UNIVERSIDAD TÉCNICA DEL NORTE

Faculta de Ingeniería en Ciencias Aplicadas

Carrera de Software

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LAS NORMAS DE SEGURIDAD ISO/IEC 27001 – 27002: 2022 PARA LA EMPRESA AIRMAXTELECOM SOLUCIONES TECNOLÓGIAS S.A.

Trabajo de grado previo a la obtención del título de Ingeniero de Software

AUTOR:

Heinz Dylan Delgado Ojeda

DIRECTOR:

PhD. Daisy Elizabeth Imbaquingo Esparza

Ibarra – Ecuador

2024

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE USO

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	105044073-2		
APELLIDOS Y NOMBRES	HEINZ DYLAN DELGADO OJEDA		
DIRECCIÓN	IBARRA - CARANQUI		
EMAIL	hddelgadoo@utn.edu.ec		
TELÉFONO FIJO:		**TELÉFONO MÓVIL:**	0978857886

DATOS DE LA OBRA	
TÍTULO	DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LAS NORMAS DE SEGURIDAD ISO/IEC 27001 – 27002: 2022 PARA LA EMPRESA AIRMAXTELECOM SOLUCIONES TECNOLÓGIAS S.A.
AUTOR(ES):	HEINZ DYLAN DELGADO OJEDA
FECHA:	
PROGRAMA	PREGRADO
TÍTULO POR EL QUE OPTA:	INGENIERO EN SOFTWARE
DIRECTOR:	PhD DAISY IMBAQUINGO
ASESOR 1:	MACARTHUR ORTEGA

2. Constancias

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

Ibarra, a los 29 días del mes de julio del 2024

EL AUTOR:

Heinz Dylan Delgado Ojeda

C.I: 105044073-2

CERTIFICACIÓN DIRECTOR

Ibarra 29 de julio del 2024

CERTIFICACIÓN DIRECTOR DEL TRABAJO DE TITULACIÓN

Por medio del presente yo PhD. Daisy Imbaquingo Esparza, certifico que el Sr. Heinz Dylan Delgado Ojeda portador de la cedula de ciudadanía número 1050440732, ha trabajado en el desarrollo del proyecto de grado "Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en las normas de seguridad ISO/IEC 27001 – 27002: 2022 para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGIAS S.A", previo a la obtención del Título de Ingeniero en Software realizado con interés profesional y responsabilidad que certifico con honor de verdad.

Es todo en cuanto puedo certificar a la verdad

Atentamente

PhD. Daisy Imbaquingo

DIRECTOR DE TRABAJO DE GRADO

Dedicatoria

El presente trabajo de grado quiero dedicarlo a mi madre, Claudia Ojeda, mi padre Miguel Delgado, quienes fueron los pioneros de una formación estudiantil de calidad, por alentarme a seguir adelante cuando más difícil se tornó mi camino llenó de obstáculos y siempre estuvieron apoyándome con muchas ganas y esfuerzo, a no rendirme logrando cumplir una meta más, no solo es un logro personal, también es un logro familiar ya que sin Dios y sin ellos no sería posible.

A mis hermanas, sobrina, quienes fueron uno de los pilares fundamentales en este camino universitario.

Desde el fondo de mi corazón dedico este logro que con esfuerzo, ganas y dedicación llegó a cumplirse.

HEINZ DYLAN DELGADO OJEDA

Agradecimientos

Quiero agradecer desde el fondo de mi corazón a Dios, a mis padres Claudia Ojeda, Miguel Delgado, quienes con tanto esfuerzo, agotaron los recursos necesarios para lograr formarme como un profesional, cuando quise desistir, lograron animarme a seguir adelante en uno de los escalones y metas más importantes de mi vida.

Agradezco a las personas que aportaron con su grano de arena para lograr culminar esta meta importante, a Karen Estacio, Carolina Herrera, Mishel Mejía, Andrés Benavides, a la empresa AIRMAXTELECOM por permitir el desarrollo de este trabajo y brindarme conocimiento.

