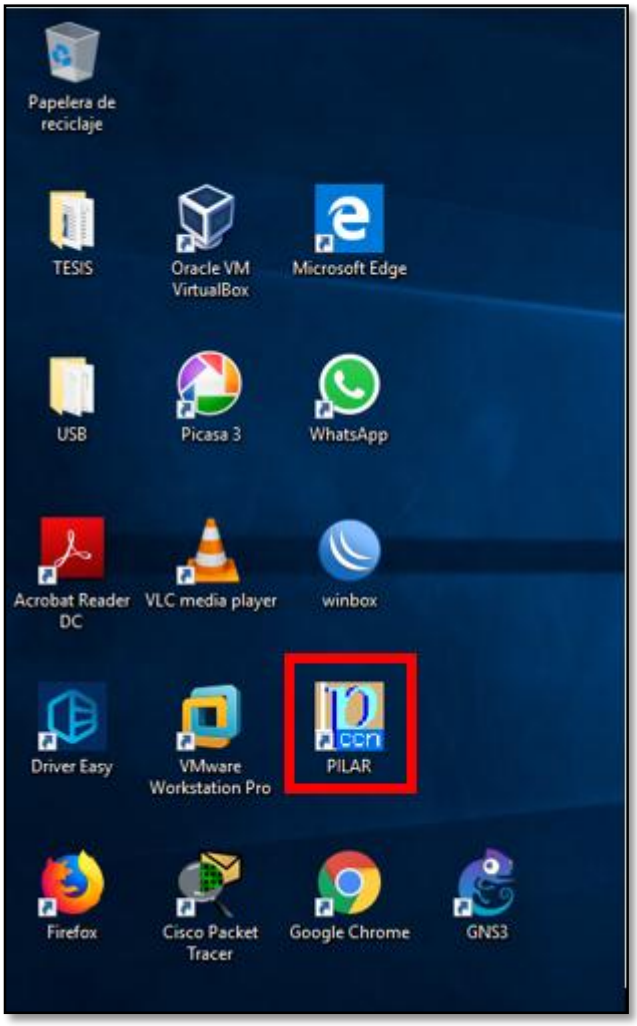
Una vez finalizada la estación de la herramienta de Análisis y Gestión de Riesgo PILAR, aparece el icono en el escritorio de la PC y está lista para su uso.



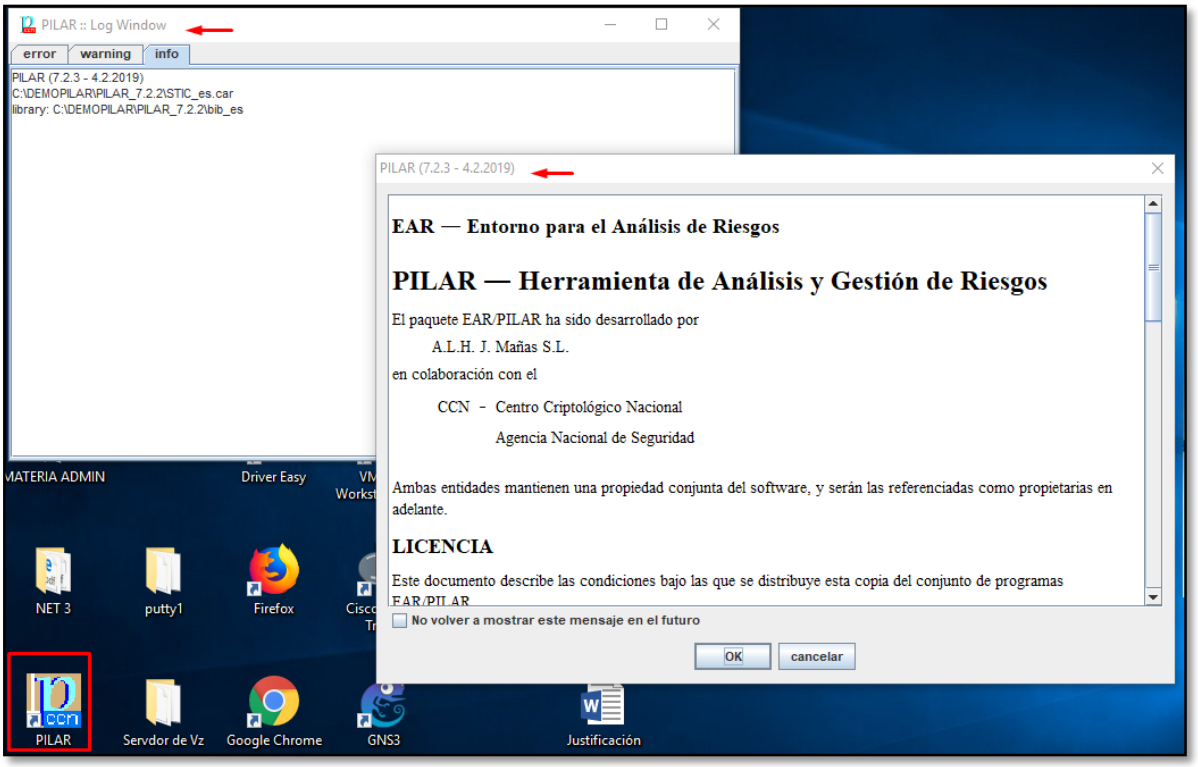
Anexo 4: Manual de Uso de PILAR

1.1. Configuración

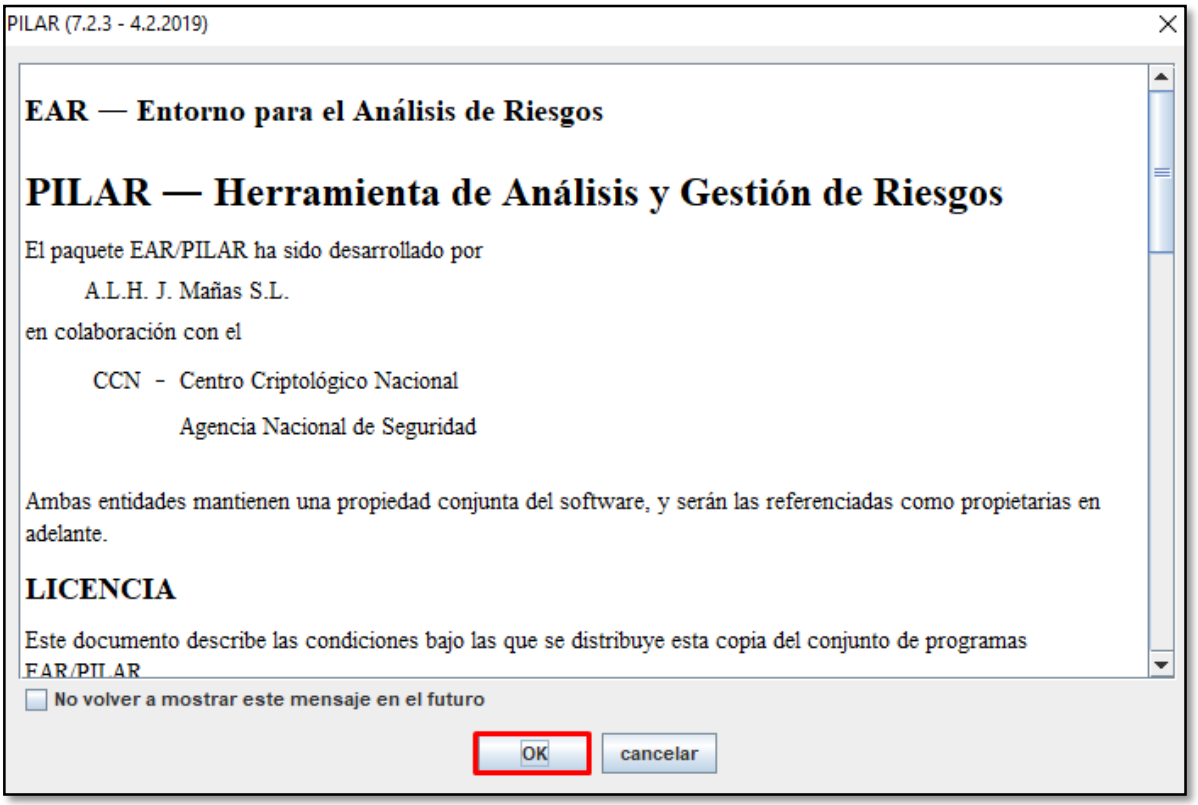
Una vez terminada la instalación se dirige al icono de **PILAR** y hacemos **doble clic** para iniciar la herramienta.



Inicialmente nos aparece dos pantallas de la herramienta, la pantalla de la parte izquierda nos indica que PILAR esta en funcionamiento y las librerías que se usan, y la pantalla derecha donde se configura y se realiza el desarrollo de la administración.

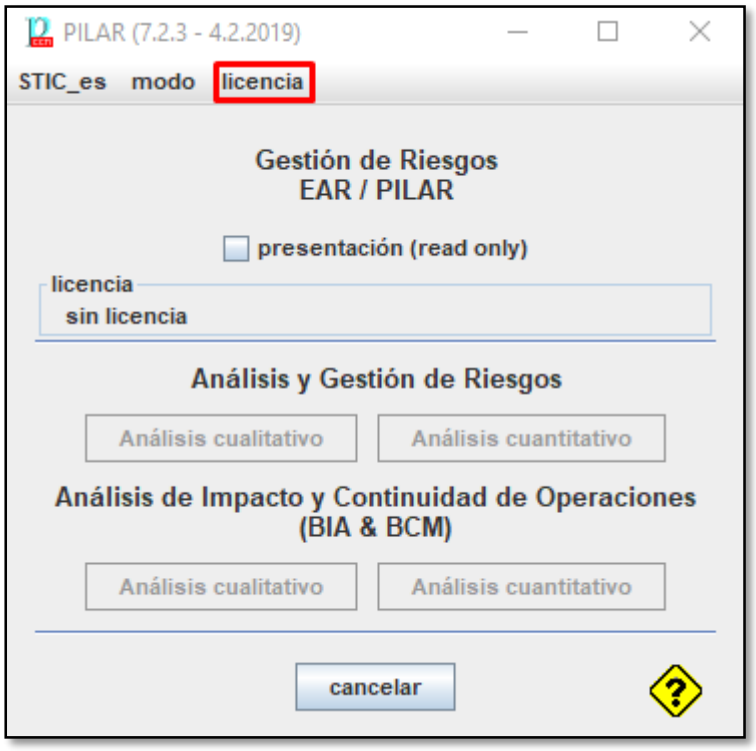


PILAR necesita de cierta configuración para su uso, en la imagen daremos clic izquierdo en **OK** para iniciar.

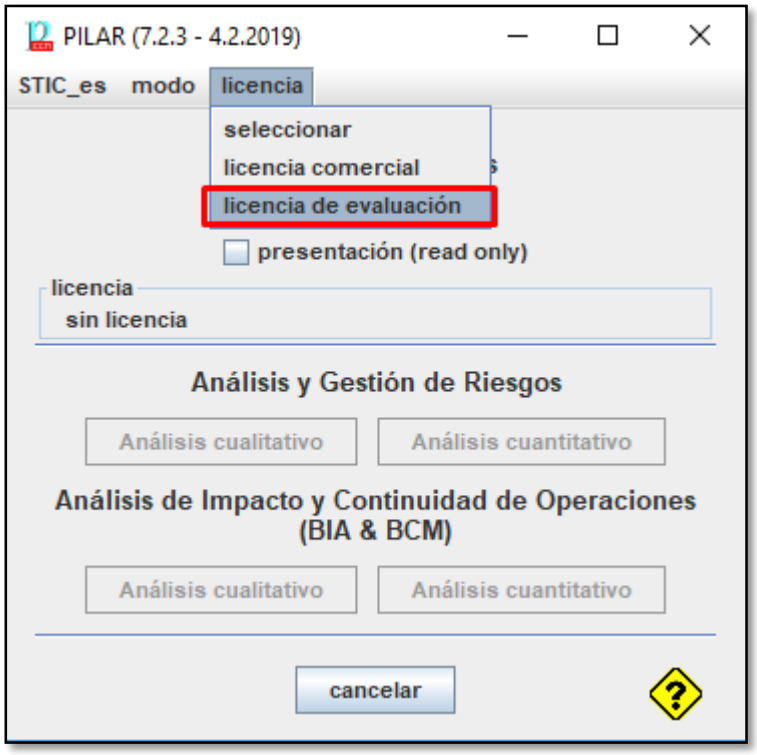


Aparece la pantalla principal, en la cual solicita una licencia para continuar la configuración, en este caso vamos a configurar una licencia de evaluación la cual nos permite usar esta herramienta un determinado tiempo. Nos vamos a la pestaña **licencia** y damos clic.

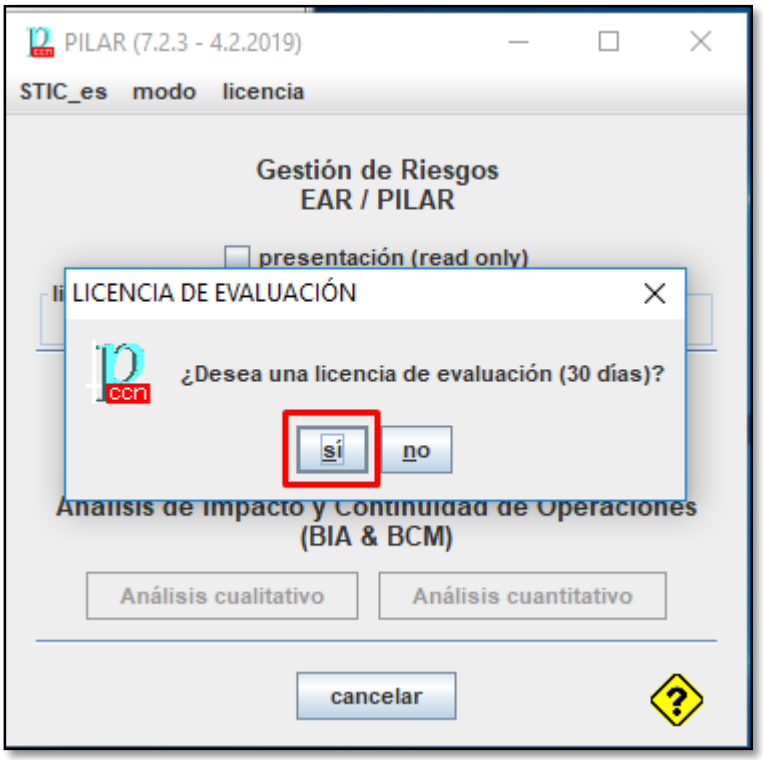
1.2. Licencia



Al momento de realizar clic nos parece los tipos de licencias que se puede usar, seleccionamos la **licencia de evaluación**.



Una vez seleccionada la licencia de evaluación, pulsamos en **SI** para tener un tiempo de prueba de la herramienta.

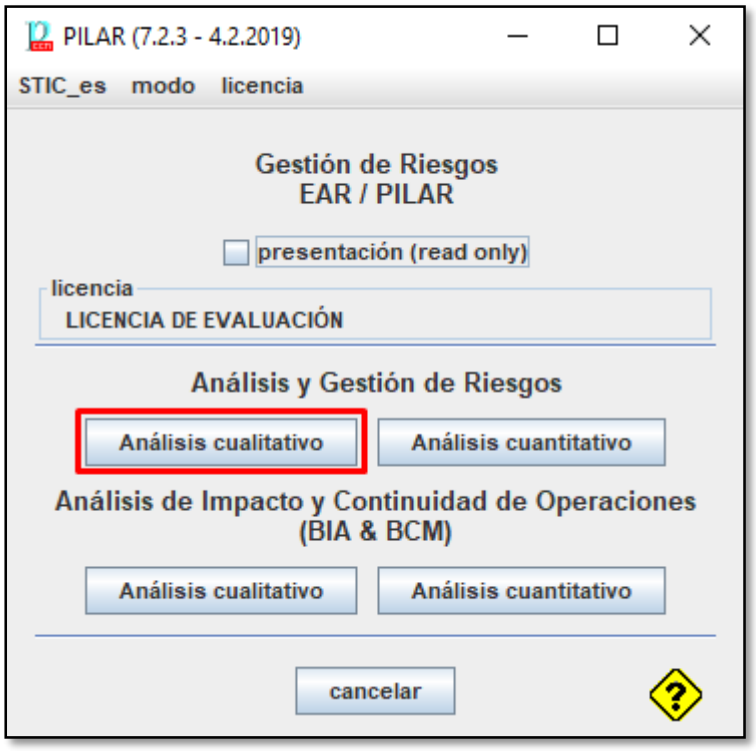


1.3. Seleccione el tipo de análisis

- ✓ Riesgo: analiza confidencialidad, integridad, disponibilidad.
- ✓ BCM: analiza continuidad del negocio interrupciones del servicio
- ✓ Cualitativo: usa una escala de valores relativos
- ✓ Cuantitativo: usa valores numéricos

Autorizada la licencia, nos dirigimos al análisis cualitativo de riesgo, que es la función más habitual.

1.4. Análisis Cualitativo

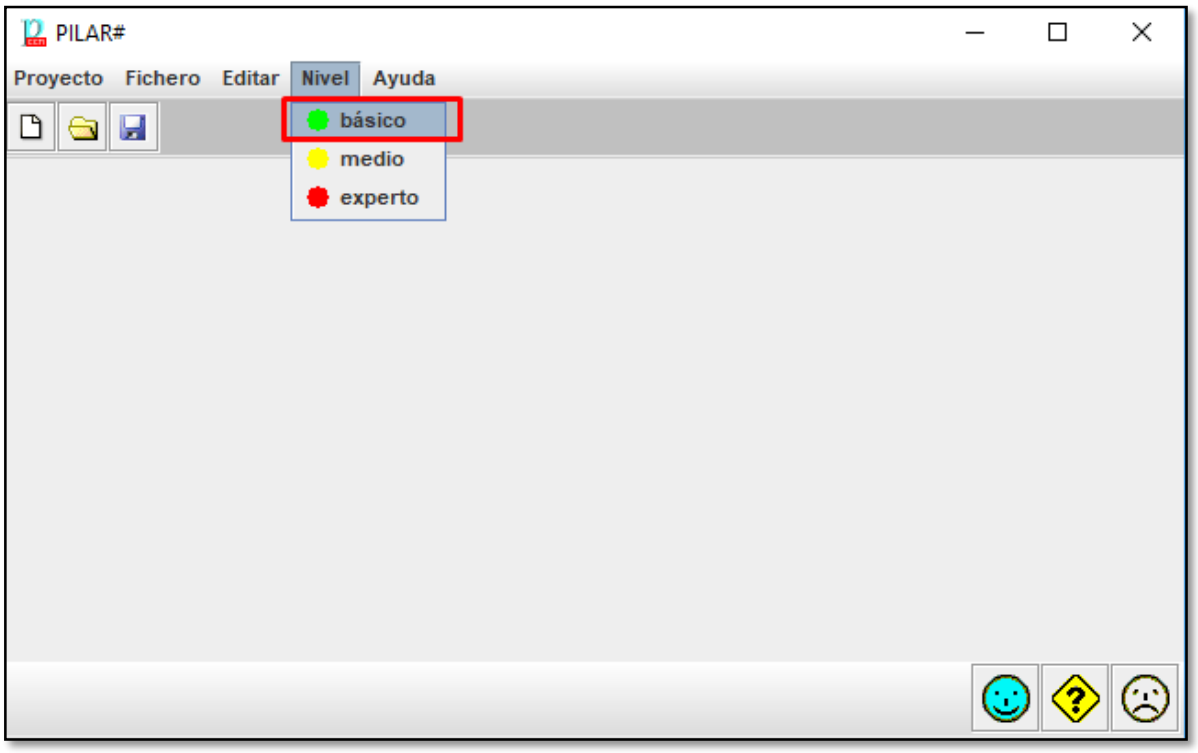


Una vez que se ingresa al análisis cualitativo, en la pestaña NIVEL aparece tres niveles de uso, los cuales son: **Básico, Medio y Experto**.

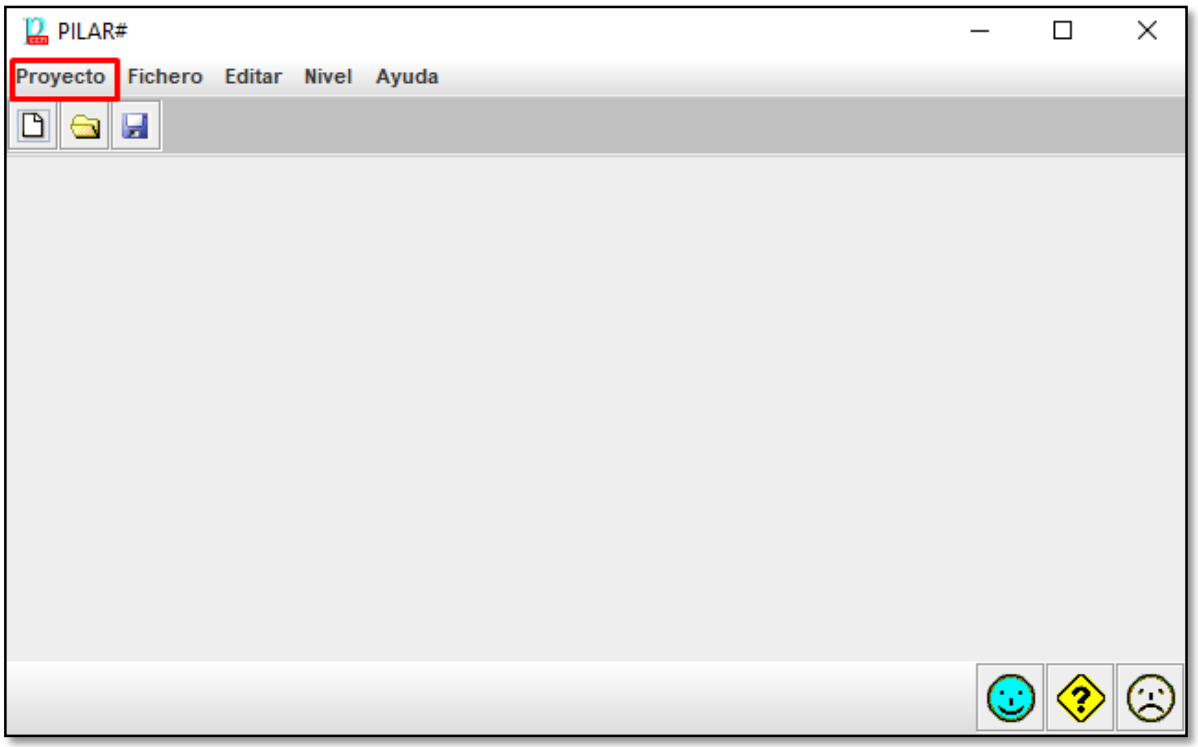
El manual especifica los tres modos de uso de la herramienta, seleccionamos el modo **Básico**.

1.5. Crear Activos

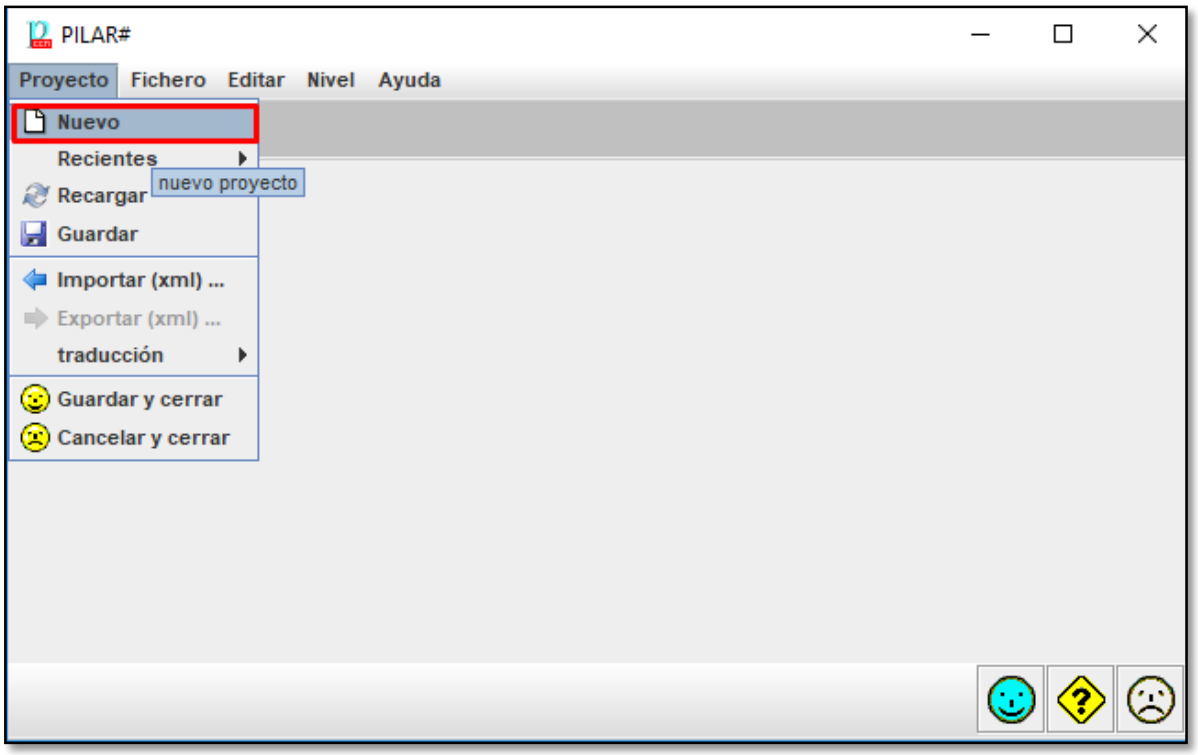
Los Activos de PILAR son Hardware, Software de comunicación.



En la pantalla de modo Básico, en la pestaña Proyecto pulsamos clic.



La cual aparece algunos ítems a seleccionar, como no se tiene ningún proyecto creado seleccionamos **Nuevo.**



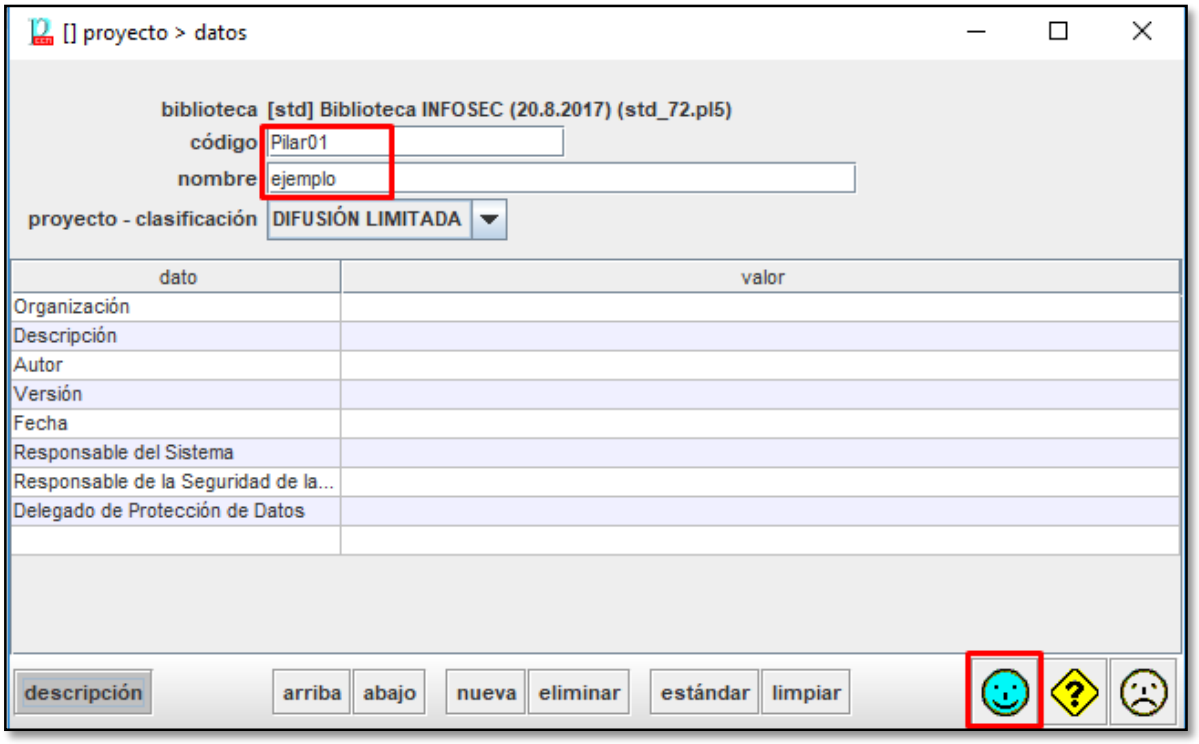
1.6. Activos

Para crear un proyecto nuevo debemos llenar las siguientes casillas:

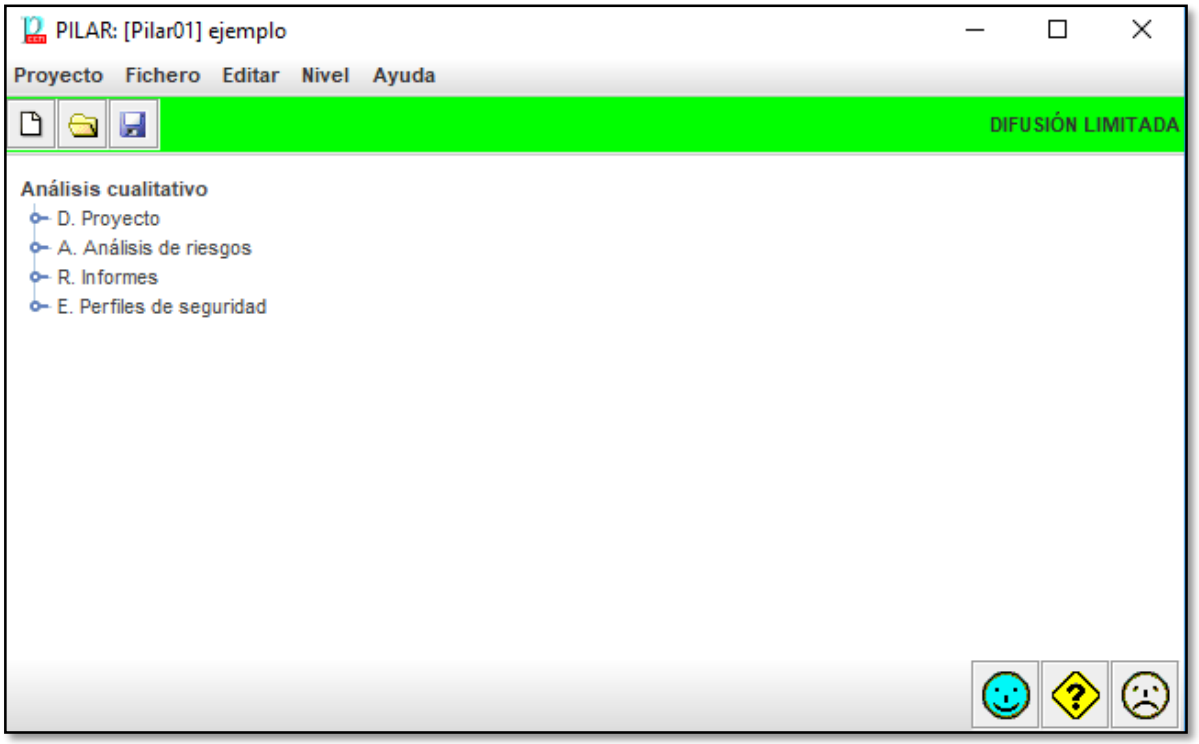
Código: Ingresamos un código cualquiera

Nombre: Ingresamos un nombre cualquiera

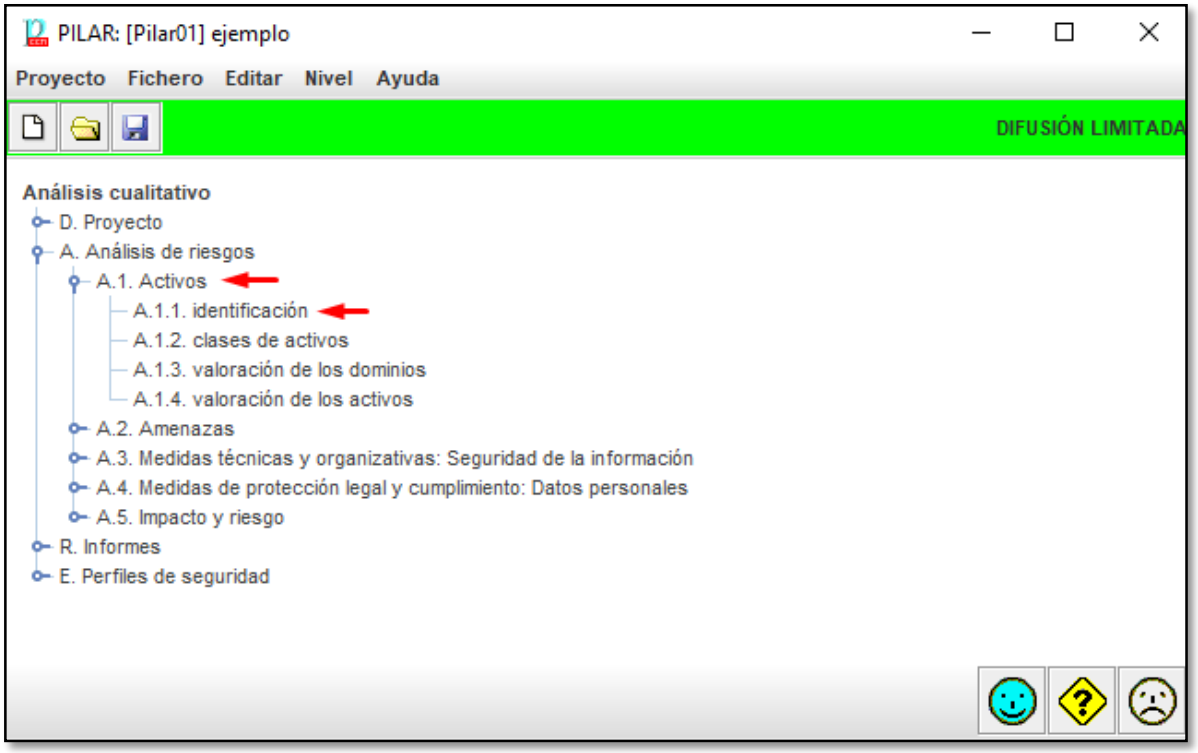
En las casillas de datos, debe llenar con los datos de la empresa y personas a cargo de su administración. Para este manual no se llenaron esos datos y el nombre del proyecto es **ejemplo** y el código **Pilar01**. Para poder guardar la información se dirige en la parte inferior derecha de la pantalla en la **Carita Feliz.**



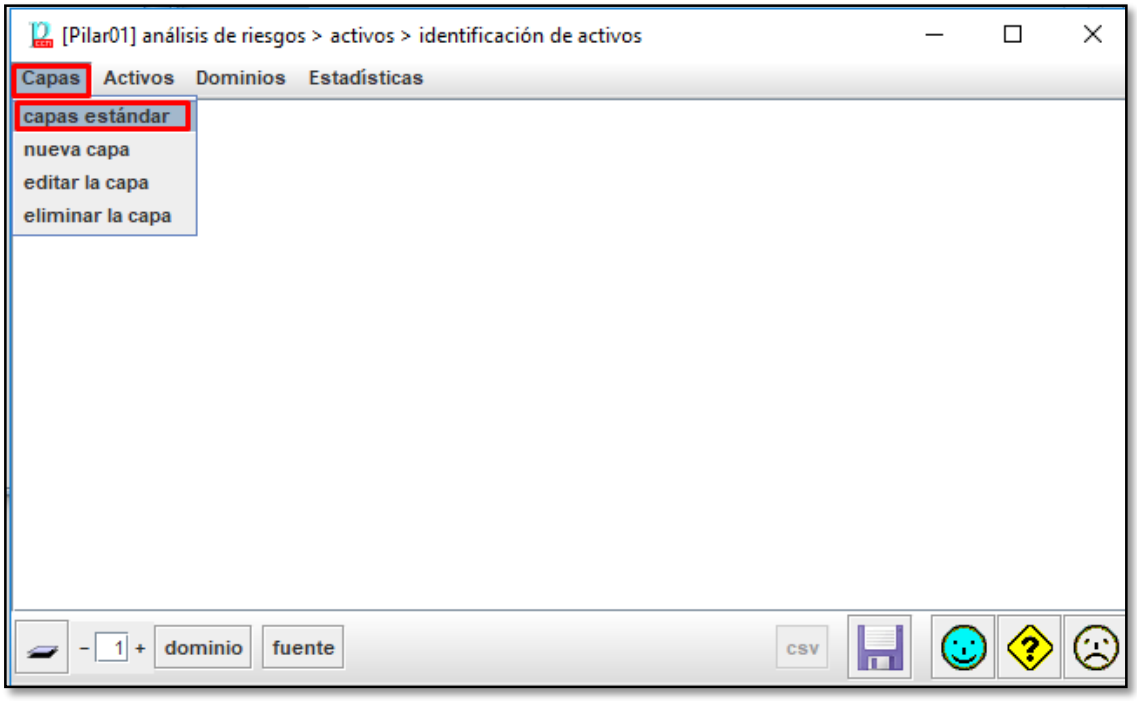
Una vez completa la descripción del proyecto, y aparece un árbol de opciones donde vamos a ingresar nuestros activos.



Para el ingreso de activos, hacemos clic en la opción análisis de riesgos > Identificación.

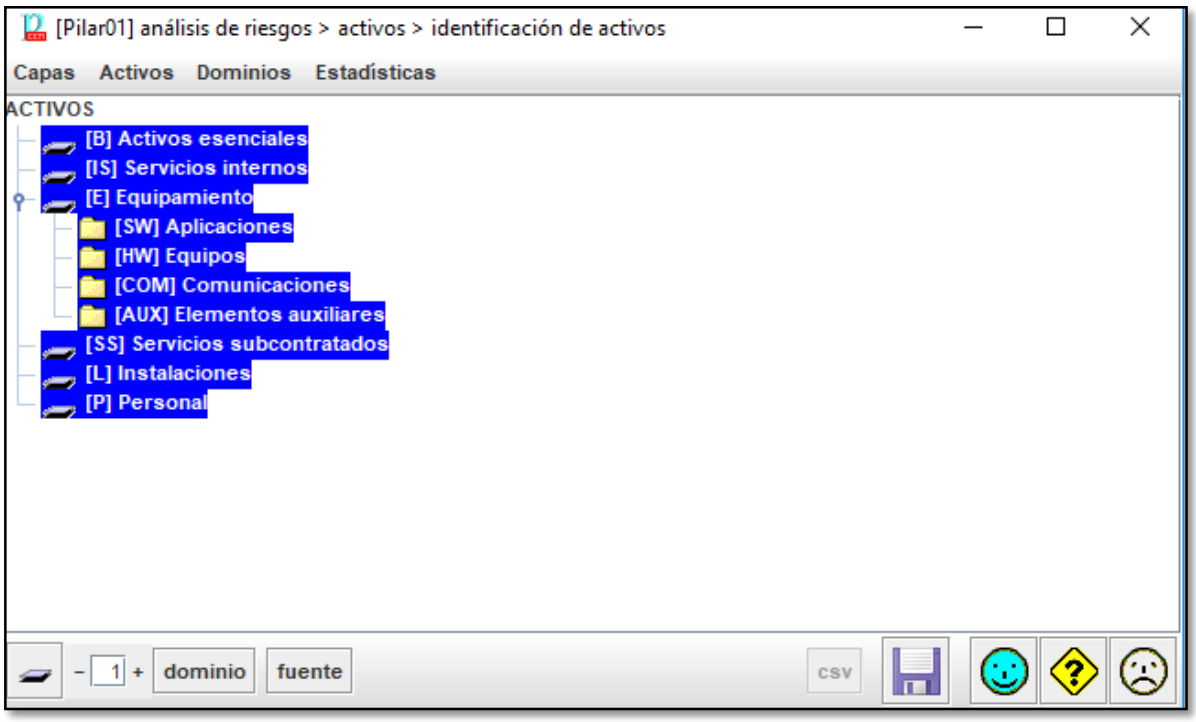


Ingresamos a la opción para identificar activos, en la pestaña **Capas** hacemos clic y seleccionamos la opción **capa estándar**.



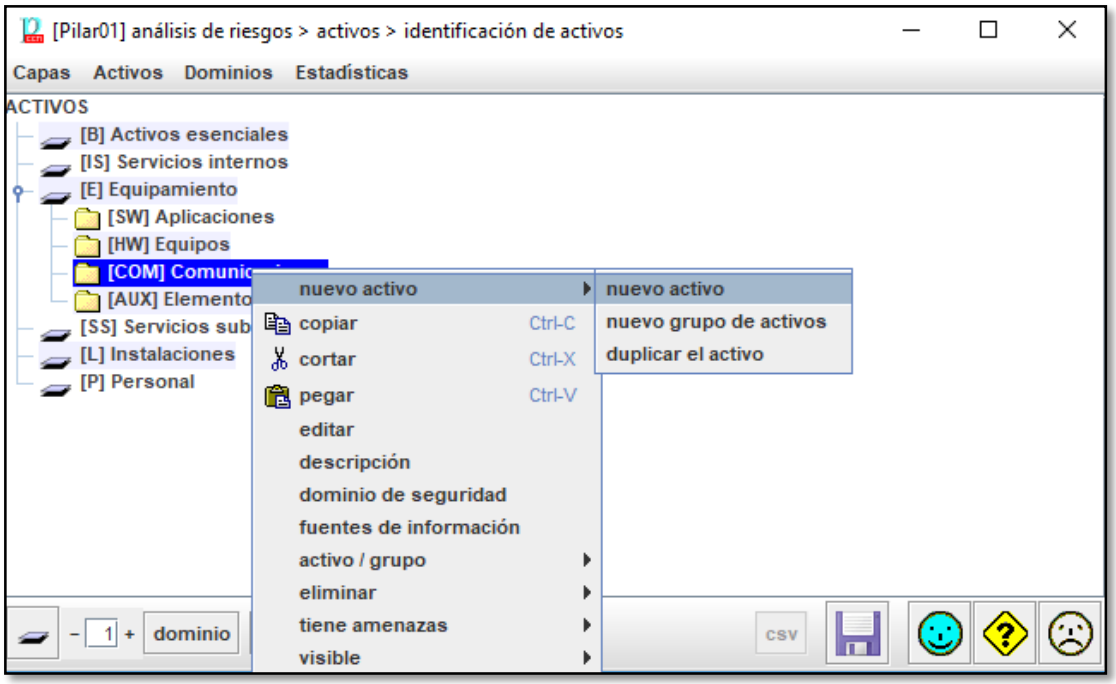
1.7. Identificación de Activos

Como ejemplo aparecen estos activos ya creados, y donde realizaremos cambios.

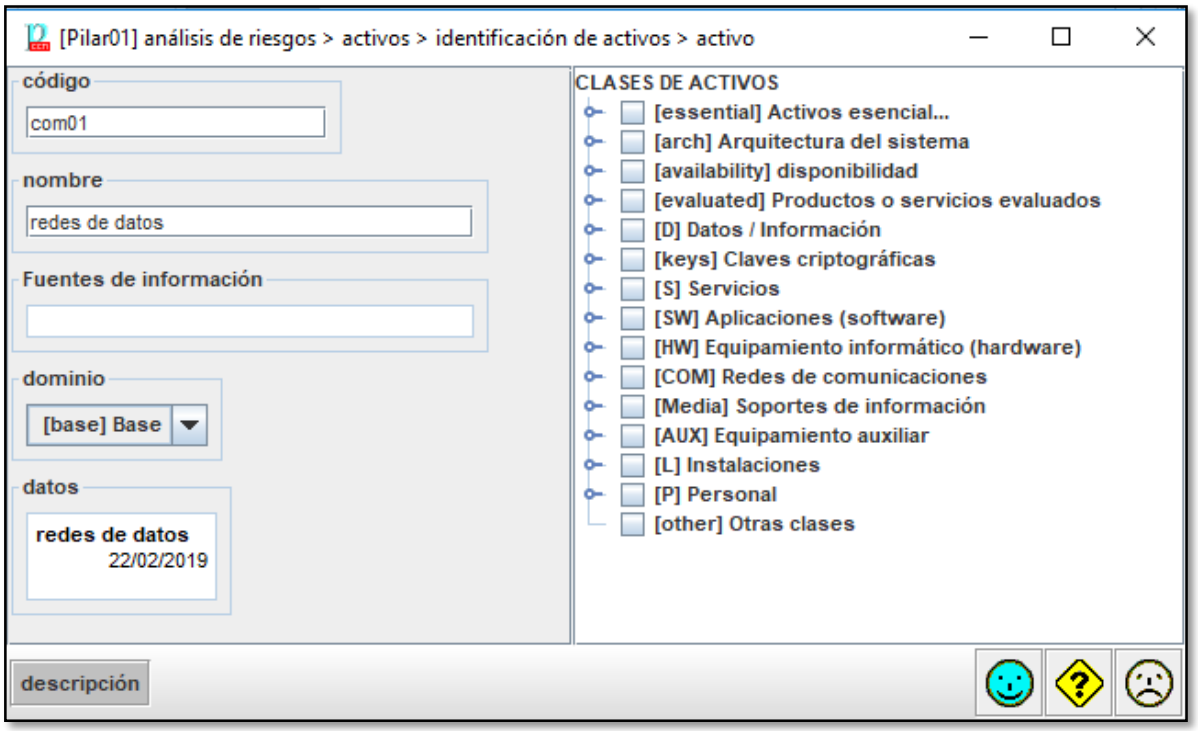


En la carpeta Comunicaciones > nuevo activo > nuevo activo y pulamos clic, para crear un activo.

1.8. Crear Activos



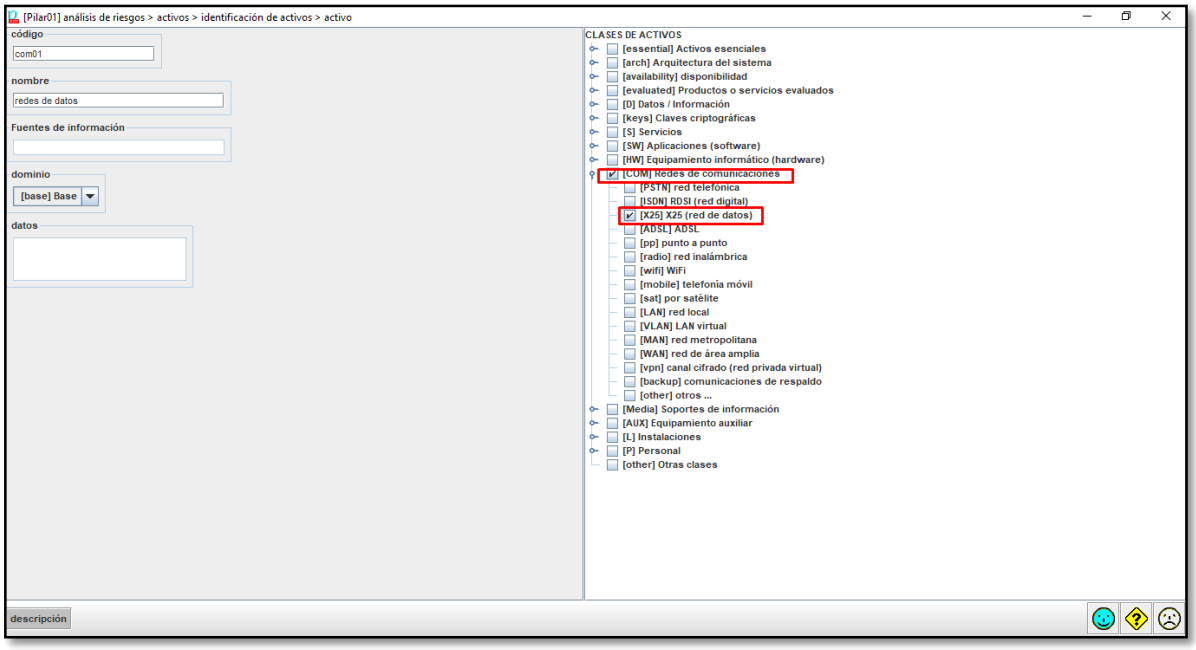
La cual debemos llenar con los datos del activo que se desea ingresar. **Se puede poner cualquier código y nombre**, en datos se puede colocar una breve descripción si requiere. Para guardar nos dirigimos a la parte inferior derecha y pulsamos la **Carita Feliz**.