Agradezco a los docentes que estuvieron en cada peldaño universitario, a mi tutora de trabajo de titulación, la PhD Daisy Imbaquingo, MSc Cosme Ortega que gracias a su tiempo, dedicación y orientación pude lograr realizar un trabajo de calidad.

A todos ustedes expreso mi eterna gratitud.

HEINZ DYLAN DELGADO OJEDA

TABLA DE CONTENIDOS

Índice de Figuras

Índice de Tablas

Resumen

En el documento se encuentra estructurado por cuatro capítulos, en cada uno se detalla el proceso que se realizó para el desarrollo de Trabajo de Grado: “DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LAS NORMAS DE SEGURIDAD ISO/IEC 27001 – 27002: 2022 PARA LA EMPRESA AIRMAXTELECOM SOLUCIONES TECNOLÓGIAS S.A.”

En la sección de introducción se puede encontrar la situación actual, prospectiva, planteamiento del problema, objetivos generales y específicos, alcance y justificación.

En el capítulo 1, como objetivo se comprende el análisis de la literatura en base a las Normas de Seguridad ISO/IEC 27001 y 27002: 2022.

En el capítulo 2, se desarrolla el levantamiento y evaluación de riesgos en la seguridad de la información de los activos de la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.

El en capítulo 3, se desarrolla la propuesta del Sistema de Gestión de Seguridad de la Información basado en las Normas de Seguridad ISO/IEC 27001 y 27002: 2022, políticas de seguridad de la información, proceso de implementación y mejora continua.

En el capítulo 4, se realiza el proceso de validación el Sistema de Gestión de Seguridad de la Información utilizando el método Delphi.

Finalmente se plantea las conclusiones, recomendaciones, como adjunto se encuentra las referencias bibliográficas y anexos del trabajo de grado.

Abstract

The document is structured in four chapters, each one detailing the process that was carried out for the development of the Degree Project: 'DESIGN OF AN INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) BASED ON THE SECURITY STANDARDS ISO/IEC 27001 - 27002: 2022 FOR THE COMPANY AIRMAXTELECOM SOLUCIONES TECNOLÓGIAS S.A.'.

In the introduction section you can find the current situation, prospective, problem statement, general and specific objectives, scope, and justification.

In chapter 1, the objective is the analysis of the literature based on the ISO/IEC 27001 and 27002: 2022 Security Standards.

In chapter 2, the survey and risk assessment of the information security of the assets of the company AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A. is developed.

Chapter 3 develops the proposal of the Information Security Management System based on the ISO/IEC 27001 and 27002: 2022 Security Standards, information security policies, implementation process and continuous improvement.

In chapter 4, the validation process of the Information Security Management System is carried out using the Delphi method.

Finally, the conclusions, recommendations, bibliographical references and annexes of the degree work are included.

Introducción

Tema

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LAS NORMAS DE SEGURIDAD ISO/IEC 27001 – 27002: 2022 PARA LA EMPRESA AIRMAXTELECOM SOLUCIONES TECNOLÓGIAS S.A.

Problema

Situación Actual

La empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGIAS S.A. es una empresa que brinda el servicio de internet a sus clientes de forma rápida y segura cuenta diferentes sucursales alrededor del país con un posicionamiento considerable en el mercado.

Su principal fuente de servicio al cliente es ser proveedores de internet con su matriz en la ciudad de Ibarra – Imbabura, continúa creciendo con la prestación de servicios de televisión, rastreo satelital, se plantea mejorar el servicio de internet en las áreas rurales

La empresa de internet cuenta con una estructura adecuada para brindar este servicio, equipos actualizados, innovadores, cuenta con plataforma digital en donde se puede monitorear las actividades que se realizan dentro y fuera de ella, control de los trabajadores en sus procesos de instalación del servicio, infraestructura de internet, plataforma de pagos digitales para facilidad del cliente, cuenta con soporte técnico en todos los días de la semana para brindar una mejor experiencia de navegación a sus clientes, se encuentra aplicando normas de calidad en sus establecimientos para dar una mejor calidad en servicio y seguir creciendo en su cartera de clientes.