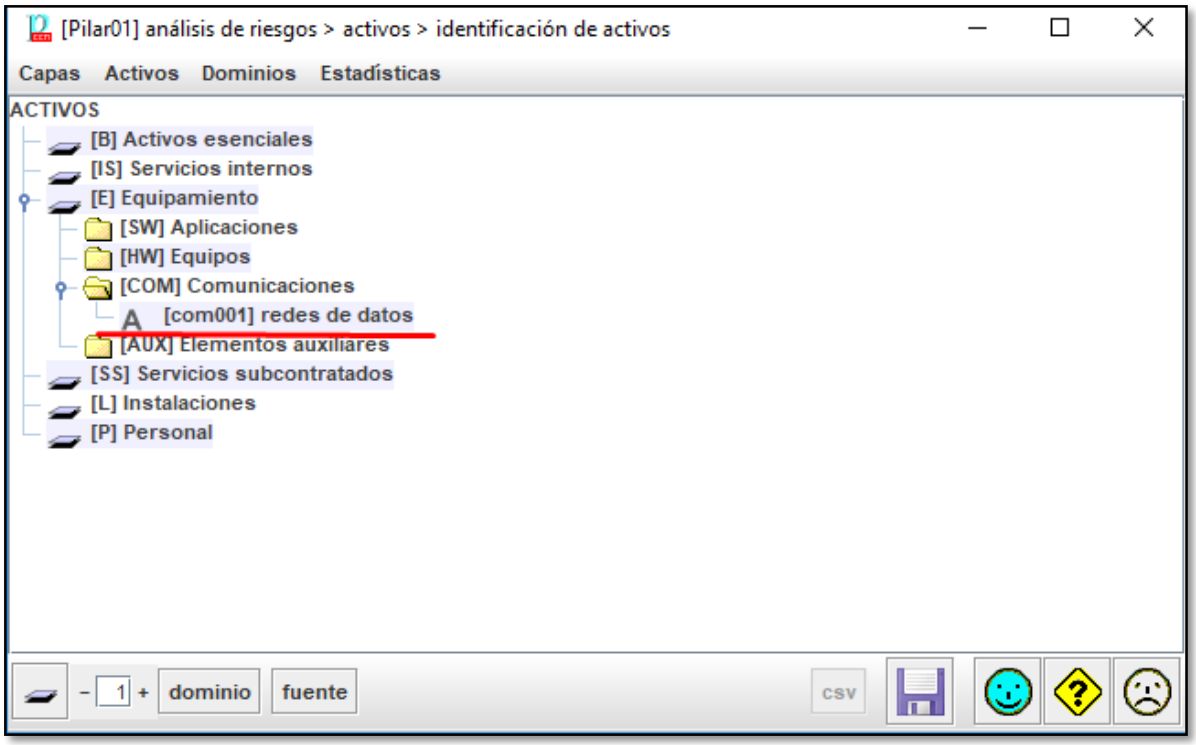
1.9. Clases de Activos

Una vez seleccionada esta opción, aparece un árbol de redes que podemos escoger, según el tipo de activo que este sea. En la parte derecha seleccionamos que clase de activo, en este caso **red de datos.**

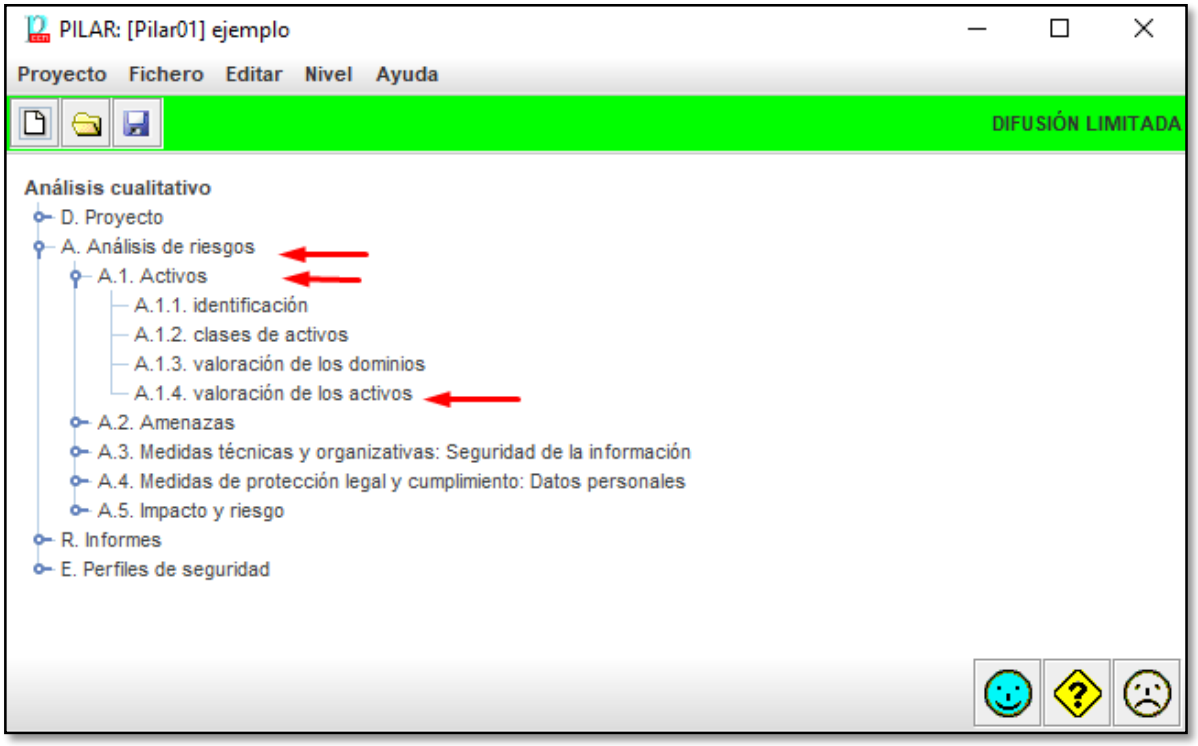
En este caso escogemos la opción **Red de Datos**. Guardamos mediante el icono en la parte inferior izquierda.



Ya se creó el activo dentro de la carpeta de Comunicación



Una vez creado el activo, vamos a valoración de activos.



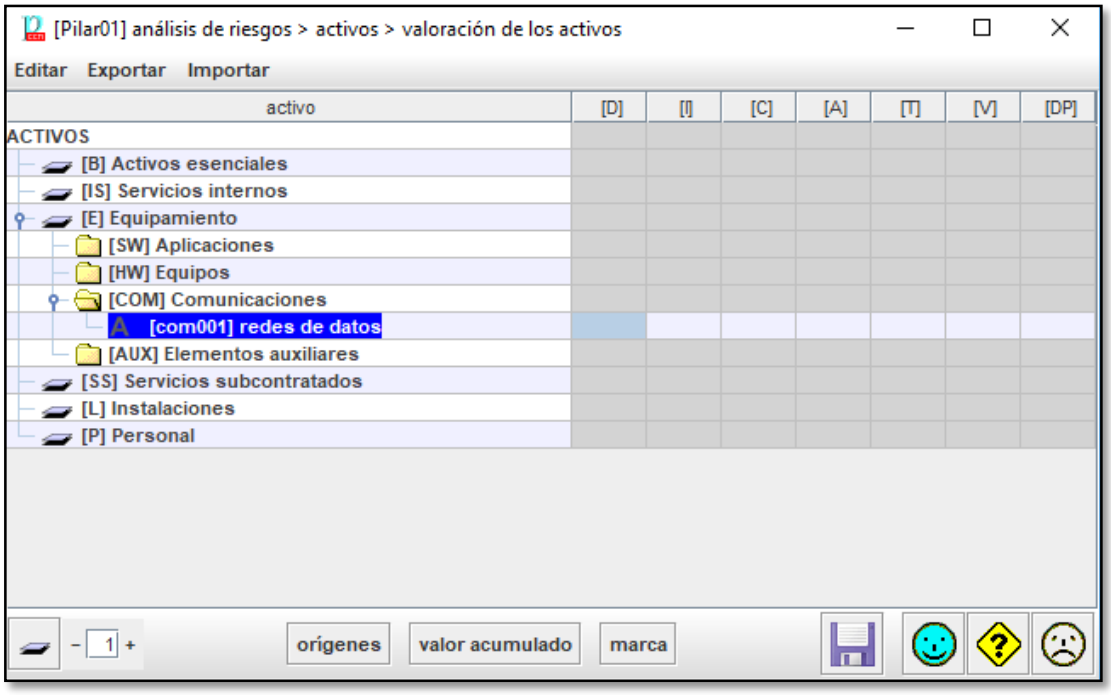
Aquí tenemos las carpetas de activos.

1.9.1. Valoración de Activos

Análisis de riesgos > Activos > Valoración de Activos

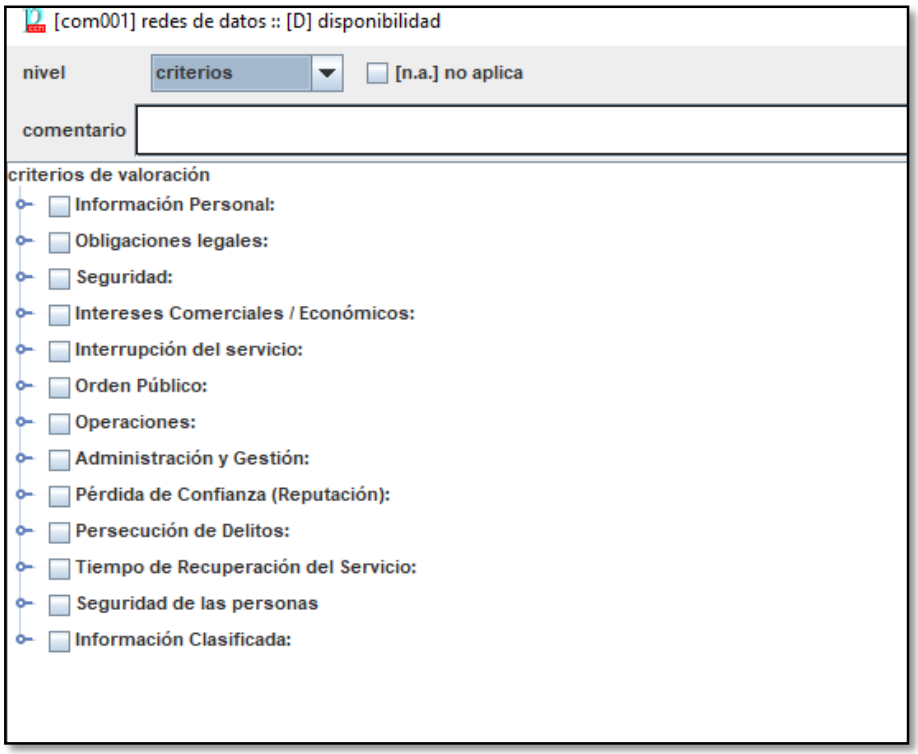
Para los activos de información, valore el nivel requerido de seguridad entre 0 (despreciable) y 10 (el máximo).

Con respecto de la confidencialidad, la integridad, la autenticidad y la trazabilidad, si no especifica ningún nivel, PILAR entenderá que el activo no tiene requisitos significativos en esa dimensión (por ejemplo, no hay requisitos de confidencialidad en la información que es pública)

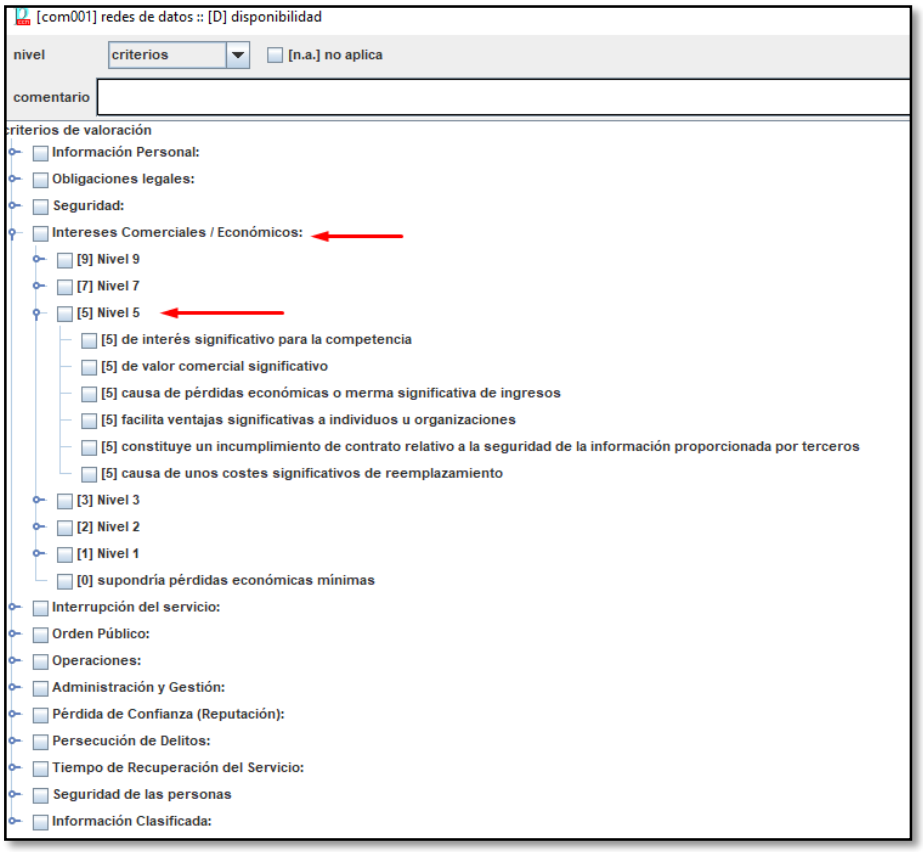


1.9.2 Evaluación de Activos

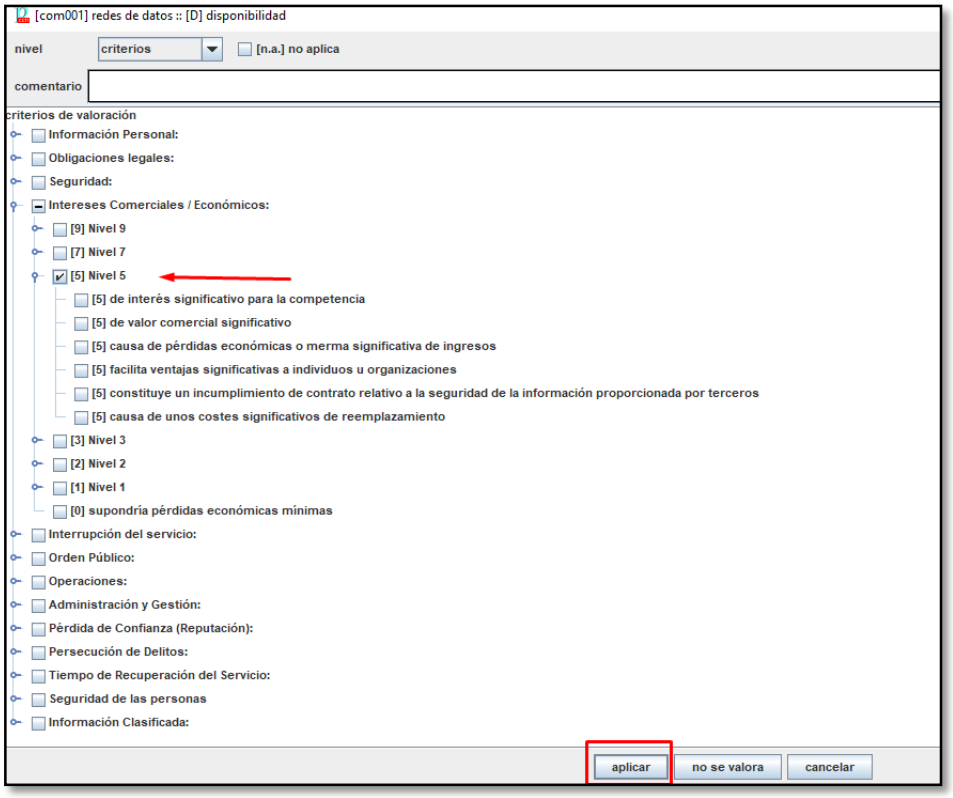
Se hace clic derecho en la disponibilidad, abriendo la venta de evaluación, en la cual nos salen todas las opciones a evaluar.



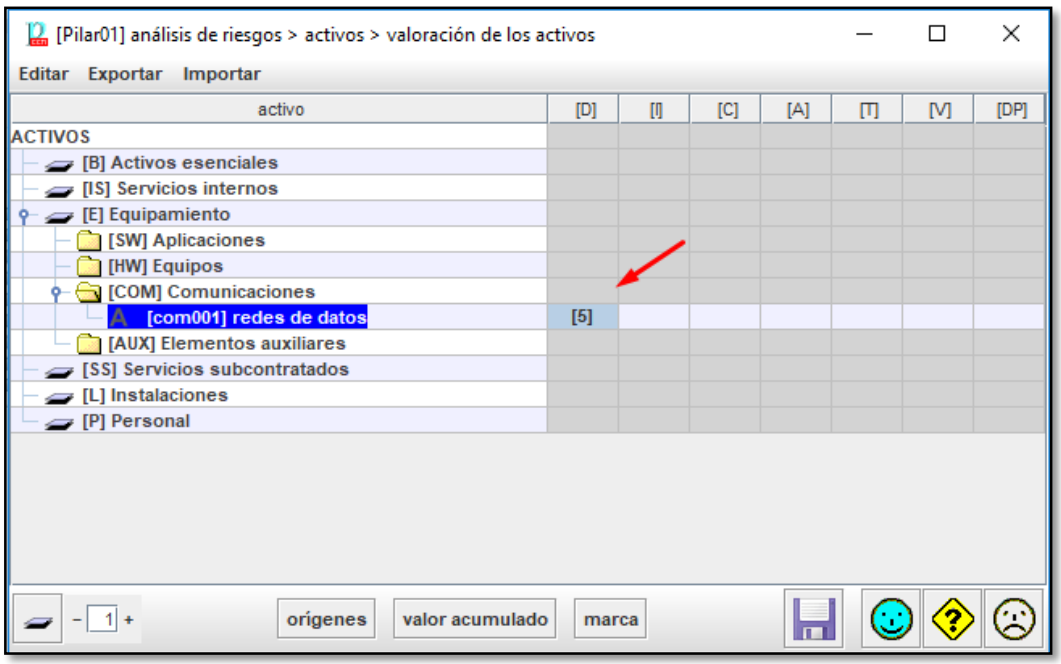
En los criterios de valoración nos indica todos los criterios a valorar, si vamos a la opción de **Intereses Comerciales / Económicos** y desplegamos la opción de Nivel 5, permite seleccionar las siguientes opciones.



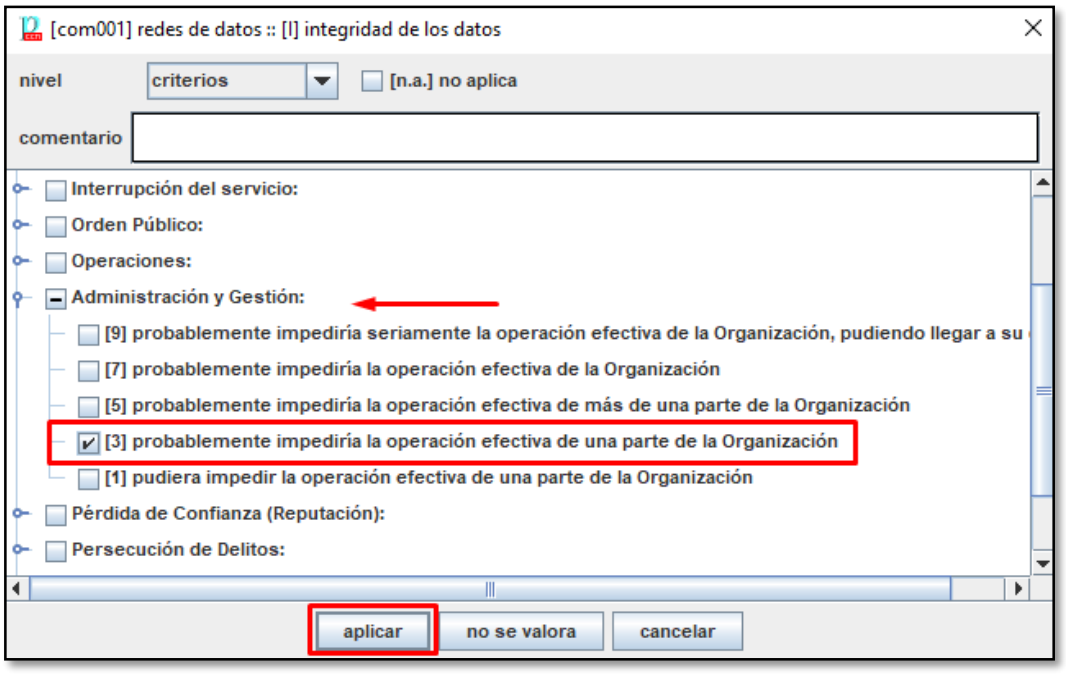
Si se cree que esto es relevante para la red, podemos seleccionar todo el nivel o solo partes, en el ejemplo seleccionamos todo el nivel y pulsamos **Aplicar**.



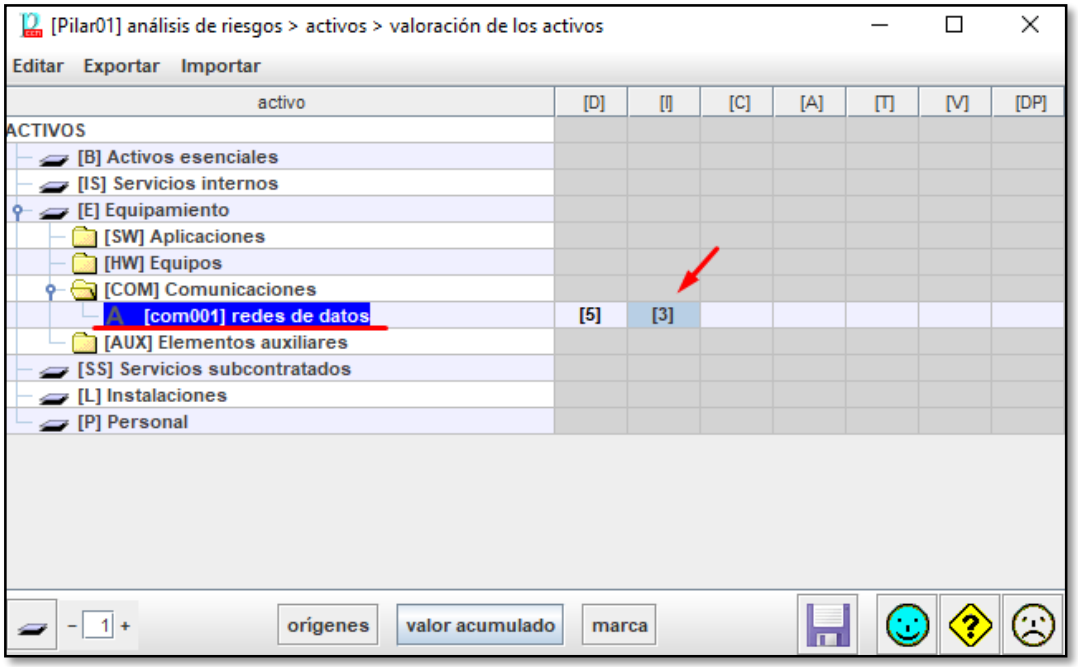
Una vez que aplicamos la disponibilidad nos aparece en la pantalla de la calificación que seleccionamos.



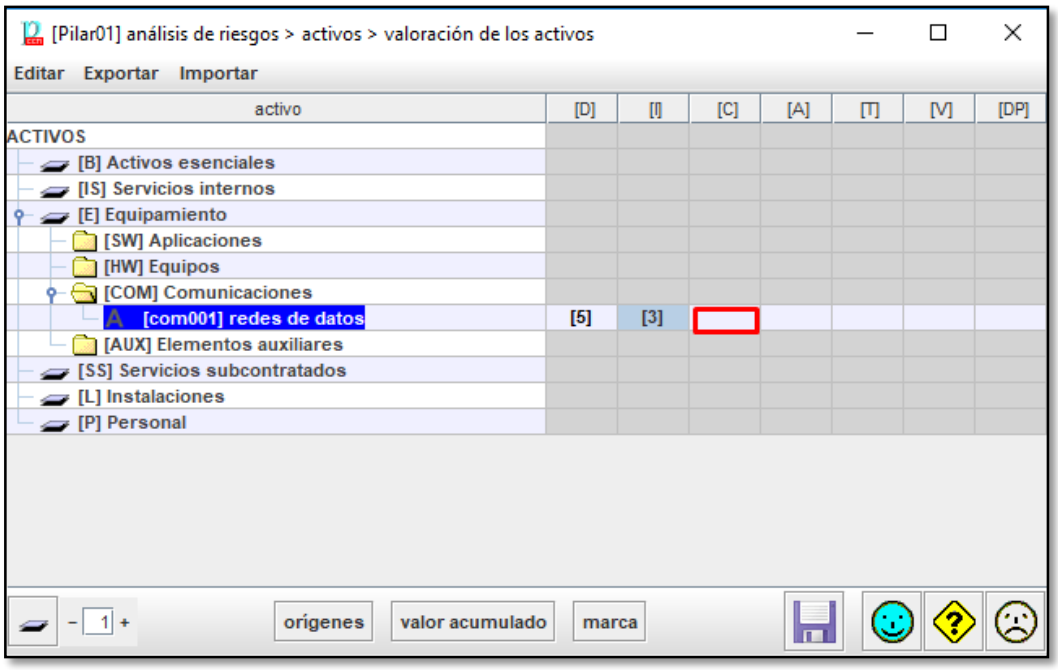
Para la opción de Integridad de datos, seleccionamos de las opciones la de administración y Gestión > Opción 3 > Aplicar.



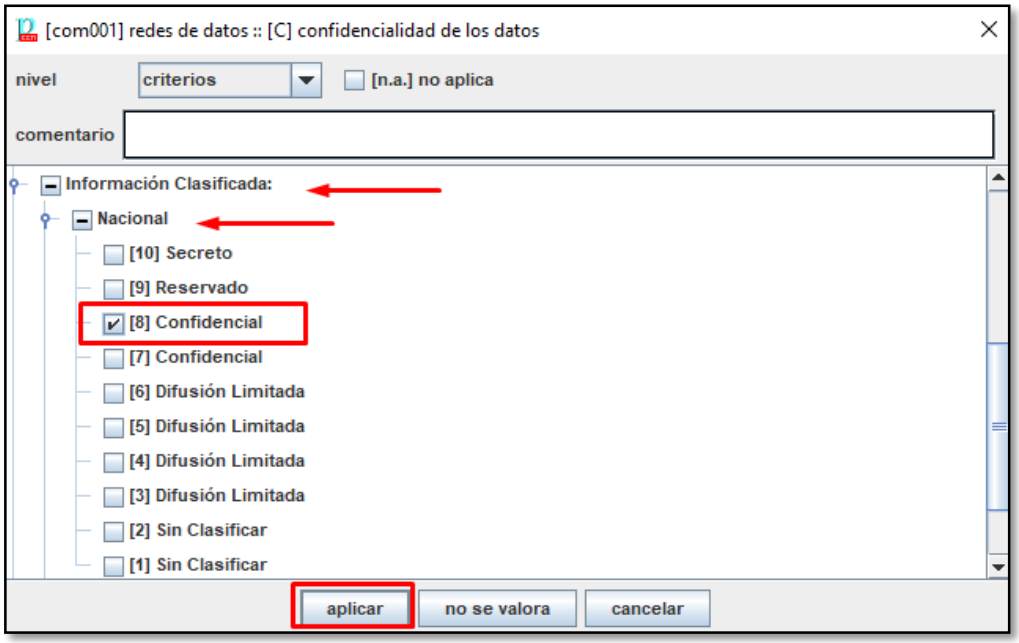
Una vez que aplicamos la integridad de los datos nos aparece en la pantalla de la calificación que seleccionamos.



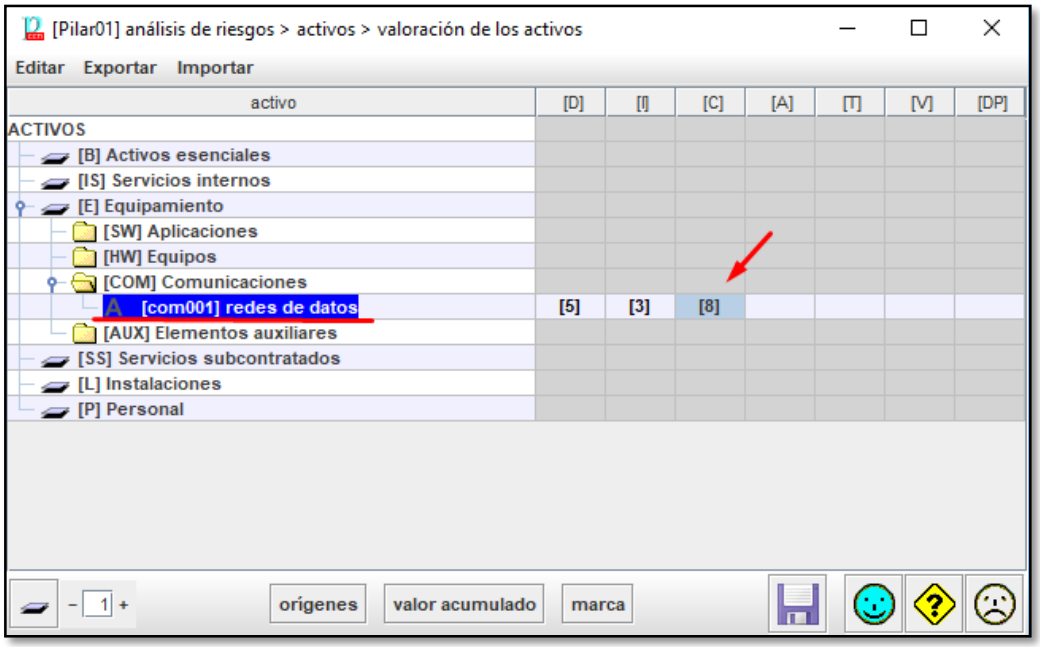
De igual forma para la Confidencialidad de los datos, pulsamos clic derecho en el espacio y nos dirige a la valoración del activo.



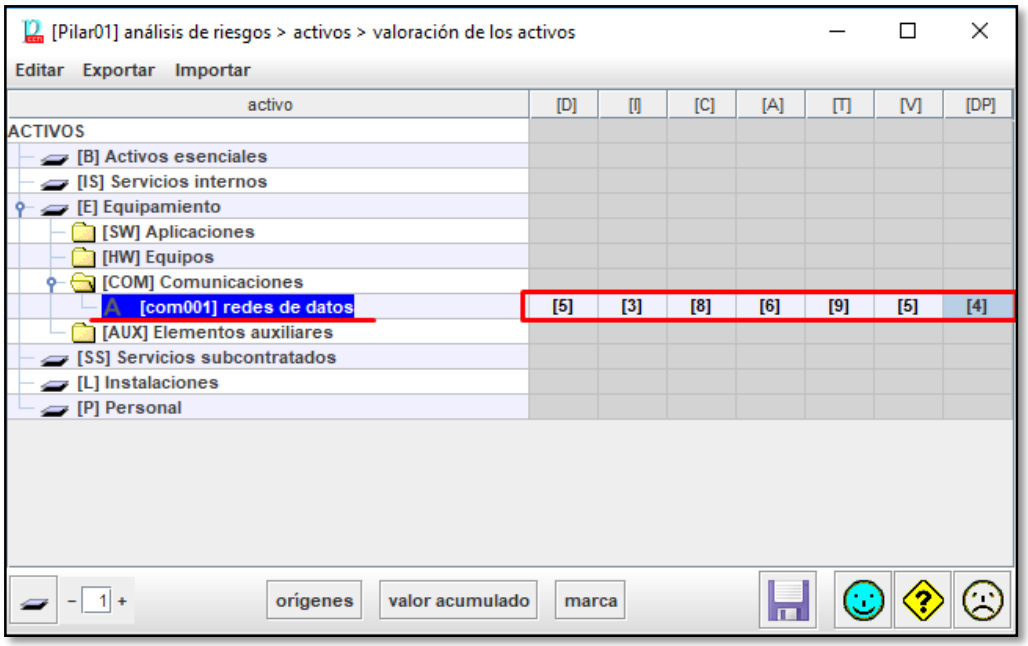
Se dirige **a Información clasificada > Nacional > Confidencial. Pulsamos Aplicar.**



De igual forma para la Confidencialidad de los datos, pulsamos Aplicar y aparece la valoración dada.



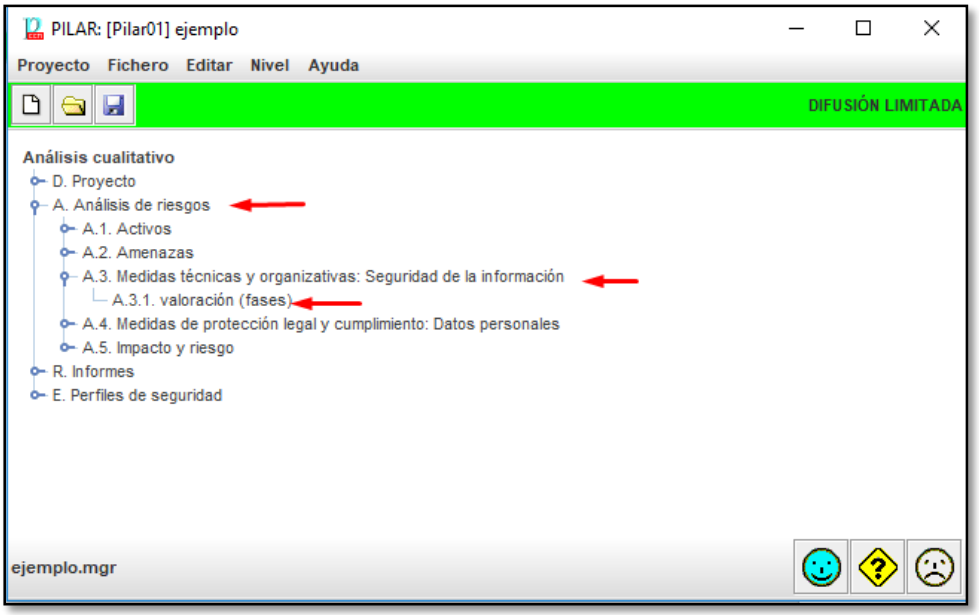
Se debe llenar todos los campos a valorar y luego guardamos la calificación.



1.10. Salvaguardas

Las salvaguardas son medidas de emergencia para mitigar las posibles amenazas que se tiene con respecto a un activo.

Para ingresar a las Salvaguardas, clic en **Análisis de riesgo > Medidas técnicas > Valoración.**



PILAR en los activos creados y valorados indica L1 – L2, el cual da una valoración y las fases del proyecto, para la administración y los objetivos deseados y el plazo de cada objetivo.

Salvaguardas

Valoración	Fases del Proyecto
L0 = Inexistente	Current = Actual
L1 = Inicial	3m = A 3 meses
L2 = Reproducible e Intuitivo	1y = A 1 año
L3 = Proceso Definido	Target = Objetivo Deseado
L4 = Gestionable y Medible	
L5= Optimizado	

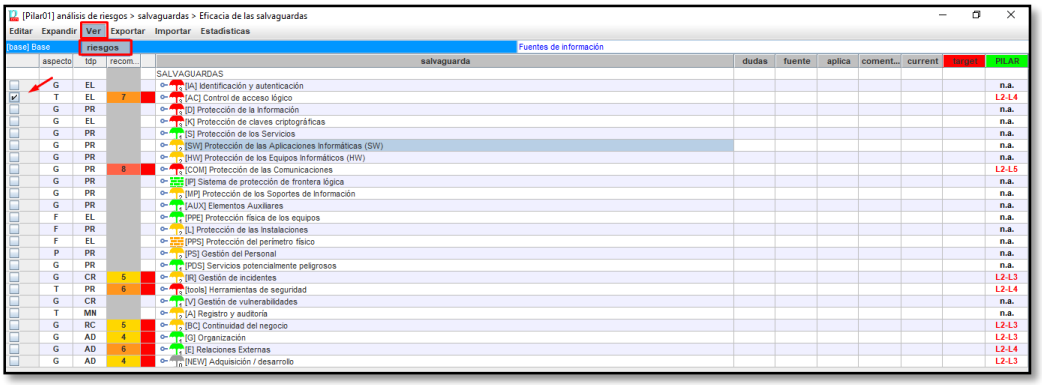
1.11. Amenazas

Las columnas presentan fases del proyecto. Sirven para evaluar la madurez de las medidas en varios momentos y poder observar la evolución de la seguridad del sistema. Típicamente, hay 2 fases: la situación actual y adónde nos proponemos llegar. Una última columna, PILAR sirve para que PILAR proponga un objetivo “razonable” o “prudente”.

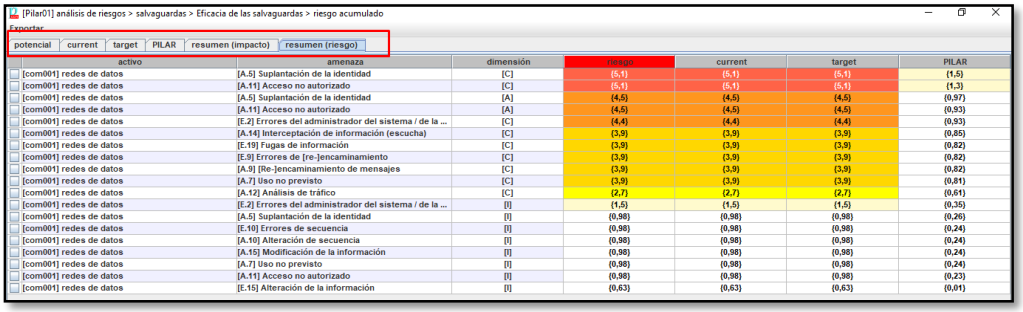
No todas las salvaguardas son igual de importantes:

3	máximo peso	crítica
2	peso alto	muy importante
1	peso normal	importante
0	peso bajo	interesante
✓	aseguramiento: componentes certificados	

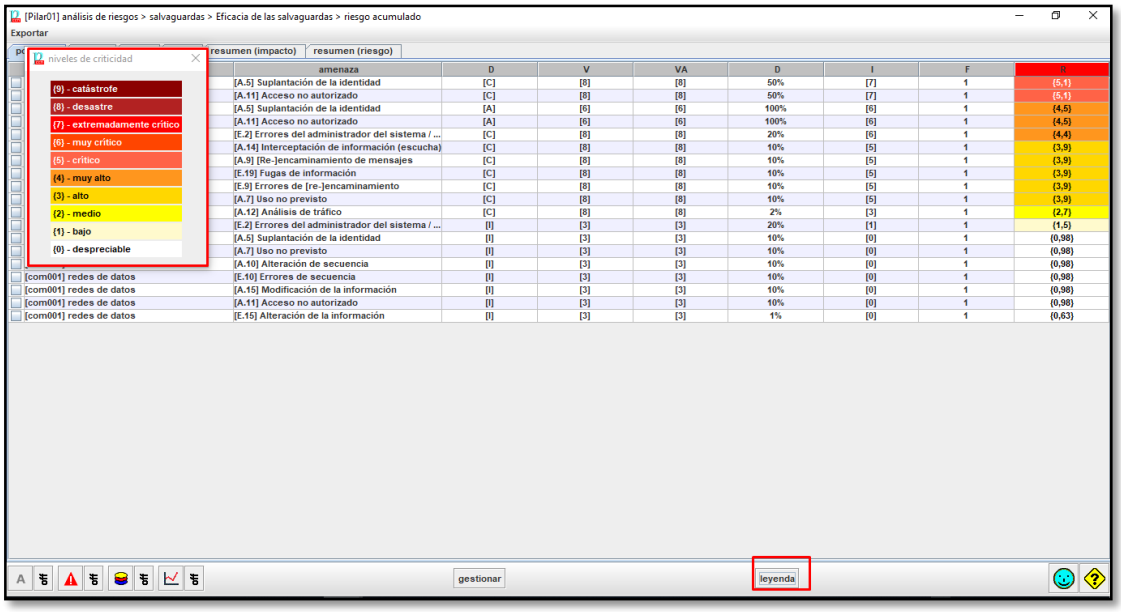
Para poder ver los riesgos que se tiene en los activos, seleccionamos **el activo** > pulsamos la opción superior izquierda **VER** y seleccionamos **RIESGO.**



Dando como resultado los posibles riesgos que tienen los activos, en la parte superior izquierda tenemos las opciones que se pueden presentar en los activos. Y los niveles y porcentajes de riesgo que se tiene, dando calificaciones del 1 – 10 de riesgos que se tiene.



Pulsando la opción LEYENDA en la parte inferior, indica los niveles de criticidad mediante numeración y colores. En los colores críticos que son pasando de la numeración 5 es donde debemos tomar medidas.



PILAR se distribuye con una serie de informes predefinidos. Algunos informes están codificados dentro de la herramienta (textual y gráfica), mientras que otros vienen regidos por patrones. Los patrones son plantillas RTF que pueden editarse con muchos procesadores de textos.

Las gráficas pueden ser útiles para presentaciones, como gráficos a adjuntar al texto. Algunos informes textuales son valiosos en sí mismos, a veces como informe final del análisis, a veces como material de trabajo para que los propietarios de los activos puedan aportar o validar información de sus propiedades.

Anexo 5: Fichas técnicas servidores

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

FICHA TÉCNICA DE SERVIDORES

CARACTERÍSTICAS	DESCRIPCIÓN
Responsable	Ing. Deisy Imbaquingo
Modelo	IBM System x3500 M4
Memoria RAM	7.6 GB
Disco Duro	610 GB
Ubicación Física	RACK 3
Función	Servidor Revista Universitaria
Procesador	Intel Xeon ® CPU E5405 2.0GH x 12
Número de Serie/Identificador UTN	KQ5M81T/1410103.327.0079
Estado	Activo (X) Inactivo ( )
Sistema Operativo	Centos 7
Usuarios Finales	Estudiantes (X) Profesores (X) Administrativos (X)
Observaciones	

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

FICHA TÉCNICA DE SERVIDORES

CARACTERÍSTICAS	DESCRIPCIÓN
Responsable	Ing. Fabián Cuzme
Modelo	IBM System x3500 M4
Memoria RAM	7.6 GB
Disco Duro	135 GB
Ubicación Física	RACK 3
Función	Servidor Reactivos
Procesador	Intel Xeon ® CPU E5405 2.0GH x 12
Número de Serie o Identificador	KQ6M81V/110103.327.0078
Estado	Activo (X) Inactivo ( )
Sistema Operativo	Centos 6.5
Usuarios Finales	Estudiantes (X) Profesores (X) Administrativos (X)
Observaciones	

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

FICHA TÉCNICA DE SERVIDORES

CARACTERÍSTICAS	DESCRIPCIÓN
Responsable	Ing. Hernán Domínguez
Modelo	IBM System x3200 M2
Memoria RAM	2 GB
Disco Duro	1 TB
Ubicación Física	RACK 2
Función	Servidor Radius
Procesador	Dual-core Xeon E3110 3.0
Número de Serie/Identificador UTN	103QCPYOF560/1410107.001.5050
Estado	Activo (X) Inactivo ( )
Sistema Operativo	
Usuarios Finales	Estudiantes (X) Profesores (X) Administrativos (X)
Observaciones	

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

FICHA TÉCNICA DE SERVIDORES

CARACTERÍSTICAS	DESCRIPCIÓN
Responsable	Ing. Hernán Domínguez
Modelo	HP Proliant DL 360 G9
Memoria RAM	32 GB
Disco Duro	3x 450 GB
Interfaces de Comunicación	4 x GB
Ubicación Física	RACK 3
Función	Servidor Proxmox (PV1)
Procesador	Intel Xeon ® CPU E5-2620 V3
Número de Serie/Identificador UTN	MXQ51704F7/1410107.018.02017
Estado	Activo (X) Inactivo ( )
Sistema Operativo	Ubuntu Server 14.04 LTS
Usuarios Finales	Estudiantes (X) Profesores (X) Administrativos ( )
Observaciones	

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

FICHA TÉCNICA DE SERVIDORES

CARACTERÍSTICAS	DESCRIPCIÓN
Responsable	Ing. Hernán Domínguez
Modelo	HP ProLiant DL360 Gen 9
Memoria RAM	32 GB
Disco Duro	3x450 GB
Interfaces de Comunicación	4 x 1GBE
Ubicación Física	RACK 2
Función	Servidor Proxmox (PV2)
Procesador	Intel Xeon ® CPU E5-2620 V3
Número de Serie/Identificador UTN	MXQ51500L9/1410107.018.02015
Estado	Activo (X) Inactivo ( )
Sistema Operativo	Ubuntu Server 14.04 LTS
Usuarios Finales	Estudiantes (X) Profesores (X) Administrativos ( )
Observaciones	

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

FICHA TÉCNICA DE SERVIDORES

CARACTERÍSTICAS	DESCRIPCIÓN
Responsable	Ing. Hernán Domínguez
Modelo	HP ProLiant DL360 Gen 9
Memoria RAM	32 GB
Disco Duro	3x450 GB
Interfaces de Comunicación	4 x 1GBE
Ubicación Física	RACK 2
Función	Servidor Proxmox (PV3)
Procesador	Intel Xeon ® CPU E5-2620 V3
Número de Serie/Identificador UTN	MXQ51500L9/1410107.018.02015
Estado	Activo (X) Inactivo ( )
Sistema Operativo	Ubuntu Server 14.04 LTS
Usuarios Finales	Estudiantes (X) Profesores (X) Administrativos ( )
Observaciones	

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

FICHA TÉCNICA DE SERVIDORES

CARACTERÍSTICAS	DESCRIPCIÓN
Responsable	Ing. Hernán Domínguez
Modelo	HP Proliant DL 150 G9
Memoria RAM	1 GB / 16 GB (max)
Disco Duro	160 GB
Ubicación Física	RACK 2
Función	Servidor Proxmox (PV4)
Procesador	Intel Xeon ® CPU E5405 Quad Core
Número de Serie/Identificador UTN	MXS8460A5J/1410107.001.728
Estado	Activo (X) Inactivo ( )
Sistema Operativo	Ubuntu Server 14.04 LTS
Usuarios Finales	Estudiantes (X) Profesores (X) Administrativos ( )
Observaciones	

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN
FICHA TÉCNICA DE SERVIDORES

CARACTERÍSTICAS	DESCRIPCIÓN
Responsable	Ing. Fabián Cuzme
Modelo	HP Proliant ML 150 G5
Memoria RAM	4.8 GB
Disco Duro	150 GB
Ubicación Física	RACK 3
Función	Servicio de encuestas y evaluación Opina
Procesador	Intel Xeon ® CPU E54405 GHz x 4
Número de Serie/Identificador UTN	MXS8460A5P/1410107.001.727
Estado	Activo (X) Inactivo ( )
Sistema Operativo	Ubuntu 12.10
Usuarios Finales	Estudiantes (X) Profesores (X) Administrativos (X)
Observaciones	

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

FICHA TÉCNICA DE SERVIDORES

CARACTERÍSTICAS	DESCRIPCIÓN
Responsable	Ing. Pablo Landeta
Modelo	IBM System x3250 M3
Memoria RAM	
Disco Duro	
Ubicación Física	RACK 3
Función	Servidor GeoPortal
Procesador	
Número de Serie/Identificador UTN	
Estado	Activo (X) Inactivo ( )
Sistema Operativo	Ubuntu 12.10
Usuarios Finales	Estudiantes (X) Profesores (X) Administrativos ( )
Observaciones	

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

FICHA TÉCNICA DE SERVIDORES

CARACTERÍSTICAS	DESCRIPCIÓN
Responsable	Ing. Mauricio Rea
Modelo	IBM System x3250
Memoria RAM	
Disco Duro	
Ubicación Física	RACK 3
Función	Servidor Pruebas CISIC
Procesador	
Número de Serie/Identificador UTN	
Estado	Activo (X) Inactivo ( )
Sistema Operativo	
Usuarios Finales	Estudiantes (X) Profesores (X) Administrativos ( )
Observaciones	

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

FICHA TÉCNICA DE SERVIDORES

CARACTERÍSTICAS	DESCRIPCIÓN
Responsable	Ing. Ludmila Stamburgo
Modelo	PC “Clon” H81M-S1
Memoria RAM	4.8 GB
Disco Duro	150 GB
Ubicación Física	RACK 3
Función	Servidor Biométricos
Procesador	Intel Xeon (R) CPU E54405 GHz x 4
Número de Serie/Identificador UTN	
Estado	Activo (X) Inactivo ( )
Sistema Operativo	Ubuntu 12.10
Usuarios Finales	Estudiantes ( ) Profesores (X) Administrativos (X)
Observaciones	

Anexo 6: Acta Mesa de Trabajo

MESA DE TRABAJO	
DATACENTER FICA-UTN	
CRITERIOS Y VALORACIÓN PARA LOS ACTIVOS	
Fecha: 21 de Enero de 2019	**Lugar:** Data Center FICA
Hora de Inicio: 9:00am	**Hora de Finalización:** 12:00pm

Objetivos:

- Establecer criterios para la valoración de activos con base a criterios recomendados en la metodología Magerit. Estos valores deben estar en una escala común.
- Determinar el valor para cada activo de la organización.

Criterios de Valoración

La asignación de valores en este proyecto se realiza mediante valoración cualitativa, el cual permite asignar el valor a los activos utilizando una escala de niveles como se muestra en las tablas a continuación.

Para poder asignar un valor a la propiedad de disponibilidad se responde a la pregunta ¿Qué importancia tendría que el activo no estuviera disponible?