Prospectiva

La prospectiva en cuanto a una mejora en la empresa de internet AIRMAXTELECOM SOLUCIONES TECNOLÓGIAS S.A. implica desarrollar un Sistema de Gestión de Seguridad de la Información basado en las normas de Seguridad ISO/IEC 27001 y 27002: 2022., en contexto a esta situación actual es necesario enfocarse en la seguridad de la información de los clientes y del personal que labora en la empresa. Este sistema permitirá elevar el nivel de seguridad no solo en el área de tecnologías, también apoya a las demás áreas y departamentos que conforman la empresa, cuenta con la estructura del sistema que en base a normativas, políticas y regulaciones vigentes en el año en curso para poder hacerle frente a situaciones que puedan comprometer la seguridad de la información la cual es considerado un activo crítico e importante.

Se recomienda realizar la gestión de riesgos periódicamente, simulacros en los cuales se pueda llegar a levantar el servicio en el menor tiempo posible y evitar la pérdida de clientes en caso de surgir alguna catástrofe manteniendo un esquema ágil y seguro.

Planteamiento del Problema

La empresa de internet AIRMAXTELECOM SOLUCIONES TECNOLÓGIAS S.A. en el desarrollo de sus actividades, cuenta con un bajo índice de adopción en normativas de seguridad de la información. Debido a esta problemática se desencadenan ciertas causa y efectos que podrían comprometer la seguridad de la información interna y externa.

El impacto potencial que puede causar la vulneración en la seguridad de la información conlleva a una pérdida de confiabilidad y continuidad del desarrollo de actividades empresariales, puede causar daños colaterales con los clientes que adquieren este servicio y su información puede verse comprometida, este y otras causas y efectos se pueden visualizar en la Figura 1.

Figura 1

Planteamiento del Problema (Causa/Efecto)

Nota: Elaboración Propia.

Objetivos

Objetivo General

Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma de seguridad ISO/IEC 27001-27002 para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.

Objetivos específicos

- Realizar un análisis de la información respectiva y realizar el marco teórico basado en las normas ISO/IEC 27001-27002, revisión de la literatura de la metodología Magerit y Gestión de Seguridad.
- Levantamiento de activos y evaluación de riesgos de seguridad de la información a los que se enfrenta la empresa, considerando amenazas internas y externas, así como las posibles vulnerabilidades existentes en los sistemas y procesos.
- Diseñar una propuesta de un Sistema de Gestión de Seguridad de la Información.
- Validar la propuesta de un Sistema de Gestión de Seguridad de la Información (SGSI) para la empresa AIRMAXTELECOM SOLUCIONES TECNOLOGICAS S.A

Alcance

Se plantea definir un Sistema de Gestión de Seguridad de la Información lo cual conlleva una política para la empresa AIRMAXTELECOM SOLUCIONES TECNOLOGICAS S. A en su matriz Ibarra, con la cual se podrá verificar la existencia de activos que se vean involucrados en la seguridad de la información mediante el uso de la norma ISO 27001- 27002:2022, así como el software Pilar, ayudará en el análisis de riesgos y vulnerabilidades, permitiendo identificar los puntos críticos y establecer los lineamientos necesarios para el desarrollo y la implementación del SGSI, se utilizará los recursos de la sección cuatro que abarca los contextos de la organización y plantear una política de seguridad de la información la que ayude a tener un manejo óptimo de la información, la cual asegure al usuario y a la empresa que dicho activo valioso se encuentre seguro, la misma que servirá para analizar los riesgos y vulnerabilidades de tal forma que se pueda conocer los lineamientos para el desarrollo de un SGSI, incluyendo el estudio de estándares internacionales, leyes de protección de datos, regulaciones sectoriales y cualquier otra normativa relevante.(PILAR - Inicio, 2023.)

Se realizará el levantamiento de la información y activos que cuenta la matriz, evaluar sus riesgos, la cual permitirá obtener un sondeo de la situación actual de la empresa y con ayuda de la política de seguridad incentivar a su correcto uso y manejo responsable de la misma. Se utilizará Pilar en conjunto con la norma ISO 27001-27002:2022 para guiar este proceso y garantizar que se cumplan los estándares de seguridad de la información establecidos.