Criterios de la valoración DISPONIIBILIDAD		
Extremo	10	Información cuya inaccesibilidad durante corto tiempo podría impedir la ejecución de las actividades del Data Center.
Muy alto	9	Información cuya inaccesibilidad durante una hora podría impedir la ejecución de las actividades del Data Center.
Alto	6-8	Información cuya inaccesibilidad durante la jornada podría impedir la ejecución de las actividades del Data Center.
Medio	3-5	Información cuya inaccesibilidad durante 2 días podría impedir la ejecución de las actividades del Data Center.
Bajo	1-2	Información cuya inaccesibilidad durante una semana podría impedir la ejecución de las actividades del Data Center.
Despreciable	0	Información cuya inaccesibilidad no afecta a la actividad normal del Data Center.

En el caso de la propiedad de integridad es necesario responder a la pregunta ¿qué importancia tendría que los datos fueran modificados fuera de control?

Criterios de la valoración INTEGRIDAD		
Extremo	10	Información cuya modificación no autorizada no podría repararse, impidiendo la realización de las actividades del Data Center.
Muy alto	9	Información cuya modificación no autorizada sea muy difícil de reparar, causando graves daños en realización de las actividades del Data Center.
Alto	6-8	Información cuya modificación no autorizada sea de difícil reparación, causando daños en realización de las actividades del Data Center.
Medio	3-5	Información cuya modificación no autorizada impida por un periodo significativo la realización de las actividades del Data Center.
Bajo	1-2	Información cuya modificación no autorizada que pueda repararse, aunque podría ocasionar por un periodo corto, la suspensión de la realización de las actividades del Data Center.
Despreciable	0	Información cuya modificación no autorizada es de fácil reparación, o que no afecte la realización de las actividades del Data Center.

En la propiedad de confidencialidad se debe responder a la pregunta ¿qué importancia tendría que el dato fuera conocido por personas no autorizadas?

Criterios de la valoración CONFIDENCIALIDAD		
Extremo	10	Información que puede ser conocida por muy pocas personas, cuya divulgación podría ocasionar perjuicios a las actividades del Data Center.
Muy alto	9	Información que puede ser conocida por un grupo muy reducido, cuya divulgación podría ocasionar perjuicios a las actividades del Data Center.
Alto	6-8	Información que puede ser conocida por los usuarios del Data Center, pero su mal uso o divulgación pueda ocasionar inconvenientes en las actividades del Data Center.
Medio	3-5	Información que puede ser conocida y utilizada por todos los usuarios del Data Center.
Bajo	1-2	Información que puede ser conocida y usado por todos los usuarios o personal dentro de la Facultad.
Despreciable	0	Información que puede ser conocida y utilizada sin autorización por cualquier persona, dentro o fuera del Data Center.

Ante la propiedad de autenticidad se debe responder a la pregunta ¿Qué importancia tendría que quien accede al servicio no sea realmente quien cree?

Criterios de la valoración AUTENTICIDAD		
Extremo	10	Que acceda otra persona no designada, impidiendo la realización de las actividades del Data Center.
Muy alto	9	Que acceda otra persona no designada, causando prejuicios en la realización de las actividades del Data Center.
Alto	6-8	Que acceda otras personas no designadas, conociendo información que podría causar daños en las actividades del Data Center.
Medio	3-5	Que acceda otras personas no designadas, conociendo información que podría causar daños en una parte del Data Center.
Bajo	1-2	Que accedan otras personas no designadas, con la probabilidad de causar un daño menor.
Despreciable	0	Que accedan otras personas no designadas, no supondría daño alguno.

Valoración de Activos

Se determina el valor de un activo frente a cada propiedad de la seguridad de la información mediante el análisis de las funciones e importancia de cada activo para la continuidad de la institución, basándose en los criterios antes descritos, plasmando los resultados en la siguiente tabla.

ACTIVOS DEL DATACENTER FICA				
		Esenciales		
Código	**Disponibilidad**	**Integridad**	**Confidencialidad**	**Autenticidad**
ESFICA1/RU	8	9		4
ESFICA2/SRR	9	8	7	5
		Equipos informáticos (Hardware)		
HWFICA1/PV1	5	7	6	8
HWFICA2/PV2	5	7	6	8
HWFICA3/PV3	5	7	6	8
HWFICA4/PV4	5	7	6	8
HWFICA5/SS	4	5	5	6
HWFICA6/CS1	7	9	5	9
HWFICA7/CS2	5	8	4	5
HWFICA8/SWC	10	9	8	9
HWFICA9/RTM	10	9	8	9
HWFICA10/SWD1	10	9	5	9
HWFICA11/SWQP	10	9	6	9
HWFICA12/SWD2	10	9	5	8
HWFICA13/SWD3	10	9	5	9

	Aplicaciones informáticas (Software)			
SWFICA1/P	6	8	8	7
SWFICA2/O	4	8	8	6
SWFICA3/M	5	8	5	5
SWFICA4/B	4	9	8	9
	Elementos Auxiliar			
EAFICA1/SE	6			
EAFICA2/AA	5			
EAFICA3/UPS	4			
EAFICA4/CS	4	3	3	2
EAFICA5/CA	9	7	5	7
EAFICA6/BB	9			
EAFICA7/CU	6			

Damos a conocer el acta firmada en la reunión de la mesa de trabajo del Lunes, 21 de enero de 2019, en la cual se determina los criterios y valoración de activos. Siendo los responsables Ing. Santiago Meneses encargado del Data Center y Sra. Vanessa Jácome autora proyecto de titulación.

Ing. Santiago Meneses
Técnico-Docente
Encargado Data Center FICA

Sra. Vanessa Jácome
Autora
Proyecto de Titulación

Anexo 7: Análisis de Riesgo

1. Objetivo:

El presente Anexo contiene los resultados del análisis de riesgos realizado a los activos de información del Data Center la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica del Norte (UTN) en base a la Metodología de Análisis y Gestión de Riesgos Tecnológicos (Magerit).

2. Inventario de activos de información

El presente análisis incluye 26 activos ordenados en base al grupo de activos descritos en la Metodología Magerit,

ACTIVOS DEL DATACENTER FICA - UTN		
Esenciales		
Código	**Nombre**	**Detalle**
ESFICA1/RU	RU	IBM Systemx3500 M4 Revista Universitaria
ESFICA2/SRR	SRR	Servidor Radius
Equipos informáticos (Hardware)		
Código	**Nombre**	**Detalle**
HWFICA1/PV1	HPPV1	HP Proliant DL360 G9 (Proxmox PV3)
HWFICA2/PV2	HPPV2	HP Proliant DL360 G9 (Proxmox PV2)
HWFICA3/PV3	HPPV3	HP Proliant DL360 G9 (Proxmox PV3)
HWFICA4/PV4	HPPV4	HP Proliant ML150 (Proxmox PV4)
HWFICA5/SS	IBMSS	IBM System x3650 M3 (Sin Servicio)
HWFICA6/CS1	IBMCS1	IBM System x3250 M3 (CISIC)
HWFICA7/CS2	IBMCS2	IBM System x3250 (CISIC)
HWFICA8/SWC	CORE	Switch de Core Catalyst 4506-E
HWFICA9/RTM	ROUTER	RouterBoard 1100AHX2 Mikrotik
HWFICA10/SWD1	SWD1	Switch de Distribución 3Com 4500G PROXMOX
HWFICA11/SWQP	SWQP	Switch de distribución inalámbrica QPCOM
HWFICA12/SWD2	SWD2	Switch de distribución CISCO Linksys SR224G
HWFICA13/SWD3	SWD3	Switch de Distribución 3Com 3226 SERVIDORES
Aplicaciones informáticas (Software)		
Código	**Nombre**	**Detalle**
SWFICA1/P	SRP	Proxmox
SWFICA2/O	SRO	Opina
SWFICA3/M	SRM	Reactivos
SWFICA4/B	SRB	PC tipo Clon H8M-S1

Elementos Auxiliar		
Código	**Nombre**	**Detalle**
EAFICA1/SE	SE	Sistema Eléctrico
EAFICA2/AA	AA	Aire Acondicionado
EAFICA3/UPS	UPS	UPS
EAFICA4/CS	CS	Cámara de Seguridad
EAFICA5/CA	CA	Control de Acceso
EAFICA6/BB	BB	Backbone
EAFICA7/CU	CE	Cableado Estructurado

3. Resultados

En las siguientes tablas se ilustra la valoración de las amenazas/vulnerabilidades que afectan a las propiedades de la seguridad de la información, por cada uno de los activos de información citados en la anterior tabla.

Siendo:

P = Probabilidad

D = Disponibilidad

I = Integridad

C = Confidencialidad

A = Autenticidad

Valoración de las amenazas activo ESFICA1/RU (RU Servidor Revista Universitaria)

AMENAZAS/VULNERABILIDADES	**[P]**	**[D]**	**[I]**	**[C]**	**[A]**
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[I.4] Contaminación electromagnética	1	10%			
[I.5] Avería de origen físico o lógico	1	50%			
[I.6] Corte del suministro eléctrico	1	100%			

[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%			
[I.11] Emanaciones electromagnéticas	1			1%	
[E.8] Difusión de software dañino	1	10%	10%	10%	
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%	
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	0,1	100%		100%	
[A.7] Uso no previsto	1	1%	1%	10%	
[A.8] Difusión de software dañino	1	100%	100%	100%	
[A.11] Acceso no autorizado	1	10%	10%	50%	
[A.22] Manipulación de programas	1	50%	100%	100%	
[A.23] Manipulación del hardware	0,5	50%		50%	
[A.24] Denegación de servicio	2	100%			
[A.25] Robo de equipos	0,1	100%		100%	
[A.26] Ataque destructivo	1	100%			

Valoración de las amenazas activo ESFICA2/SRR (SRR Servidor Radius)

AMENAZAS	**[P]**	**[D]**	**[I]**	**[C]**	**[A]**
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[I.4] Contaminación electromagnética	1	10%			
[I.5] Avería de origen físico o lógico	1	50%			
[I.6] Corte del suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%			
[I.11] Emanaciones electromagnéticas	1			1%	
[E.1] Errores de los usuarios	1	10%	10%	10%	
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%	

[E.3] Errores de monitorización (log)	1		1%		
[E.4] Errores de configuración	1		1%		
[E.15] Alteración de la información	1		50%		
[E.18] Destrucción de la información	1	10%			
[E.19] Fugas de información	1			10%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	0,1	100%		100%	
[A.3] Manipulación de los registros de actividad (log)	100		50%		
[A.4] Manipulación de los ficheros de configuración	10	10%	10%	10%	
[A.5] Suplantación de la identidad	10		50%	50%	100%
[A.6] Abuso de privilegios de acceso	10	1%	10%	50%	100%
[A.7] Uso no previsto	1	1%	10%	10%	
[A.11] Acceso no autorizado	100	10%	10%	50%	100%
[A.15] Modificación de la información	10		50%		
[A.18] Destrucción de la información	1	50%			
[A.23] Manipulación del hardware	0,5	50%		50%	
[A.24] Denegación de servicio	10	100%			
[A.25] Robo de equipos	0,1	100%		100%	
[A.26] Ataque destructivo	1	100%			

Valoración de las amenazas activo SWFICA1/P (SRP Servidor Proxmox)

AMENAZAS	**[P]**	**[D]**	**[I]**	**[C]**	**[A]**
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[I.4] Contaminación electromagnética	1	10%			
[I.5] Avería de origen físico o lógico	1	50%			
[I.6] Corte del suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%			

[I.11] Emanaciones electromagnéticas	1			1%	
[E.8] Difusión de software dañino	1	10%	10%	10%	
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%	
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	0,1	100%		100%	
[A.7] Uso no previsto	1	1%	1%	10%	
[A.8] Difusión de software dañino	1	100%	100%	100%	
[A.11] Acceso no autorizado	1	10%	10%	50%	
[A.22] Manipulación de programas	1	50%	100%	100%	
[A.23] Manipulación del hardware	0,5	50%		50%	
[A.24] Denegación de servicio	2	100%			
[A.25] Robo de equipos	0,1	100%		100%	
[A.26] Ataque destructivo	1	100%			

Valoración de las amenazas activo SWFICA2/O (SRO Servidor Opina)

AMENAZAS	**[P]**	**[D]**	**[I]**	**[C]**	**[A]**
[I.5] Avería de origen físico o lógico	1	50%			
[E.1] Errores de los usuarios	1	10%	10%	10%	
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%	
[E.3] Errores de monitorización (log)	1		1%		
[E.8] Difusión de software dañino	1	10%	10%	10%	
[E.15] Alteración de la información	1		1%		
[E.18] Destrucción de la información	1	10%			
[E.19] Fugas de información	1			10%	
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%	
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%		
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[A.3] Manipulación de los registros de actividad (log)	100		50%		
[A.5] Suplantación de la identidad	10		50%	50%	100%
[A.6] Abuso de privilegios de acceso	10	1%	10%	50%	100%

[A.7] Uso no previsto	1	1%	10%	10%	
[A.8] Difusión de software dañino	1	100%	100%	100%	
[A.11] Acceso no autorizado	100		10%	50%	100%
[A.15] Modificación de la información	10		50%		
[A.18] Destrucción de la información	1	50%			
[A.22] Manipulación de programas	1	50%	100%	100%	
[A.24] Denegación de servicio	10	50%			

Valoración de las amenazas activo SWFICA3/M (SRM Servidor Reactivos)

AMENAZAS	**[P]**	**[D]**	**[I]**	**[C]**	**[A]**
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[I.4] Contaminación electromagnética	1	10%			
[I.5] Avería de origen físico o lógico	1	50%			
[I.6] Corte del suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%			
[I.11] Emanaciones electromagnéticas	1			1%	
[E.1] Errores de los usuarios	1	10%	10%	10%	
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%	
[E.3] Errores de monitorización (log)	1		1%		
[E.8] Difusión de software dañino	1	10%	10%	10%	
[E.15] Alteración de la información	1		1%		
[E.18] Destrucción de la información	1	10%			
[E.19] Fugas de información	1			10%	
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%	
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			

[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	0,1	100%		100%	
[A.3] Manipulación de los registros de actividad (log)	100		50%		
[A.5] Suplantación de la identidad	10		50%	50%	100%
[A.6] Abuso de privilegios de acceso	10	1%	10%	50%	100%
[A.7] Uso no previsto	1	1%	10%	10%	
[A.8] Difusión de software dañino	1	100%	100%	100%	
[A.11] Acceso no autorizado	100	10%	10%	50%	100%
[A.15] Modificación de la información	10		50%		
[A.18] Destrucción de la información	1	50%			
[A.22] Manipulación de programas	1	50%	100%	100%	
[A.23] Manipulación del hardware	0,5	50%		50%	
[A.24] Denegación de servicio	10	100%			
[A.25] Robo de equipos	0,1	100%		100%	
[A.26] Ataque destructivo	1	100%			

Valoración de las amenazas activo SWFICA4/B (SRB Servidor Biométrico)

AMENAZAS	**[P]**	**[D]**	**[I]**	**[C]**	**[A]**
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[I.4] Contaminación electromagnética	1	10%			
[I.5] Avería de origen físico o lógico	1	50%			
[I.6] Corte del suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%			
[I.11] Emanaciones electromagnéticas	1			1%	
[E.1] Errores de los usuarios	1	10%	10%	10%	
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%	
[E.3] Errores de monitorización (log)	1		1%		
[E.8] Difusión de software dañino	1	10%	10%	10%	

[E.15] Alteración de la información	1		1%		
[E.18] Destrucción de la información	1	10%			
[E.19] Fugas de información	1			10%	
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%	
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	0,1	100%		100%	
[A.3] Manipulación de los registros de actividad (log)	100		50%		
[A.5] Suplantación de la identidad	10		50%	50%	100%
[A.6] Abuso de privilegios de acceso	10	1%	10%	50%	100%
[A.7] Uso no previsto	1	1%	10%	10%	
[A.8] Difusión de software dañino	1	100%	100%	100%	
[A.11] Acceso no autorizado	100	10%	10%	50%	100%
[A.15] Modificación de la información	10		50%		
[A.18] Destrucción de la información	1	50%			
[A.22] Manipulación de programas	1	50%	100%	100%	
[A.23] Manipulación del hardware	0,5	50%		50%	
[A.24] Denegación de servicio	10	100%			
[A.25] Robo de equipos	0,1	100%		100%	
[A.26] Ataque destructivo	1	100%			

Valoración de las amenazas activo HWFICA1/PV1 (Servidor HP Proxmox PV1)

AMENAZAS	**[P]**	**[D]**	**[I]**	**[C]**	**[A]**
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[I.4] Contaminación electromagnética	1	10%			
[I.5] Avería de origen físico o lógico	1	50%			
[I.6] Corte del suministro eléctrico	1	100%			

[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%			
[I.11] Emanaciones electromagnéticas	1			1%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	1	100%		100%	
[A.7] Uso no previsto	1	1%	1%	10%	
[A.11] Acceso no autorizado	1	10%	10%	50%	
[A.23] Manipulación del hardware	0,5	50%		50%	
[A.24] Denegación de servicio	2	100%			
[A.25] Robo de equipos	0,5	100%		100%	
[A.26] Ataque destructivo	1	100%			

Valoración de las amenazas activo HWFICA2/PV2 (Servidor HP Proxmox PV2)

AMENAZAS	**[P]**	**[D]**	**[I]**	**[C]**	**[A]**
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[I.4] Contaminación electromagnética	1	10%			
[I.5] Avería de origen físico o lógico	1	50%			
[I.6] Corte del suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%			
[I.11] Emanaciones electromagnéticas	1			1%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	1	100%		100%	
[A.7] Uso no previsto	1	1%	1%	10%	
[A.11] Acceso no autorizado	1	10%	10%	50%	
[A.23] Manipulación del hardware	0,5	50%		50%	
[A.24] Denegación de servicio	2	100%			

[A.25] Robo de equipos	0,5	100%		100%	
[A.26] Ataque destructivo	1	100%			

Valoración de las amenazas activo HWFICA3/PV3 (Servidor HP Proxmox PV3)

AMENAZAS	[P]	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[I.4] Contaminación electromagnética	1	10%			
[I.5] Avería de origen físico o lógico	1	50%			
[I.6] Corte del suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%			
[I.11] Emanaciones electromagnéticas	1			1%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	1	100%		100%	
[A.7] Uso no previsto	1	1%	1%	10%	
[A.11] Acceso no autorizado	1	10%	10%	50%	
[A.23] Manipulación del hardware	0,5	50%		50%	
[A.24] Denegación de servicio	2	100%			
[A.25] Robo de equipos	0,5	100%		100%	
[A.26] Ataque destructivo	1	100%			

Valoración de las amenazas activo HWFICA4/PV4 (Servidor HP Proxmox PV4)

AMENAZAS	[P]	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			

[I.4] Contaminación electromagnética	1	10%			
[I.5] Avería de origen físico o lógico	1	50%			
[I.6] Corte del suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%			
[I.11] Emanaciones electromagnéticas	1			1%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	1	100%		100%	
[A.7] Uso no previsto	1	1%	1%	10%	
[A.11] Acceso no autorizado	1	10%	10%	50%	
[A.23] Manipulación del hardware	0,5	50%		50%	
[A.24] Denegación de servicio	2	100%			
[A.25] Robo de equipos	0,5	100%		100%	
[A.26] Ataque destructivo	1	100%			

Valoración de las amenazas activo HWFICA5/SS (Servidor IBM Sin Servicio)

AMENAZAS	**[P]**	**[D]**	**[I]**	**[C]**	**[A]**
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[I.4] Contaminación electromagnética	1	10%			
[I.5] Avería de origen físico o lógico	1	50%			
[I.6] Corte del suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%			
[I.11] Emanaciones electromagnéticas	1			1%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	0,1	100%		100%	
[A.7] Uso no previsto	1	1%	1%	10%	
[A.11] Acceso no autorizado	1	10%	10%	50%	
[A.23] Manipulación del hardware	0,5	50%		50%	

[A.24] Denegación de servicio	2	100%			
[A.25] Robo de equipos	0,1	100%		100%	
[A.26] Ataque destructivo	1	100%			

Valoración de las amenazas activo HWFICA6/CS1 (Servidor IBM CISIC GEOPORTAL)

AMENAZAS	[P]	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[I.4] Contaminación electromagnética	1	10%			
[I.5] Avería de origen físico o lógico	1	50%			
[I.6] Corte del suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%			
[I.11] Emanaciones electromagnéticas	1			1%	
[E.1] Errores de los usuarios	1	10%	10%	10%	
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%	
[E.8] Difusión de software dañino	1	10%	10%	10%	
[E.15] Alteración de la información	1		1%		
[E.18] Destrucción de la información	1	10%			
[E.19] Fugas de información	1			10%	
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%	
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	0,1	100%		100%	
[A.5] Suplantación de la identidad	10		50%	50%	100%
[A.6] Abuso de privilegios de acceso	10	1%	10%	50%	100%
[A.7] Uso no previsto	1	1%	10%	10%	
[A.8] Difusión de software dañino	1	100%	100%	100%	
[A.11] Acceso no autorizado	100	10%	10%	50%	100%

[A.15] Modificación de la información	10		50%		
[A.18] Destrucción de la información	1	50%			
[A.22] Manipulación de programas	1	50%	100%	100%	
[A.23] Manipulación del hardware	0,5	50%		50%	
[A.24] Denegación de servicio	10	100%			
[A.25] Robo de equipos	0,1	100%		100%	
[A.26] Ataque destructivo	1	100%			

Valoración de las amenazas activo HWFICA7/CS2 (Servidor IBM CISIC PRUEBAS)

AMENAZAS	**[P]**	**[D]**	**[I]**	**[C]**	**[A]**
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[I.4] Contaminación electromagnética	1	10%			
[I.5] Avería de origen físico o lógico	1	50%			
[I.6] Corte del suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%			
[I.11] Emanaciones electromagnéticas	1			1%	
[E.1] Errores de los usuarios	1	10%	10%	10%	
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%	
[E.8] Difusión de software dañino	1	10%	10%	10%	
[E.15] Alteración de la información	1		1%		
[E.18] Destrucción de la información	1	10%			
[E.19] Fugas de información	1			10%	
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%	
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	0,1	100%		100%	
[A.5] Suplantación de la identidad	10		50%	50%	100%

[A.6] Abuso de privilegios de acceso	10	1%	10%	50%	100%
[A.7] Uso no previsto	1	1%	10%	10%	
[A.8] Difusión de software dañino	1	100%	100%	100%	
[A.11] Acceso no autorizado	100	10%	10%	50%	100%
[A.15] Modificación de la información	10		50%		
[A.18] Destrucción de la información	1	50%			
[A.22] Manipulación de programas	1	50%	100%	100%	
[A.23] Manipulación del hardware	0,5	50%		50%	
[A.24] Denegación de servicio	10	100%			
[A.25] Robo de equipos	0,1	100%		100%	
[A.26] Ataque destructivo	1	100%			

Valoración de las amenazas activo HWFICA8/SWC (Switch CORE)

AMENAZAS	**[P]**	**[D]**	**[I]**	**[C]**	**[A]**
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[I.4] Contaminación electromagnética	1	10%			
[I.5] Avería de origen físico o lógico	1	50%			
[I.6] Corte del suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%			
[I.11] Emanaciones electromagnéticas	1			1%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	1	20%			
[A.7] Uso no previsto	1	10%		10%	
[A.11] Acceso no autorizado	1	10%	10%	50%	
[A.23] Manipulación del hardware	0,5	100%		50%	
[A.24] Denegación de servicio	2	100%			
[A.25] Robo de equipos	0,5	20%			
[A.26] Ataque destructivo	1	100%			

Valoración de las amenazas activo HWFICA9/RTM (Router MikroTik)

AMENAZAS	[P]	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[I.4] Contaminación electromagnética	1	10%			
[I.5] Avería de origen físico o lógico	1	50%			
[I.6] Corte del suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%			
[I.11] Emanaciones electromagnéticas	1			1%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	1	20%			
[A.7] Uso no previsto	1	10%		10%	
[A.11] Acceso no autorizado	1	10%	10%	50%	
[A.23] Manipulación del hardware	0,5	100%		50%	
[A.24] Denegación de servicio	2	100%			
[A.25] Robo de equipos	0,5	20%			
[A.26] Ataque destructivo	1	100%			

Valoración de las amenazas activo HWFICA10/SWD1 (Switch Distribución 1 Conectado a Proxmox y Radius)

AMENAZAS	[P]	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[I.4] Contaminación electromagnética	1	10%			
[I.5] Avería de origen físico o lógico	1	50%			

[I.6] Corte del suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%			
[I.11] Emanaciones electromagnéticas	1			1%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	1	20%			
[A.7] Uso no previsto	1	10%		10%	
[A.11] Acceso no autorizado	1	10%	10%	50%	
[A.23] Manipulación del hardware	0,5	100%		50%	
[A.24] Denegación de servicio	2	100%			
[A.25] Robo de equipos	0,5	20%			
[A.26] Ataque destructivo	1	100%			

Valoración de las amenazas activo HWFICA11/SWQP (Switch QPCom Red Wifi FICA)

AMENAZAS	**[P]**	**[D]**	**[I]**	**[C]**	**[A]**
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[I.4] Contaminación electromagnética	1	10%			
[I.5] Avería de origen físico o lógico	1	50%			
[I.6] Corte del suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%			
[I.11] Emanaciones electromagnéticas	1			1%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	1	20%			
[A.7] Uso no previsto	1	10%		10%	
[A.11] Acceso no autorizado	1	10%	10%	50%	
[A.23] Manipulación del hardware	0,5	100%		50%	
[A.24] Denegación de servicio	2	100%			

[A.25] Robo de equipos	0,5	20%			
[A.26] Ataque destructivo	1	100%			

Valoración de las amenazas activo HWFICA12/SWD2 (Switch Distribucion 2 Conectado a Servidores CISIC)

AMENAZAS	[P]	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[I.4] Contaminación electromagnética	1	10%			
[I.5] Avería de origen físico o lógico	1	50%			
[I.6] Corte del suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%			
[I.11] Emanaciones electromagnéticas	1			1%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	1	20%			
[A.7] Uso no previsto	1	10%		10%	
[A.11] Acceso no autorizado	1	10%	10%	50%	
[A.23] Manipulación del hardware	0,5	100%		50%	
[A.24] Denegación de servicio	2	100%			
[A.25] Robo de equipos	0,5	20%			
[A.26] Ataque destructivo	1	100%			

Valoración de las amenazas activo HWFICA12/SWD3 (Switch Distribución 3 Conectado a Servidores de Torre)

AMENAZAS	[P]	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			

[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[I.4] Contaminación electromagnética	1	10%			
[I.5] Avería de origen físico o lógico	1	50%			
[I.6] Corte del suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%			
[I.11] Emanaciones electromagnéticas	1			1%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	1	20%			
[A.7] Uso no previsto	1	10%		10%	
[A.11] Acceso no autorizado	1	10%	10%	50%	
[A.23] Manipulación del hardware	0,5	100%		50%	
[A.24] Denegación de servicio	2	100%			
[A.25] Robo de equipos	0,5	20%			
[A.26] Ataque destructivo	1	100%			

Valoración de las amenazas activo EAFICA1/SE (Sistema Eléctrico)

AMENAZAS	**[P]**	**[D]**	**[I]**	**[C]**	**[A]**
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[A.7] Uso no previsto	1	10%			
[A.23] Manipulación del hardware	1	10%			
[A.25] Robo de equipos	0,5	100%			
[A.26] Ataque destructivo	1	100%			

Valoración de las amenazas activo EAFICA2/AA (Aire Acondicionado)

AMENAZAS	[P]	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	10%			
[N.2] Daños por agua	0,1	10%			
[N.*] Desastres naturales	0,1	10%			
[I.1] Fuego	0,5	10%			
[I.2] Daños por agua	0,5	10%			
[I.*] Desastres industriales	0,5	10%			
[I.3] Contaminación medioambiental	0,1	10%			
[I.6] Corte del suministro eléctrico	1	10%			
[I.9] Interrupción de otros servicios o suministros esenciales	1	10%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[A.7] Uso no previsto	1	10%			
[A.23] Manipulación del hardware	1	10%			
[A.25] Robo de equipos	0,5	10%			
[A.26] Ataque destructivo	1	10%			

Valoración de las amenazas activo EAFICA3/UPS (Sistema de Alimentación Interrumpida)

AMENAZAS	[P]	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	1%			
[N.2] Daños por agua	0,1	1%			
[N.*] Desastres naturales	0,1	1%			
[I.1] Fuego	0,5	1%			
[I.2] Daños por agua	0,5	1%			
[I.*] Desastres industriales	0,5	1%			
[I.3] Contaminación medioambiental	0,1	1%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	1%			
[A.7] Uso no previsto	1	1%			
[A.23] Manipulación del hardware	1	1%			
[A.25] Robo de equipos	0,5	1%			
[A.26] Ataque destructivo	1	1%			

Valoración de las amenazas activo EAFICA4/CS (Cámara de Seguridad)

AMENAZAS	[P]	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	100%			

[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[A.7] Uso no previsto	1	50%	1%	1%	
[A.23] Manipulación del hardware	1	50%		50%	
[A.25] Robo de equipos	0,5	10%			
[A.26] Ataque destructivo	1	10%			

Valoración de las amenazas activo EAFICA5/CA (Control de Acceso)

AMENAZAS	**[P]**	**[D]**	**[I]**	**[C]**	**[A]**
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[A.7] Uso no previsto	1	50%	1%	1%	
[A.23] Manipulación del hardware	1	50%		50%	
[A.25] Robo de equipos	0,5	10%			
[A.26] Ataque destructivo	1	10%			

Valoración de las amenazas activo EAFICA6/BB (Backbone)

AMENAZAS	**[P]**	**[D]**	**[I]**	**[C]**	**[A]**
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			

[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[A.7] Uso no previsto	1	50%	1%	1%	
[A.23] Manipulación del hardware	1	50%		50%	
[A.25] Robo de equipos	0,8	100%		0	
[A.26] Ataque destructivo	1	100%			

Valoración de las amenazas activo EAFICA7/CE (Cableado Estructurado)

AMENAZAS	**[P]**	**[D]**	**[I]**	**[C]**	**[A]**
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[N.*] Desastres naturales	0,1	100%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[I.4] Contaminación electromagnética	0,5	10%			
[I.11] Emanaciones electromagnéticas	1			1%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[A.7] Uso no previsto	1	50%	1%	1%	
[A.11] Acceso no autorizado	1		10%	50%	
[A.23] Manipulación del hardware	1	50%		50%	
[A.25] Robo de equipos	0,8	100%		0	
[A.26] Ataque destructivo	1	100%			

Anexo 8: Tratamiento del Riesgo

1. Objetivo:

Seleccionar las opciones de tratamiento de riesgos por cada una de las amenazas identificadas en el Análisis de Riesgos, presentado los resultados en grupos de activos en base a la Metodología de Análisis y Gestión de Riesgos Tecnológicos (Magerit).

2. Inventario de activos de información

El presente análisis incluye 26 activos ordenados en base al grupo de activos descritos en la Metodología Magerit.

ACTIVOS DEL DATACENTER FICA - UTN		
Esenciales		
Código	**Nombre**	**Detalle**
ESFICA1/RU	RU	IBM Systemx3500 M4 Revista Universitaria
ESFICA2/SRR	SRR	Servidor Radius
Equipos informáticos (Hardware)		
Código	**Nombre**	**Detalle**
HWFICA1/PV1	HPPV1	HP Proliant DL360 G9 (Proxmox PV1)
HWFICA2/PV2	HPPV2	HP Proliant DL360 G9 (Proxmox PV2)
HWFICA3/PV3	HPPV3	HP Proliant DL360 G9 (Proxmox PV3)
HWFICA4/PV4	HPPV4	HP Proliant ML150 (Proxmox PV4)

HWFICA5/SS	IBMSS	IBM System x3650 M3 (Sin Servicio)
HWFICA6/CS1	IBMCS1	IBM System x3250 M3 (CISIC)
HWFICA7/CS2	IBMCS2	IBM System x3250 (CISIC)
HWFICA8/SWC	CORE	Switch de Core Catalyst 4506-E
HWFICA9/RTM	ROUTER	RouterBoard 1100AHX2 Mikrotik
HWFICA10/SWD1	SWD1	Switch de Distribución 3Com 4500G PROXMOX
HWFICA11/SWQP	SWQP	Switch de distribución inalámbrica QPCOM
HWFICA12/SWD2	SWD2	Switch de distribución CISCO Linksys SR224G
HWFICA13/SWD3	SWD3	Switch de Distribución 3Com 3226 SERVIDORES
Aplicaciones informáticas (Software)		
Código	**Nombre**	**Detalle**
SWFICA1/P	SRP	Proxmox
SWFICA2/O	SRO	Opina
SWFICA3/M	SRM	Reactivos o moodle
SWFICA4/B	SRB	PC tipo Clon H8M-S1
Elementos Auxiliar		
Código	**Nombre**	**Detalle**
EAFICA1/SE	SE	Sistema Eléctrico

EAFICA2/AA	AA	Aire Acondicionado
EAFICA3/UPS	UPS	UPS
EAFICA4/CS	CS	Cámara de Seguridad
EAFICA5/CA	CA	Control de Acceso
EAFICA6/BB	BB	Backbone
EAFICA7/CU	CE	Cableado Estructurado

3. Resultados

Para cada grupo de activos de información se ha seleccionado la opción de tratamiento de riesgo en base a lo descrito en la Metodología de Análisis y Gestión de Riesgos Tecnológicos (Magerit):

Eliminación: El proceso de eliminación implica prescindir de ciertos elementos de la red, pero que esto no altere los objetivos de la Organización. Existen dos opciones de como ejecutar este proceso:

- Eliminar cierto activo y emplear otro en su lugar.
- Reordenar la arquitectura del sistema, para de esta forma cambiar el valor acumulado en ciertos activos.

Mitigación

La mitigación del riesgo se refiere a una de dos opciones:

- Reducir la degradación causada por una amenaza

- Reducir la probabilidad de que una amenaza de materializa

En las dos opciones la solución es mejorar el conjunto de salvaguardas. En algunas ocasiones subir el nivel de las salvaguardas implica el despliegue de más equipos, lo que esto se convierte en un nuevo activo, y se deberá realizar un nuevo análisis de riesgo para cerciorarse que el riesgo sea menor que del sistema original.

Compartición: Este proceso consiste en transferir el riesgo de forma total o parcial. En ocasiones la empresa no tiene la capacidad de tratamiento y precisa la contratación de un tercero con capacidad para reducir y gestionar el riesgo.

Financiación: En este proceso se requiere que la organización debe estar preparada financieramente para cuando haya que responder por las consecuencias de una amenaza materializada.

En la tabla que se muestra a continuación se detalla las vulnerabilidades y riesgos a los que se enfrenta cada activo según la amenaza a la que está expuesto.

IDENTIFICACION DE VULNERABILIDADES Y RIESGOS

AMENAZA	VULNERABILIDAD	RIESGO
[N.1] Fuego	Carencia de garantía de los equipos.	Indisponibilidad total o parcial
	Archivos de respaldo de configuración inexistentes.	Imposibilidad de restauración de los servicios
[N.2] Daños por agua	Carencia de garantía de los equipos.	Daño total o parcial
	Ingreso de agua a componentes internos	Cortocircuito
[N.*] Desastres naturales	Ubicación en un área susceptible a daños físicos	Pérdida total o parcial
	Carencia de garantía de los equipos.	
[I.1] Fuego	Deficiencias en la protección física de equipos	Destrucción del equipo
	Carencia de garantía de los equipos.	
[I.2] Daños por agua	Carencia de garantía de los equipos.	Daño total o parcial
	Ingreso de agua a componentes internos	Cortocircuito
		Daño total o parcial

[I.*] Desastres industriales	Falta de procedimientos en operación y mantenimiento.	
[I.3] Contaminación medioambiental	Falta de procedimientos de tratamiento de contaminación ambiental	Afectación en el normal funcionamiento de los equipos del Data Center
[I.4] Contaminación electromagnética	Falta de procedimientos en operación y mantenimiento.	Afectación en el normal funcionamiento de los equipos del Data Center
[I.5] Avería de origen físico o lógico	Carencia de garantía de los equipos.	Indisponibilidad total o parcial
	Fallas por software	Funcionamiento errático
	Daño de los componentes internos	Fallos de los servicios
[I.6] Corte del suministro eléctrico	Archivos de respaldo de configuración inexistentes	No sea posible recuperar el funcionamiento normal
	Sensibilidad a interrupciones del servicio eléctrico	Avería de componentes internos
[I.7] Condiciones inadecuadas de temperatura o humedad	Falta de procedimientos en operación y mantenimiento.	Afectación en el normal funcionamiento de los equipos del Data Center
[I.11] Emanaciones electromagnéticas	Falta de procedimientos de tratamiento de contaminación ambiental	Afectación en el normal funcionamiento de los equipos del Data Center
[E.1] Errores de los usuarios	Errores intencionados o no intencionados	Modificación/Destrucción de información
	Falta de conocimiento en el uso de servicios	
[E.2] Errores del administrador del sistema / de la seguridad	Funciones dedicadas exclusivamente al sistema	Pérdida de información o falla de los sistemas
[E.3] Errores de monitorización (log)	No existe monitorización con frecuencia	Pérdida de datos importantes de monitorización
[E.4] Errores de configuración	Archivos de respaldo de configuración inexistentes	No sea posible recuperar el funcionamiento normal
	Falta de conocimiento cuando existen cambios de configuración	Pérdida de las funciones operativas parcial o total
[E.8] Difusión de software dañino	Software que afecte funcionalidades operativas	Infección de software malicioso en activos de información
	Falta de un procedimiento de control ante incidencias de seguridad	Infección en equipos
[E.15] Alteración de la información	Errores intencionados o no intencionadas	Alteración de información permanente de información
[E.18] Destrucción de la información	Errores intencionados o no intencionadas	Destrucción de información permanente de información
[E.19] Fugas de información	Falta de un procedimiento de detección de fallas de seguridad	Publicación de información sensible
[E.20] Vulnerabilidades de los programas (software)	Vulnerabilidades de las versiones de software	Ingreso no autorizado a los sistemas de información
		Sustracción de información sensible
		Cambios no autorizados en la configuración
[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de procedimientos en operación y mantenimiento.	Pérdida de las funciones operativas parcial o total

[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de procedimientos en operación y mantenimiento.	Afectación en el normal funcionamiento de los equipos del Data Center
[E.24] Caída del sistema por agotamiento de recursos	Falta de procedimientos en operación y mantenimiento.	Pérdida de información sensible
		Inoperatividad de los sistemas y servicios
[E.25] Pérdida de equipos	Falta de un control o verificación de equipo en Data Center	Pérdida de información sensible
		Pérdida del equipo informático
[A.3] Manipulación de los registros de actividad (log)	Falta de un responsable de la administración del sistema	Pérdida de datos importantes de monitorización
	No se revisa los datos de monitorización.	
[A.4] Manipulación de los ficheros de configuración	Falta de un responsable de la administración del sistema	Pérdida de datos importantes de configuración
[A.5] Suplantación de la identidad	No existe el adecuado manejo de credenciales	Destrucción, modificación, robo o pérdida de información
[A.6] Abuso de privilegios de acceso	No están bien definidas las funciones	Destrucción, modificación, robo o pérdida de información
[A.7] Uso no previsto	Falta políticas o normativas de acciones permitidas	Destrucción de la información por acciones no autorizadas
[A.8] Difusión de software dañino	Software que afecte funcionalidades operativas	Infección de software malicioso en activos de información
	Falta de un procedimiento de control ante incidencias de seguridad	Pérdida parcial o total de la información
[A.11] Acceso no autorizado	Falta de medio de verificación de autenticidad	Destrucción, modificación, robo o pérdida de información
[A.15] Modificación de la información	Falta de un responsable de la administración del sistema	Pérdida total o parcial de la información
[A.18] Destrucción de la información	Falta de archivos de configuración	Pérdida total o parcial de la información
[A.22] Manipulación de programas	Falta políticas o normativas de acciones permitidas	Destrucción de la información por acciones no autorizadas
[A.23] Manipulación del hardware	Falta de un control o verificación de equipo en Data Center	Perdida de equipos físico y de la información.
[A.24] Denegación de servicio	Falta de un procedimiento de control ante incidencias de seguridad	Indisponibilidad operativa de sistemas
		No disponibilidad de la información
[A.25] Robo de equipos	Falta de un control o verificación de equipo en Data Center	Pérdida de información sensible
		Pérdida del equipo informático
[A.26] Ataque destructivo	Ubicación en un área susceptible a daños físicos	Pérdida total o parcial

En las tablas que se presentan a continuación se detalla las amenazas por cada grupo de activo, y el tratamiento que se le dará, luego de haber evaluado las vulnerabilidades y los riesgos a los

que se exponen se proponen controles basados en la ISO 27002, lo cuales mejoraran la seguridad del Data Center.

GRUPO ACTIVOS: Esenciales

AMENAZAS/VULNERABILIDADES	RIESGO NO ACEPTABLE C, I, D o A	TRATAMIENTO	CONTROLES SELECCIONADOS
[N.1] Fuego	D	Mitigación Compartición	9.1, 9.2, 11.2, 6.1.7
[N.2] Daños por agua	D	Mitigación Compartición	9.1, 9.2, 11.2, 6.1.7
[N.*] Desastres naturales	D	Mitigación Compartición	5.1.1, 6.1.7, 9.1, 9.2, 15.2
[I.1] Fuego	D	Mitigación Compartición	9.1, 9.2, 11.2, 6.1.5, 11.3, 13.1
[I.2] Daños por agua	D	Mitigación Compartición	9.1, 9.2, 11.2, 6.1.5, 11.3, 13.1
[I.*] Desastres industriales	D	Mitigación Compartición	5.1.1, 15.2
[I.3] Contaminación medioambiental	D	Mitigación Compartición	9.1, 9.2, 13.1
[I.4] Contaminación electromagnética	D	Compartición	6.1.7
[I.5] Avería de origen físico o lógico	D	Mitigación Compartición	9.1, 9.2, 11.2
[I.6] Corte del suministro eléctrico	D	Mitigación	9.1, 9.2, 10.1, 11.2, 13.1
[I.7] Condiciones inadecuadas de temperatura o humedad	D	Mitigación	6.1.7, 6.1.6, 9.1, 9.2
[I.11] Emanaciones electromagnéticas	C	Compartición	6.1.7
[E.1] Errores de los usuarios	D, I, C	Mitigación	5.1.1, 15.2, 6.1.5, 8.2, 10, 11
[E.2] Errores del administrador del sistema / de la seguridad	D, I, C	Mitigación	5.1.1, 15.2, 6.1.3, 6.1.5, 7.1, 8.2, 10
[E.3] Errores de monitorización (log)	I	Mitigación	6.1.5
[E.4] Errores de configuración	I	Mitigación	5.1.1, 15.2, 6.1.3, 6.1.5, 7.1, 10, 13.1
[E.8] Difusión de software dañino	D, I, C	Mitigación Eliminación	5.1.1, 15.2, 9.2, 10.4,
[E.15] Alteración de la información	I	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 6.1.5, 8.3, 11
[E.18] Destrucción de la información	D	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 8.3, 11
[E.19] Fugas de información	C	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 6.1.5, 8.3, 11
[E.20] Vulnerabilidades de los programas (software)	D, I, C	Mitigación Eliminación	5.1.1, 15.2, 6.1.3, 7.1, 8.2
[E.21] Errores de mantenimiento / actualización de programas (software)	D, I	Mitigación	6.1.3, 7.1, 10

[E.23] Errores de mantenimiento / actualización de equipos (hardware)	D	Mitigación	6.1.3, 7.1, 9.2, 10
[E.24] Caída del sistema por agotamiento de recursos	D	Mitigación	6.1.3, 7.1, 10
[E.25] Pérdida de equipos	D, C	Mitigación Compartición	6.1.1, 6.1.3, 6.1.5, 7.1, 8.2, 8.3
[A.3] Manipulación de los registros de actividad (log)	I	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 6.1.5, 7.1, 8.3, 10, 11
[A.4] Manipulación de los ficheros de configuración	D, I, C	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 6.1.5, 7.1, 8.3, 10, 11
[A.5] Suplantación de la identidad	I, C, A	Mitigación	5.1.1, 15.2, 6.1.3, 8.2, 11.2
[A.6] Abuso de privilegios de acceso	D, I, C, A	Mitigación	6.1.1, 6.1.3, 8.3, 10, 11.2
[A.7] Uso no previsto	D, I, C	Mitigación	5.1.1, 15.2, 6.1.3, 8.3, 10
[A.8] Difusión de software dañino	D, I, C	Mitigación Eliminación	5.1.1, 15.2, 6.1.1, 10.4
[A.11] Acceso no autorizado	D, I, C, A	Mitigación	5.1.1, 15.2, 6.1.3, 7.1, 8.2, 9.1, 9.2, 11.2
[A.15] Modificación de la información	I	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 8.3
[A.18] Destrucción de la información	D	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 8.3
[A.22] Manipulación de programas	D, I, C	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 8.3
[A.23] Manipulación del hardware	D, C	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 8.3
[A.24] Denegación de servicio	D	Mitigación Eliminación	6.1.1, 8.2
[A.25] Robo de equipos	D, C	Mitigación	6.1.1, 6.1.3, 7.1, 9.1, 9.2
[A.26] Ataque destructivo	D	Mitigación	6.1.1, 6.1.3, 7.1, 9.1, 9.2

GRUPO ACTIVOS: Equipos Informáticos (Hardware)

AMENAZAS/VULNERABILIDADES	RIESGO NO ACEPTABLE C, I, D o A	TRATAMIENTO	CONTROLES SELECCIONADOS
[N.1] Fuego	D	Mitigación Compartición	9.1, 9.2, 11.2, 6.1.7
[N.2] Daños por agua	D	Mitigación Compartición	9.1, 9.2, 11.2, 6.1.7
[N.*] Desastres naturales	D	Mitigación Compartición	5.1.1, 6.1.7, 9.1, 9.2, 15.2

[I.1] Fuego	D	Mitigación Compartición	9.1, 9.2, 11.2, 6.1.5, 11.3, 13.1
[I.2] Daños por agua	D	Mitigación Compartición	9.1, 9.2, 11.2, 6.1.5, 11.3, 13.1
[I.*] Desastres industriales	D	Mitigación Compartición	5.1.1, 15.2
[I.3] Contaminación medioambiental	D	Mitigación Compartición	9.1, 9.2, 13.1
[I.4] Contaminación electromagnética	D	Compartición	6.1.7
[I.5] Avería de origen físico o lógico	D	Mitigación Compartición	9.1, 9.2, 11.2
[I.6] Corte del suministro eléctrico	D	Mitigación	9.1, 9.2, 10.1, 11.2, 13.1
[I.7] Condiciones inadecuadas de temperatura o humedad	D	Mitigación	6.1.7, 6.1.6, 9.1, 9.2
[I.11] Emanaciones electromagnéticas	C	Compartición	6.1.7
[E.1] Errores de los usuarios	D, I, C	Mitigación	5.1.1, 15.2, 6.1.5, 8.2, 10, 11
[E.2] Errores del administrador del sistema / de la seguridad	D, I, C	Mitigación	5.1.1, 15.2, 6.1.3, 6.1.5, 7.1, 8.2, 10
[E.8] Difusión de software dañino	D, I, C	Mitigación Eliminación	5.1.1, 15.2, 9.2, 10.4
[E.15] Alteración de la información	I	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 6.1.5, 8.3, 11
[E.18] Destrucción de la información	D	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 8.3, 11
[E.19] Fugas de información	C	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 6.1.5, 8.3, 11
[E.20] Vulnerabilidades de los programas (software)	D, I, C	Mitigación Eliminación	6.1.3, 7.1, 10
[E.21] Errores de mantenimiento / actualización de programas (software)	D, I	Mitigación	6.1.3, 7.1, 10
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	D	Mitigación	6.1.3, 7.1, 9.2, 10
[E.24] Caída del sistema por agotamiento de recursos	D	Mitigación	6.1.3, 7.1, 10
[E.25] Pérdida de equipos	D, C	Mitigación Compartición	6.1.1, 6.1.3, 6.1.5, 7.1, 8.2, 8.3
[A.5] Suplantación de la identidad	I, C, A	Mitigación	5.1.1, 15.2, 6.1.3, 8.2, 11.2

[A.6] Abuso de privilegios de acceso	D, I, C, A	Mitigación	6.1.1, 6.1.3, 8.3, 10, 11.2
[A.7] Uso no previsto	D, I, C	Mitigación	5.1.1, 15.2, 6.1.3, 8.3, 10
[A.8] Difusión de software dañino	D, I, C	Mitigación Eliminación	5.1.1, 15.2, 6.1.1, 10.4
[A.11] Acceso no autorizado	D, I, C, A	Mitigación	5.1.1, 15.2, 6.1.3, 7.1, 8.2, 9.1, 9.2, 11.2
[A.15] Modificación de la información	I	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 8.3
[A.18] Destrucción de la información	D	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 8.3
[A.22] Manipulación de programas	D, C	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 8.3
[A.23] Manipulación del hardware	D, C	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 8.3
[A.24] Denegación de servicio	D	Mitigación Eliminación	6.1.1, 8.2
[A.25] Robo de equipos	D, C	Mitigación	6.1.1, 6.1.3, 7.1, 9.1, 9.2
[A.26] Ataque destructivo	D	Mitigación	6.1.1, 6.1.3, 7.1, 9.1, 9.2