Además, se llevará a cabo una evaluación de la infraestructura, tecnología de la información y comunicaciones de la organización, así como de los sistemas y procesos relacionados con la gestión de la seguridad de la información. Esto incluirá la identificación de activos de información críticos y una evaluación detallada de los riesgos y vulnerabilidades presentes en la empresa.

Finalmente, se diseñará la estructura y contenido de la Política de Seguridad de la Información, estableciendo los lineamientos y directrices generales para la protección de los activos de información de la organización. Esto incluirá aspectos como la gestión de accesos, gestión de incidentes, clasificación de la información, concientización y capacitación, entre otros (Joseph Alexander Guamán Seis,2015).

Es importante destacar que este trabajo se centrará exclusivamente en el diseño de la Política de Seguridad de la Información y no abordará aspectos específicos de la implementación técnica de controles de seguridad o auditorías de cumplimiento. El alcance se limita a la etapa de diseño y planificación de la política. Todo este proceso se puede visualizar en la Figura 2:

Figura 2

Faces de un Sistema de Gestión de Seguridad de la Información

Nota: Elaboración Propia.

Metodología

Para el cumplimiento de los objetivos planteados de este proyecto de titulación se realizará mediante la siguiente directriz:

Para cumplir el objetivo 1, se realizará la revisión de la norma y analizar cada punto que se debe aplicar, ayudando a tener una idea más clara y concreta de los pasos a seguir, con esto se recopilará información, logrando realizar cada acción solicitada en la norma a cabalidad obteniendo los resultados y alcance planteado, así también revisar la literatura de Magerit y Gestión de riesgos (Gobierno et al., 2019).

Para cumplir el objetivo 2: Se realizará un levantamiento de información de los activos críticos de la empresa con la ayuda del software Pilar el cual maneja la metodología Magerit, esta información se condensará en una matriz de riesgos, en conjunto con el personal encargado con el fin de conocer el estado en el que se encuentra la empresa basándose en la norma ISO/IEC 27001-27002:2022, con el cual se diseñará el SGSI (Welive Security, 2013):

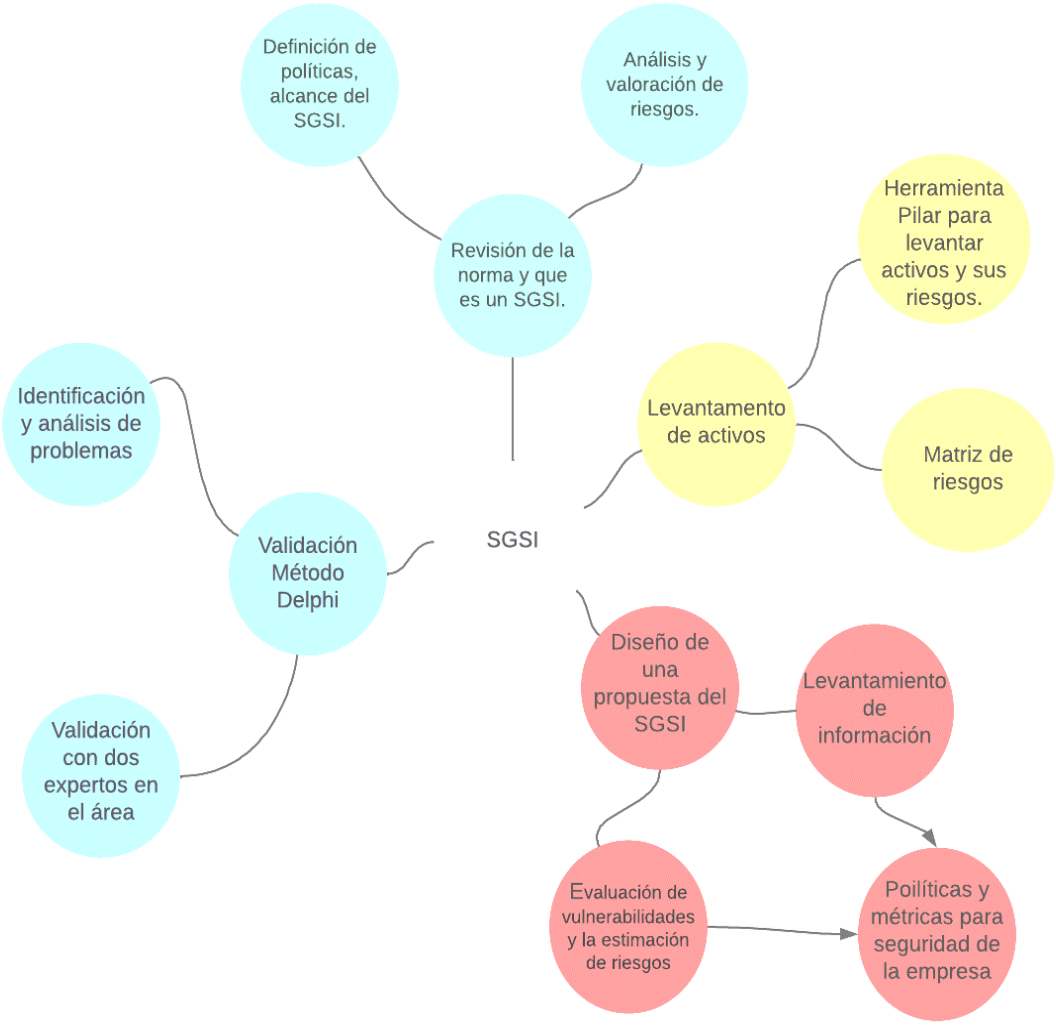
1. Comprensión del contexto
2. Alcance.
3. Establecimiento de un equipo de proyecto.
4. Planificación.
5. Análisis de riesgos.
6. Desarrollo de políticas y objetivos de seguridad de la información.
7. Diseño de controles de seguridad.
8. Documentación del SGSI