GRUPO ACTIVOS: Aplicaciones informáticas (Software)

AMENAZAS/VULNERABILIDADES	RIESGO NO ACEPTABLE C, I, D o A	TRATAMIENTO	CONTROLES SELECCIONADOS
[N.1] Fuego	D	Mitigación Compartición	9.1, 9.2, 11.2, 6.1.7
[N.2] Daños por agua	D	Mitigación Compartición	9.1, 9.2, 11.2, 6.1.7
[N.*] Desastres naturales	D	Mitigación Compartición	5.1.1, 6.1.7, 9.1, 9.2, 15.2
[I.1] Fuego	D	Mitigación Compartición	9.1, 9.2, 11.2, 6.1.5, 11.3, 13.1
[I.2] Daños por agua	D	Mitigación Compartición	9.1, 9.2, 11.2, 6.1.5, 11.3, 13.1
[I.*] Desastres industriales	D	Mitigación Compartición	5.1.1, 15.2
[I.3] Contaminación medioambiental	D	Mitigación Compartición	9.1, 9.2, 13.1

[I.4] Contaminación electromagnética	D	Compartición	6.1.7
[I.5] Avería de origen físico o lógico	D	Mitigación Compartición	9.1, 9.2, 11.2
[I.6] Corte del suministro eléctrico	D	Mitigación	9.1, 9.2, 10.1, 11.2, 13.1
[I.7] Condiciones inadecuadas de temperatura o humedad	D	Mitigación	6.1.7, 6.1.6, 9.1, 9.2
[I.11] Emanaciones electromagnéticas	C	Compartición	6.1.7
[E.1] Errores de los usuarios	D, I, C	Mitigación	5.1.1, 15.2, 6.1.5, 8.2, 10, 11
[E.2] Errores del administrador del sistema / de la seguridad	D, I, C	Mitigación	5.1.1, 15.2, 6.1.3, 6.1.5, 7.1, 8.2, 10
[E.3] Errores de monitorización (log)	I	Mitigación	6.1.5
[E.8] Difusión de software dañino	D, I, C	Mitigación Eliminación	5.1.1, 15.2, 9.2, 10.4
[E.15] Alteración de la información	I	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 6.1.5, 8.3, 11
[E.18] Destrucción de la información	D	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 8.3, 11
[E.19] Fugas de información	C	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 6.1.5, 8.3, 11
[E.20] Vulnerabilidades de los programas (software)	D, I, C	Mitigación Eliminación	5.1.1, 15.2, 6.1.3, 7.1, 8.2
[E.21] Errores de mantenimiento / actualización de programas (software)	D, I	Mitigación	6.1.3, 7.1, 10
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	D	Mitigación	6.1.3, 7.1, 9.2, 10
[E.24] Caída del sistema por agotamiento de recursos	D	Mitigación	6.1.3, 7.1, 10
[E.25] Pérdida de equipos	D, C	Mitigación Compartición	6.1.1, 6.1.3, 6.1.5, 7.1, 8.2, 8.3
[A.3] Manipulación de los registros de actividad (log)	I	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 6.1.5, 7.1, 8.3, 10, 11
[A.5] Suplantación de la identidad	I, C, A	Mitigación	5.1.1, 15.2, 6.1.3, 8.2, 11.2
[A.6] Abuso de privilegios de acceso	D, I, C, A	Mitigación	6.1.1, 6.1.3, 8.3, 10, 11.2
[A.7] Uso no previsto	D, I, C	Mitigación	5.1.1, 15.2, 6.1.3, 8.3, 10

[A.8] Difusión de software dañino	D, I, C	Mitigación Eliminación	5.1.1, 15.2, 6.1.1, 10.4
[A.11] Acceso no autorizado	D, I, C, A	Mitigación	5.1.1, 15.2, 6.1.3, 7.1, 8.2, 9.1, 9.2, 11.2
[A.15] Modificación de la información	I	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 8.3
[A.18] Destrucción de la información	D	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 8.3
[A.22] Manipulación de programas	D, I, C	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 8.3
[A.23] Manipulación del hardware	D, C	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 8.3
[A.24] Denegación de servicio	D	Mitigación Eliminación	6.1.1, 8.2
[A.25] Robo de equipos	D, C	Mitigación	6.1.1, 6.1.3, 7.1, 9.1, 9.2
[A.26] Ataque destructivo	D	Mitigación	6.1.1, 6.1.3, 7.1, 9.1, 9.2

GRUPO ACTIVOS: Elementos Auxiliar

AMENAZAS/VULNERABILIDADES	RIESGO NO ACEPTABLE C, I, D o A	TRATAMIENTO	CONTROLES SELECCIONADOS
[N.1] Fuego	D	Mitigación	9.1, 9.2, 11.2, 6.1.7
[N.2] Daños por agua	D	Mitigación	9.1, 9.2, 11.2, 6.1.7
[N.*] Desastres naturales	D	Mitigación	5.1.1, 6.1.7, 9.1, 9.2, 15.2
[I.1] Fuego	D	Mitigación	9.1, 9.2, 11.2, 6.1.5, 11.3, 13.1
[I.2] Daños por agua	D	Mitigación	9.1, 9.2, 11.2, 6.1.5, 11.3, 13.1
[I.*] Desastres industriales	D	Mitigación Financiación	5.1.1, 15.2
[I.3] Contaminación medioambiental	D	Mitigación	9.1, 9.2, 13.1
[I.4] Contaminación electromagnética	D	Mitigación	6.1.7
[I.6] Corte del suministro eléctrico	D	Mitigación	9.1, 9.2, 10.1, 11.2, 13.1
[I.11] Emanaciones electromagnéticas	I, C	Mitigación	6.1.7

[E.23] Errores de mantenimiento / actualización de equipos (hardware)	D	Mitigación Financiación	6.1.3, 7.1, 9.2, 10
[A.7] Uso no previsto	D, I, C	Mitigación	5.1.1, 15.2, 6.1.3, 8.3, 10
[A.11] Acceso no autorizado	I, C	Mitigación	5.1.1, 15.2, 6.1.3, 7.1, 8.2, 9.1, 9.2, 11.2
[A.23] Manipulación del hardware	D, C	Mitigación	5.1.1, 15.2, 6.1.1, 6.1.3, 8.3
[A.25] Robo de equipos	DD	Mitigación Financiación	6.1.1, 6.1.3, 7.1, 9.1, 9.2
[A.26] Ataque destructivo	D	Mitigación Financiación	6.1.1, 6.1.3, 7.1, 9.1, 9.2

Anexo 9: Indicadores de la Mejora de la Seguridad

Se presenta el resumen de los valores del impacto y riesgo, con la finalidad de saber en que porcentaje mejoró la seguridad de la información.

INDICADOR: IMPACTO

SIN SALVAGUARDAS				
PRINCIPIOS DE LA SEGURIDAD	**ACTIVOS**			
	Esenciales	*Equipos Informáticos (Hardware)*	*Aplicaciones Informáticas (Software)*	*Elementos Auxiliares*
Disponibilidad	9	9	10	9
Integridad	9	9	9	6
Confidencialidad	7	8	7	6
Autenticidad	9	9	3	
CON SALVAGUARDAS				
Disponibilidad	5	5	6	5
Integridad	4	4	4	2
Confidencialidad	3	4	3	2
Autenticidad	5	2	1	

Nomenclatura utilizada:

D: Disponibilidad

DM: Disponibilidad Mejorada

I: Integridad

IM: Integridad Mejorada

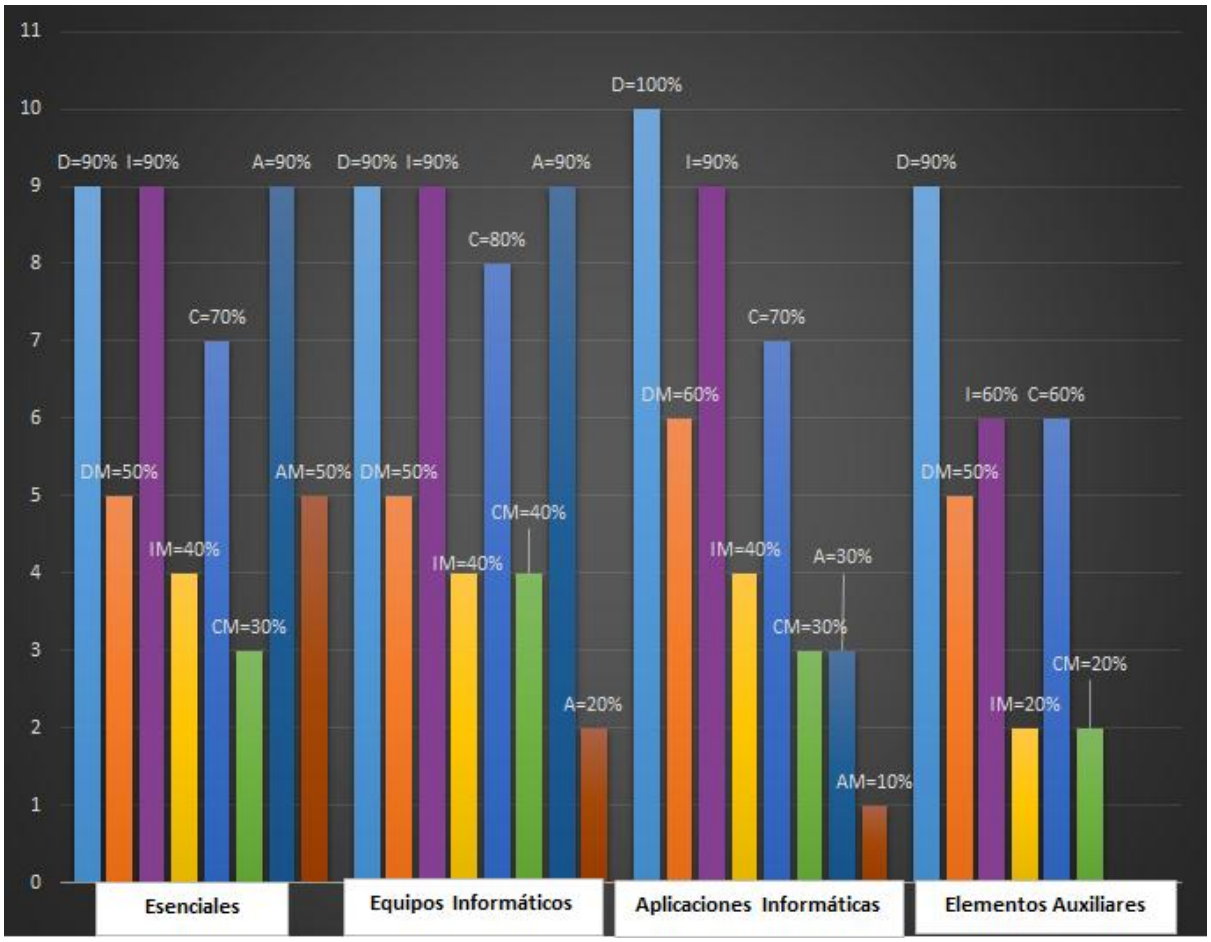
C: Confidencialidad

CM: Confidencialidad Mejorada

A: Autenticidad

AM: Autenticidad Mejorada

Representación gráfica:



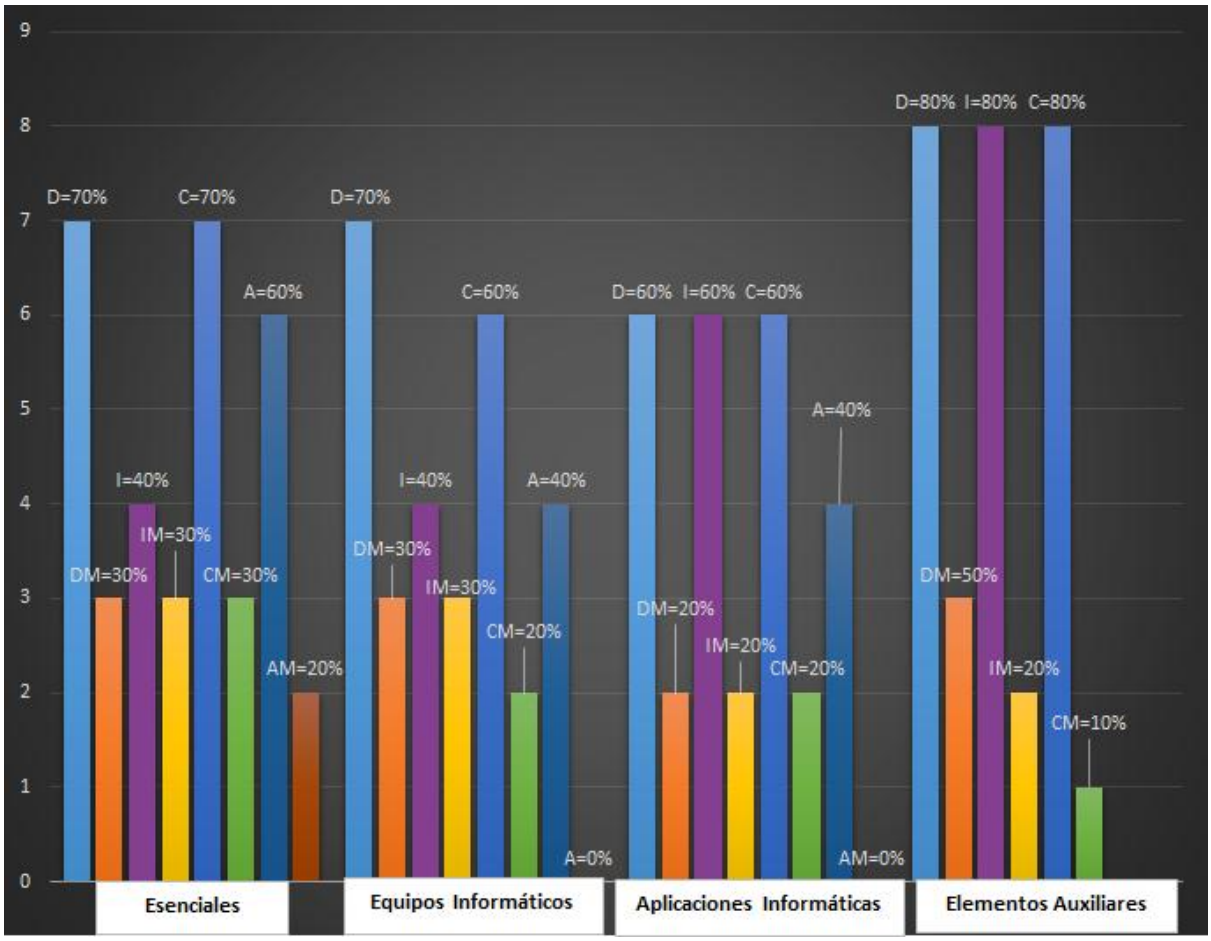
Interpretación:

En la figura anterior se muestran los porcentajes del impacto ocasionado en cada principios de seguridad (Disponibilidad, Confidencialidad, Integridad y Autenticidad) según el grupo de activo y se toma como referencia los valores del impacto que la herramienta PILAR proporciona, plasmados en el apartado 4.2.8 de este documento y se realiza una comparativa para saber, en que porcentaje disminuye el impacto después de implementar las salvaguardas, posteriormente se realiza el análisis de los valores proporcionado y se puede decir que el impacto disminuye en un porcentaje aproximado del 42%.

INDICADOR: RIESGO

SIN SALVAGUARDAS				
PRINCIPIOS DE LA SEGURIDAD	**ACTIVOS**			
	Escenciales	*Equipos Informáticos (Hardware)*	*Aplicaciones Informáticas (Software)*	*Elementos Auxiliares*
Disponibilidad	7	7	6	8
Integridad	4	4	6	8
Confidencialidad	7	6	6	8
Autenticidad	6	4	4	
CON SALVAGUARDAS				
Disponibilidad	3	3	2	3
Integridad	3	3	2	2
Confidencialidad	3	2	2	1
Autenticidad	2	0	0	

Representación gráfica:



Interpretación:

Los valores referidos para esta grafica corresponden a los descritos en el apartado 4.2.9 de este documento. Se realiza una comparativa entre el riesgo potencial y el riesgo residual, dando como resultado los porcentajes que se muestran en la gráfica y pudiendo decir que el riesgo disminuye en un 38.66% aproximadamente.

CONCLUSIÓN:

Todo sistema está expuesto a amenazas y ningún método va a garantizar el 100% de la seguridad de la información, pero se puede implementar medidas que desmayan estos riesgos. Y con este proceso se puede decir que la seguridad del Data Center mejorará en un 40.33% aproximadamente.

Anexo 10: Políticas y Procedimientos de Seguridad

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

MANUAL DE POLITICAS Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACION PARA EL DATACENTER

Versión	2.0
Realizado por:	Sr. Cristian Alfonso Perugachi MSc. Carlos Vásquez
Actualizado por:	Sra. Vanessa Marilyn Jácome Chávez MSc. Jaime Michilena
Aprobado por:	

I. PROPOSITO

En el marco de normativa de seguridad es indispensable la adopción de políticas y procedimientos para el control de la seguridad de la información y el cumplimiento por parte de los encargados y usuarios que tengan relación con el Data Center de la Facultad de Ingeniería y Ciencias Aplicadas, ubicado en la Universidad Técnica del Norte de la ciudad de Ibarra, a su vez es necesario para resguardar la información que maneja.

II. GENERALIDADES

a. El documento detalla las políticas que permitan mejorar la seguridad de la información que se maneja en el Data Center.

b. Este documento detalla las responsabilidades tanto de las personas encargadas del Data Center así como los usuarios que interactúan con su infraestructura.

c. La persona tanto privada como particular que requiera acceso para mantenimiento, instalación o remoción de algún activo del Data Center deberá conocer el documento presente y actuar de acuerdo a la misma en caso de afectación se prevé tomar los correctivos adecuados establecidos.

III. VIGENCIA

El presente documento entrará en vigencia en el momento de su aprobación por las personas encargadas de la administración del Data Center de la Facultad de Ingeniería y Ciencias Aplicadas, la misma que será revisada y actualizada conforme a las leyes o normativas actuales.

IV. DESCRIPCION RESPONSABLES

Los responsables de la administración y gestión del Data Center son los llamados a dar cumplimiento a este documento.

Administrador del Data Center.- persona encargada del Data Center, responsable del cumplimiento de los procesos y políticas establecidas; además autoriza solicitudes de ingreso y toda actividad dentro del Data Center.

Técnico encargado Data Center.- persona que asiste al administrador de la red, responsable del control de ingreso y salida de los usuarios. Se asegura del

buen funcionamiento de los equipos y el delegado de asistir en caso de fallos o inconvenientes.

Custodio del activo.- persona responsable de un activo específico, responsable de todas las tareas que en él se realice.

V. REFERENCIA

Para su desarrollo se tomara en referencia la norma ISO/IEC 27002-2005, la cual se encuentran desarrollados en forma de políticas; los objetivos de control y controles presentados en el Anexo A de la norma ISO/IEC 27001, de los cuales se tomaran en cuenta los siguientes:

5. Política de Seguridad de la Información

5.1. **Políticas de seguridad de la información**

5.1.1. Documento de políticas de seguridad de la información.

5.1.2. Revisión de las políticas de seguridad de la información.

6. Organización de seguridad de la información

6.1. Organización Interna

6.1.1. Compromiso de gestión de seguridad de la información.

6.1.2. Coordinación de seguridad de la información

6.1.3. Asignación de responsabilidades de seguridad de la información

6.1.4. Proceso de autorización para instalaciones de procesamiento de información

6.1.5. Acuerdos de confidencialidad

6.1.6. Contacto con las autoridades

6.1.7. Contacto con grupos especiales de interés

6.1.8. Revisión independiente de la seguridad de la información

7. Gestión de los Activos

7.1. Responsabilidad sobre los activos

7.2. Clasificación de la información

7.3. Manipulación de los soportes

8. Seguridad ligada a los Recursos Humanos

8.1.Durante el empleo

8.2.Cese del empleo o cambio de puesto de trabajo

9. Seguridad física y del entorno

9.1. Áreas Seguras

9.2. Seguridad de equipos

10. Gestión de Comunicaciones y Operaciones

10.1. Responsabilidades y procedimientos operacionales.

10.3.Planificación y Aceptación del sistema

10.4.Protección contra código malicioso y descargable.

10.5.Copias de seguridad

10.6.Gestión de la seguridad de Red

10.7.Manipulación de los soportes

11. Control de Acceso

11.2.Gestión de acceso de usuario

11.3.Responsabilidades del usuario

11.4.Control de acceso a la red

11.5.Control de acceso al sistema operativo

11.6.Control de acceso a la información y aplicaciones

12. Adquisición y desarrollo y mantenimiento de los sistemas de información

13. Gestión de incidentes en la seguridad de la información

13.1. Notificaciones de los eventos de seguridad de la información.

13.2. Gestión de incidentes en la seguridad de la información

14. Gestión de la continuidad del negocio

15. Cumplimiento

15.2.Cumplimiento de las políticas y normas de seguridad

VI. TERMINOS Y DEFINICIONES

Activo	Recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección. [Magerit: 2006]
Plan de seguridad	Conjunto de proyectos de seguridad que permiten materializar las decisiones de gestión de riesgos.
Proyecto de seguridad	Agrupación de tareas orientadas a tratar el riesgo del sistema. La agrupación se realiza por conveniencia, bien porque se trata de tareas que en singular carecerían de eficacia, bien porque se trata de tareas con un objetivo común, bien porque se trata de tareas que competen a una única unidad de acción.
Seguridad	La capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles. [Reglamento (CE) n 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la

	Agencia Europea de Seguridad de las Redes y de la Información].
Seguridad de la información	Confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables. [UNE 71504:2008]
Sistema de información	Los ordenadores y redes de comunicaciones electrónicas, así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento. Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar (tratar), mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. [UNE 71504:2008] Conjunto de elementos físicos, lógicos, elementos de comunicación, datos y personal que permiten el almacenamiento, transmisión y proceso de la información. [Magerit:1997] Cualquier sistema o producto destinado a almacenar, procesar o transmitir información. [CESID:1997]
Data Center	Centro de datos, es una instalación empleada para albergar los sistemas de información y sus componentes asociados, como las telecomunicaciones y los sistemas de almacenamiento, incluye fuentes de alimentación redundantes, conexiones redundantes de comunicaciones, controles de ambiente y otros dispositivos de seguridad.
Gestión de la Seguridad	Es la parte de un sistema general de gestión establecido por una organización que incluye la estructura organizativa, la planificación de las actividades, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos para desarrollar, implantar, llevar a efecto, revisar y mantener los políticas de seguridad para prevenir accidentes.

Confidencialidad	Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.
Incidencias	Sucesos, eventos que ocurren en un sistema alterándolo o interrumpiéndolo.

VII. DESARROLLO DE POLITICAS Y PROCEDIMIENTOS DE SEGURIDAD

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	5.1. Políticas de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	5.1.1. Documento de políticas de seguridad de la información		

Art. 1. Proporcionar las directrices de la dirección y el soporte para la seguridad de la información en acuerdo con los requerimientos de la FICA, de esta manera proteger los activos que conforman el Data Center en base al estándar ISO 27002.

a) Las políticas deben presentarse a todo el personal relacionado al Data Center de la FICA de manera comprensible al lector.
b) En caso de distribución externa se debe resguardar la información confidencial de las políticas.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	5.1. Políticas de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	5.1.2. Revisión de las políticas de la seguridad de la información		

Art. 2. El administrador del Data Center debe revisar las políticas de la seguridad de información en intervalos planificados y de ser necesario realizar la actualización.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	6. Organizaciones de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	6.1.1. Compromiso de gestión de seguridad de la información		

Art. 3. La administración apoyará activamente la seguridad de la información dentro del Data Center por medio de políticas claras, compromiso y asignación clara de responsabilidades.

Las responsabilidades de la administración son:

a) Identificar los objetivos de seguridad de la información
b) Revisar las políticas de la información y su aprobación.
c) Proporcionar un apoyo permanente en los proyectos de seguridad de la información
d) Proporcionar los recursos necesarios
e) Aprobar la asignación de funciones y responsabilidades de las personas relacionadas con el Data Center.
f) Socializar los planes de seguridad de la información

Art. 4. La administración debe identificar las necesidades de asesoramiento especializado interno o externo, además de su documentación.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	6. Organizaciones de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	6.1.2. Coordinación de seguridad de la información		

Art. 5. El administrador del Data Center de la FICA debe asignar los roles y responsabilidades de los usuarios, personal de seguridad, personal administrativo y docente, que hagan uso de los activos.

a) Identificar penalizaciones por exceder los roles o funciones asignadas.

b) Establecer los procesos para la seguridad de la información.

c) Identificar los cambios significativos en el Data Center.

d) Promover la formación en materia de seguridad de la información.

Art. 6. Las responsabilidades y tareas asignadas no podrán ser excedidas para de esta manera evitar modificaciones no autorizadas o el mal uso de los activos del Data Center de la FICA.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	6. Organizaciones de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	6.1.3. Asignación de responsabilidades de seguridad de la información		

Art. 7. La administración realizará la asignación de responsabilidades en acuerdo con las políticas de la información.

Art. 8. Las áreas de responsabilidad deben estar claramente definidas y se debe realizar lo siguiente:

a) Los activos y procesos de seguridad deben estar claramente definidos
b) Se debe asignar responsabilidades particulares según el activo y el proceso.
c) Los niveles de autorización deben ser definidos y documentados.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	6. Organizaciones de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	6.1.4. Proceso de autorización para instalaciones de procesamiento de información		

Art. 9. Se debe tomar en cuenta las siguientes indicaciones para la autorización de procesos:

a) Instalaciones nuevas deben tener previa autorización del administrador de la red, junto con un documento que indique su propósito y el cumplimiento de las políticas de seguridad de la información.
b) Técnico encargado debe verificar la compatibilidad del hardware y software con el sistema a implementar
c) Previa autorización la utilización de equipos externos para la configuración o mantenimiento de los activos dentro del Data Center

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	6. Organizaciones de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	6.1.5. Acuerdos de confidencialidad		

Art. 10. Se debe identificar y revisar regularmente los acuerdos de confidencialidad o no divulgación que contemplan las necesidades de protección de la información que se maneja en el Data Center.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	6. Organizaciones de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	6.1.6. Contacto con las autoridades		

Art. 11. E administrador del Data Center debe estar siempre en contacto con las autoridades de la facultad y personal responsable de la red de la Universidad Técnica del Norte para informar de cualquier incidente en la seguridad de la información que afecte al funcionamiento de los servicios implementados.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	6. Organizaciones de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	6.1.7. Contacto con grupos especiales de interés		

Art. 12. El administrador de Data Center tiene que mantener contactos adecuados con grupos de interés especial, foros de seguridad y grupos profesionales.

Art. 13. El mantener el contacto con grupos de interés presenta las siguientes ventajas:

a) Mejores prácticas y actualización permanente en la seguridad de la información.
b) Recibir alertas tempranas antes amenazas y vulnerabilidades.
c) Acceso a asesoría especializada.
d) Compartir e intercambiar información.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	6. Organizaciones de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	6.1.8. Revisión independiente de la seguridad de la información		

Art. 14. El administrador del Data Center debe implementar una revisión independiente en intervalos planificados para revisión de cambios significativos en la seguridad de la información.

Art. 15. La revisión deberá ser llevada por personal independiente del área cercana al Data Center de la FICA, con habilidades y experiencia relacionada con el área de seguridad del a información.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS		
Dominio:	7. Gestión de activos	**Destinatarios:**	Todos los usuarios
Control:	7.1. Responsabilidad de activos		

Art. 16. El técnico encargado se encarga de que los activos sean identificados, tengan un propietario, estén asignadas sus funciones e integren controles apropiados.

Art. 17. El administrador del Data Center de la FICA deben encargarse de tener claramente identificados los activos.

Existen varios tipos de activos los cuales son:

a) Información: bases de datos y archivos, acuerdos, documentación de sistemas, investigaciones, manuales de usuario, procedimientos de soporte, planes de continuidad, información archivada, etc.
b) Activos de Software: aplicaciones, sistemas y herramientas de desarrollo.
c) Activos Físicos: equipos de computación, equipos de comunicación, dispositivos portátiles y otros equipos.
d) Servicios: Servicios de comunicación y computación.

Art. 18. Toda la información de los activos y su procesamiento debe ser asignado a un custodio que sea parte de la FICA

El custodio del activo es responsable por:

a) Asegurarse de que la información del activo sea procesada y clasificada de manera apropiada.
b) Definir un periodo para la revisión de permisos de acceso.
c) Implementar debidamente controles de accesos al activo correspondiente.

Art. 19. El administrador del Data Center FICA y el custodio del activo deben definir las reglas y la documentación pertinente para su uso.

Se debe tener registro de equipos ajenos que ingresen al Data Center.

Se debe definir procedimientos y medidas disciplinarias en el caso de incumplir con las responsabilidades asignadas.

Se debe definir y documentar las autorizaciones de acceso.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	7. Gestión de activos	**Destinatarios:**	Todos los usuarios
	Control:	7.2. Clasificación de la información		

Art. 20. La información debe clasificarse para indicar la necesidad, las prioridades y su grado de protección.

Art. 21. Las clasificaciones y los controles de protección deben tomar en cuenta las necesidades del usuario final del Data Center FICA.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	7. Gestión de activos	**Destinatarios:**	Todos los usuarios
	Control:	7.3. Manipulación de los soportes.		

Art. 22. Todos los medios (discos, unidades de almacenamiento, etc.) deberán ser controlados y físicamente protegidos, estableciendo procedimientos operativos adecuados para evitar la divulgación, modificación o destrucción de información.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	8. Seguridad ligada a los Recursos Humanos	**Destinatarios:**	Todos los usuarios
	Control:	8.1. Durante el empleo		

Art. 23. Todos los empleados de la organización, contratistas y usuarios de terceros deben tener conocimiento de las en políticas y procedimientos organizacionales que sean relevantes para la función de su trabajo.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	8. Seguridad ligada a los Recursos Humanos	**Destinatarios:**	Todos los usuarios
	Control:	8.2. Cese del empleo o cambio de puesto de trabajo		

Art. 24. Asegurar que los empleados, contratistas y terceros que abandonan la organización o cambian de puesto de trabajo de una manera segura.

Art. 25. Cuando exista cambio en asignación de custodio de los activos, las credenciales de usuarios, deberán ser cambiadas de manera inmediata.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	9. Seguridad Física y del entorno	**Destinatarios:**	Todos los usuarios
	Control:	9.1. Areas Seguras		

Art. 26. Se debe tener restringido el acceso a personal no autorizado a las instalaciones donde se encuentran los activos. Además, cada activo administrable debe poseer contraseñas para así evitar el acceso no deseado.

Art. 27. Debe existir una revisión periódica de las instalaciones por los bomberos o personal especializado.

Art. 28. Frente a desastres naturales o industriales se debe realizar simulacros internos para minimizar los riesgos.

Art. 29. Debe tener un procedimiento de emergencia normado por instituciones externas de seguridad.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	9. Seguridad Física y del entorno	**Destinatarios:**	Todos los usuarios
	Control:	9.2. Seguridad de equipos		

Art. 30. Se debe habilitar y especificar vías de evacuación en caso de incendios.

Art. 31. Se debe tener medios manuales de extinción de incendios (extintores portátiles, hidrantes).

Art. 32. Se debe tener un sistema automático de alerta de incendios, que notifique de manera inmediata a los servicios de ayuda exterior.

Art. 33. Se debe tener un plan de mantenimiento, verificación de los dispositivos y los sistemas contra incendios.

Art. 34. Se debe mantener en buen estado el UPS para redundancia en el sistema eléctrico continuo y hacer revisiones de los controles de temperatura periódicamente del UPS y del sistema

de climatización. Además, realizar mantenimiento del sistema de alerta de fallos eléctricos y niveles de temperatura.

Art. 35. Para tener una administración adecuada se debe mantener una gestión centralizada del cableado y utilizar herramientas de gestión para la misma.

Art. 36. Se debe mantener un etiquetado adecuado del cableado estructurado y un inventario actualizado.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	10. Gestión de Comunicaciones y Operaciones	**Destinatarios:**	Todos los usuarios
	Control:	10.1. Responsabilidades y procedimientos operacionales		

Art. 37. El administrado tiene la tarea de establecer responsabilidades y procedimientos para la gestión de todos los activos encargados del procesamiento de información.

Art. 38. Cada custodio de un activo, debe establecer los procedimientos de inicio, terminación, respaldo, mantenimiento del activo.

Estos procedimientos deben contar con los siguientes parámetros:

a) Tratamiento de la información
b) Tiempos de realización de un trabajo
c) Contacto de apoyo técnico
d) Instrucciones especiales para el manejo del activo
e) Procedimiento de reinicio y recuperación del sistema

Art. 39. Los cambios en los activos deben ser controlados y debidamente documentados.

Los siguientes parámetros deben ser considerados en particular:

a) Identificación de cambios significativos.

b) Planificación y comprobación de cambios.

c) Evaluación de posibles impactos

d) Aprobación de cambios propuestos.

Art. 40. Se debe definir las funciones y responsabilidades para evitar los cambios no autorizados o mala utilización de los activos del Data Center FICA.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	10. Gestión de Comunicaciones y Operaciones	**Destinatarios:**	Todos los usuarios
	Control:	10.3. Planificación y aceptación del sistema		

Art. 41. El administrador debe planificar de manera anticipada los recursos necesarios del sistema que se implementará, para evitar sobrecargas que incidan en el funcionamiento de los servicios integrados en el Data Center de la FICA.

Art. 42. El administrador del Data Center de la FICA tiene que identificar las condiciones de los recursos del sistema mediante un sistema de monitorización para identificar posibles cuellos de botella y tomar las medidas adecuadas para evitar pérdidas de información.

Art. 43. El administrador del Data Center de la FICA tiene que asegurar que se cumplan los requisitos de adaptación para la implementación de sistemas y actualizaciones.

Para poder integrar un sistema es necesario cumplir con lo siguiente:

a) Requerimientos de sistema

b) Procedimiento de recuperación, reinicio y planes de contingencia.

c) Pruebas de funcionamiento

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	10. Gestión de Comunicaciones y Operaciones	**Destinatarios:**	Todos los usuarios
	Control:	10.4. Protección contra código malicioso y descargable.		

Art. 44. Se debe tener en cuenta las precauciones para prevenir y detectar la introducción de código malicioso y cada custodio del activo debe tener su propio software de detección de código malicioso.

Art. 45. El administrador del Data Center de la FICA debe implementar los controles de detección, prevención y recuperación para proteger contra código malicioso.

Se debe implementar un software de detección de código malicioso para el cual se debe considerar lo siguiente:

a) Evitar uso no autorizado de software en los activos que integran el Data Center

b) Realizar revisiones periódicas de los activos que manejan información sensible de la organización.

c) Instalación y actualización de software de detección de código malicioso.

d) Comprobación de cualquier medio extraíble que ingrese al Data Center

e) Definir procedimientos para enfrentar una infección

f) Preparación de planes de continuidad

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	10. Gestión de Comunicaciones y Operaciones	**Destinatarios:**	Todos los usuarios
	Control:	10.5. Copias de seguridad		

Art. 46. El administrador del Data Center de la FICA establecerá procedimientos de rutina y la estrategia de respaldo de la información.

Art. 47. Se debe realizar instalaciones de respaldo de la información importante y el software en caso de existir un desastre o fallo generalizado, de lo que será responsable cada custodio del activo.

Hay que considerar lo siguiente para la información de respaldo:

a) Registro de la información de respaldo y los procedimientos a realizar para su restauración
b) La frecuencia de realización de respaldos debe estar documentada
c) Las copias de seguridad deben almacenarse en una ubicación externa
d) Se debe probar o actualizar periódicamente la información de respaldo
e) Los respaldos pueden ser protegidos mediante cifrado

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	10. Gestión de Comunicaciones y Operaciones	**Destinatarios:**	Todos los usuarios
	Control:	10.6. Gestión de la seguridad de red		

Art. 48. El administrador del Data Center debe proteger la información mediante sistemas de seguridad aplicados en la infraestructura de red.

Art. 49. Las redes deben estar gestionadas y controladas para protegerlas de amenazas externas e internas que ponen en riesgo la seguridad de los sistemas, para esto el administrador del Data Center de la FICA deben considerar lo siguiente:

a) Debe establecer responsabilidades y procedimientos para la gestión de equipos remotos.
b) Se deben establecer controles especiales para proteger la confidencialidad e integridad de los datos que se transportan por redes públicas e inalámbricas.
c) Se debe implementar un sistema de monitoreo en la red para registrar acciones relevantes de seguridad y poder actuar en caso de irregularidades.

Art. 50. Se debe implementar controles de seguridad que le den un valor agregado como separación de redes privadas, implementación de un firewall y sistema de detección de intrusiones.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	10. Gestión de Comunicaciones y Operaciones	**Destinatarios:**	Todos los usuarios
	Control:	10.7. Manipulación de dispositivos de soporte		

Art. 51. El administrador del Data Center de la FICA debe establecer los procedimientos para la entrada o salida de medios externos.

Art. 52. Se debe tomar en cuenta las siguientes directrices para el manejo de medios externos:

a) Si el contenido del medio extraíble que ya no es necesario, se debe eliminar dicha información.

b) Se debe requerir autorización para la utilización de los medios extraíbles removidos del Data Center FICA.

c) Todos los medios extraíbles deben almacenarse en un entorno seguro.

d) Se debe registrar los medios extraíbles que ingresan o salen del Data Center.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	11. Control de accesos	**Destinatarios:**	Todos los usuarios
	Control:	11.2. Gestión de acceso de usuario		

Art. 53. El administrador del Data Center debe generar los procedimientos para el acceso de usuario, desde el registro inicial de nuevos usuarios, hasta su eliminación.

Art.54. El procedimiento para el registro y cancelación de acceso para cada usuario debe incluir:

a) Usar identificadores únicos para asignar responsabilidades directas al usuario.

b) Autorización del propietario del sistema o servicio de información.

c) Nivel de acceso concedido.

d) Declaración escrita de sus derechos de acceso.

e) Firma de responsabilidad del usuario

f) Registro formal de las personas autorizadas.

g) Eliminar el acceso a los usuarios que finalizaron su trabajo en el Data Center FICA

h) Revisar periódicamente los derechos de acceso.

Art. 55. Los sistemas que requieran protección contra accesos no autorizados deben tener un control basado en un proceso formal de autorización, que contempla los siguientes pasos:

a) Los privilegios de acceso según el sistema y las aplicaciones.
b) Privilegios asignados según el evento que se presento
c) Registro de todos los privilegios asignados según el usuario
d) Se debe asignar un ID independiente por usuario.

Art. 56. La asignación de contraseñas para el acceso a los sistemas u servicios debe incluir los siguientes requisitos:

a) Firma de responsabilidad del usuario.
b) En caso de que todos los usuarios requieran una contraseña para el uso de un servicio se les asignara una temporal, que deberán cambiar inmediatamente por una de su preferencia.
c) Establecer los procedimientos para verificar la identidad de un usuario antes de restablecer una contraseña.
d) Las contraseñas temporales deben entregarse a los usuarios de manera segura.
e) Las contraseñas deben almacenarse en sistemas con las seguridades necesarias.
f) Se debe reemplazar las contraseñas predeterminadas de un sistema después de su instalación.

Art. 57. El administrador del Data Center FICA debe revisar los derechos de acceso a los usuarios en intervalos regulares, tomando en cuenta los siguientes parámetros:

a) Los derechos de acceso de usuario deben revisarse cada 6 meses y después de cualquier cambio en los privilegios o posición del usuario.
b) Los derechos deben ser revisados y reasignados cuando un usuario cambia de posición laboral dentro de la facultad.
c) Los accesos con privilegios especiales deben ser revisados cada 3 meses.
d) Los cambios en accesos privilegiados deben registrarse de manera mensual.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS		
Dominio:	11. Control de accesos	**Destinatarios:**	Todos los usuarios
Control:	11.3. Responsabilidades del usuario		

Art. 58. Los usuarios deben ser conscientes de sus responsabilidades en lo que se refiere a uso de contraseñas y seguridad de su equipo de trabajo.

Art. 59. Los usuarios deben realizar buenas prácticas de seguridad en la selección y uso de las contraseñas, por medio de los siguientes pasos:

a) Mantener la confidencialidad de las contraseñas
b) No almacenar la contraseña en un registro de fácil acceso.
c) Cambiar la contraseña en caso de vulnerabilidades en el sistema
d) Contraseña con longitud aceptable:
    1. Fácil de recordar
    2. No relacionada con aspectos directamente relacionados a la persona
    3. No vulnerables a ataques de diccionario
    4. Sin caracteres consecutivos o repetitivos.
e) Cambiar la contraseña en intervalos regulares
f) No almacenar las contraseñas en la cache de los navegadores
g) Cambiar contraseñas temporales en el primer inicio de sesión
h) No compartir contraseñas individuales de los usuarios.
i) No usar la misma contraseña en todas las cuentas.

Art. 60. Los custodios de los activos deben estar conscientes de los procedimientos y requisitos para proteger un equipo del Data Center FICA, la recomendación general es:

a) Cerrar sesiones activas al terminar.
b) Asegurar los terminales mediante contraseña en caso de no utilizarlo.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	11. Control de accesos	**Destinatarios:**	Todos los usuarios
	Control:	11.4. Control de acceso a la red		

Art. 61. El administrador del Data Center FICA regula el acceso de los usuarios a las redes y servicios para no comprometer su seguridad y garantizar:

a) Interfaces apropiadas de comunicación entre la red del Data Center FICA, las redes públicas y la intranet de la Universidad Técnica del Norte.
b) Mecanismos de autenticación entre los usuarios y el equipo.
c) Control de acceso del usuario a los servicios.

Art. 62. La autenticación de usuarios remotos con privilegios se realizará mediante controles criptográficos y la utilización de técnicas como VPN, o doble autenticación utilizando la dirección MAC.

Art. 63. Es recomendable dividir en dominios la red lógica, y separar la red pública de la intranet, se puede aplicar un gateway o firewall que se encargue de separar y proteger los sistemas y servicios.

Art. 64. Para todas las redes externas que soliciten acceso a los servicios de la organización se debe restringir a través de pasarelas, firewall o proxy de red que filtren el tráfico. Para aplicaciones como:

a) Correo electrónico
b) Transferencia de archivos
c) Acceso interactivo
d) Acceso a la aplicación

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS		
Dominio:	11. Control de accesos	**Destinatarios:**	Todos los usuarios
Control:	11.5. Control de acceso al sistema operativo		

Art. 65. Cada custodio de un activo, debe encargarse de la seguridad para restringir el acceso a los sistemas operativos a los usuarios no autorizados, considerando que las instalaciones deben ser capaces de:

a) Autenticar usuarios no autorizados.
b) Registrar intentos de autenticación exitosos o fallidos.
c) Registrar el uso de privilegios especiales del sistema.
d) Emitir alarmas cuando se rompan las seguridades.
e) Proporcionar medios adecuados para la autenticación
f) Regular tiempos de conexión

Art. 66. Se deben establecer procedimientos para minimizar accesos no autorizados, para esto debe cumplir los siguientes requisitos:

a) No mostrar identificadores de sistema hasta que no se complete el inicio de sesión.
b) Advertencia general de que solo los usuarios autorizados deben tener acceso a la computadora
c) No mostrar mensajes de ayuda para inicio de sesión
d) Limitar número de intentos para autenticación y registrarlos
e) Registrar login exitoso
f) No mostrar la contraseña introducida.
g) No transmitir contraseñas en texto plano a través de una red

Art. 67. Los sistemas de contraseñas deben ser interactivos y deben garantizar contraseñas de calidad realizando lo siguiente:

a) Imponer el uso de identificadores de usuario y contraseñas individuales

b) Permitir al usuario seleccionar y cambiar su contraseña mediante confirmación

c) Imponer parámetros para la selección de contraseñas

d) Obligar al cambio de contraseña temporal en el primer inicio de sesión

e) Evitar reutilización de contraseñas

f) Almacenar las contraseñas de manera independiente

g) Almacenar y transmitir contraseñas de forma protegida

Art. 68. El administrador debe integrar medidas de seguridad que permitan controlar los tiempos en pantalla de sesión, además de cierre de conexiones inactivas que exceden cierta cantidad de tiempo.

Art. 69. Los controles de conexión por tiempo deben ser implementados en aplicaciones informáticas sensibles y en conexiones desde una red pública.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	11. Control de accesos	**Destinatarios:**	Todos los usuarios
	Control:	11.6. Control de acceso a la información y aplicaciones		

Art. 70. El acceso lógico al software de la aplicación y la información debe limitarse a los usuarios autorizados.

Los sistemas de aplicación deben:

a) Proteger de accesos no autorizados y software malintencionado.

b) Aislar los sistemas en caso de una infección que comprometa recursos

Art. 71. El administrador del Data Center FICA deben implementar los siguientes requisitos de restricción:

a) Controlar permisos del usuario para lectura y escritura.
b) Asegurar la información sensible para su envió y compartición solo a servidores y usuarios autorizados.

Art. 72. Se debe tomar en cuenta las siguientes consideraciones para los sistemas informáticos sensibles:

a) El propietario del sistema debe documentar la sensibilidad del sistema.
b) El propietario debe identificar los sistemas con los que interactuara la información sensible contenida.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	12. Adquisición, desarrollo y mantenimiento de los sistemas de información	**Destinatarios:**	Todos los usuarios
	Control:			

Art. 73. Se deberá realizar una gestión apropiada de las claves.

Art. 74. El técnico encargado del Data Center es el responsable directo de las adquisiciones y desarrollo de nuevos sistemas informáticos; para lo cual deberá ser sustentado mediante el desarrollo de proyectos individuales.

Art. 75. El administrador y técnico encargado, son los llamados a asignar o realizar el debido mantenimiento del sistema informático.

a) El encargado debe realizar revisiones y mantenimiento programado para asegurar el correcto funcionamiento de los equipos.

b) Se deberá realzar un informe de las novedades ocurridas a lo largo del mantenimiento.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	13. Gestión de incidentes de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	13.1. Notificación de los eventos de seguridad de la información		

Art. 76. Se deberían comunicar los eventos en la seguridad de información lo más rápido posible mediante canales de gestión apropiados.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	13. Gestión de incidentes de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	13.2. Gestión de incidentes en la seguridad de la información		

Art. 77. Todo usuario y empleado que se relacione con el Data Center FICA debe reportar cualquier tipo de evento o vulnerabilidad que incide directamente en la seguridad de los activos.

Art. 78. El administrador del Data Center debe designar al personal que estará encargado de gestionar las incidencias que se presente en el sistema, teniendo este que seguirlos siguientes procesos, para la atención de la respectiva incidencia.

a) El personal asignado debe recibir una incidencia, debe determinar si la incidencia cuenta con los datos necesarios para responder a la misma. Si no el caso el encargado solicitara más información sobre la incidencia.

b) El personal asignado a partir de recibir todo la información de la incidencia, esta pasa a ser aceptada, para posteriormente ser asignada a un responsable que deberá resolver dicha incidencia.

Art. 79. Se seguirá el procedimiento para presentación de informes sobre los sucesos de la seguridad de la información, además de respuesta y escalamiento de incidentes.

Estos procesos deberán incluir:

a) Retroalimentación para asegurar que no se repitan las mismas fallas.

b) Formularios de información de eventos.

c) Comportamiento correcto en caso de vulnerabilidades siguiendo el proceso descrito

c.1. Anotar todos los detalles importantes

c.2. Informar al administrador del Data Center FICA

Art. 80. Los documentos de resolución de incidentes deberán ser del conocimiento de todos los usuarios que accedan al Data Center y de esta manera reducir la probabilidad de incidentes futuros.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	14. Gestión de continuidad del negocio	**Destinatarios:**	Todos los usuarios
	Control:			

Art. 81. Se debe desarrollar e implementar planes de continuidad incluyendo la seguridad de la información, designando: roles y responsabilidades, objetivos y alcance, recursos

necesarios, formación, pruebas de los planes, revisiones y mantenimiento de los planes con frecuentes copias de seguridad y almacenamiento seguro con la respectiva aprobación y difusión de la documentación.

Art. 82. Cada custodio de los distintos activos deben presentar un plan el cual asegure la recuperación de la información de dicho activo.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	15. Cumplimiento	**Destinatarios:**	Todos los usuarios
	Control:	15.2. Cumplimiento de las políticas y normas de seguridad		

Art. 83. El administrador del Data Center FICA tiene la responsabilidad de verificar el cumplimiento de las políticas de seguridad.

Art. 84. Se debe revisar y verificar periódicamente los procedimientos operativos, el cumplimiento de políticas, normas y reglamentos técnicos por parte del personal del Data Center.

Art. 85. Las sanciones que se pueden presentar por el incumplimiento de las políticas son las siguientes:

a) Llamado de atención de manera escrita y verbal

b) Suspensión temporal del acceso a los activos del Data Center

c) Suspensión permanente del acceso a los activos del Data Center

d) Reposición del costo de los activos dañados, sustraídos o extraviados que se den por acción directa del usuario o encargado.