Para cumplir el objetivo 3: Mediante la información levantada y recopilada, se realizará las políticas y métricas que sean óptimas para la empresa, realizando así el diseño de la propuesta del SGSI para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.

Para cumplir el objetivo 4, se realizará la validación por el método Delphi, se utiliza para identificar y solucionar problemas o analizar una situación. Consiste en agrupar las opiniones de varios expertos en el tema, sin necesidad de estar en el mismo sitio, para tener un mejor entendimiento sobre la evolución o comportamiento de una empresa. mediante dos expertos (Método Delphi: definición, características, fases y ejemplos, 2021.).

Para el desarrollo y cumplimiento de estos objetivos se tiene estructurada la siguiente metodología, su puede observar en la Figura 3:

Figura 3 *Diagrama del Proceso del SGSI*



Nota: Elaboración Propia.

Justificación

propósito de este trabajo de titulación es desarrollar una propuesta estratégica de seguridad de la información para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A., con el objetivo de cumplir con los requisitos establecidos en los Objetivos de Desarrollo Sostenible (ODS). Específicamente, se enfocará en el ODS número nueve, que busca fomentar la industrialización sostenible, promover la innovación y construir infraestructuras resilientes y sostenibles, así como en el

ODS número 16 que se centra en la construcción de sociedades pacíficas, justas y transparentes (Objetivos y metas de desarrollo sostenible - Desarrollo Sostenible, 2020).

Para respaldar esta propuesta, se utilizará el marco legal establecido en el artículo 9 de la Ley Orgánica de Protección de Datos Personales, el cual establece que el tratamiento de datos personales es un bien legítimo y garantiza la protección de datos. A través del análisis realizado, se verificará la existencia de posibles amenazas que puedan comprometer la seguridad de la información de la empresa (Llano Alex, 2019)

Este enfoque permitirá desarrollar una política de seguridad de la información basada en mejores prácticas y estándares reconocidos internacionalmente, como la norma ISO 27001. La implementación de controles de seguridad adecuados garantizará la confidencialidad, integridad y disponibilidad de los datos, fortaleciendo así la confianza de los clientes y asegurando el cumplimiento de las regulaciones de protección de datos (A Maureira Sánchez, 2015.)

Justificación Tecnológica. - La creciente dependencia de las empresas en el entorno digital, particularmente en el ámbito de internet, ha aumentado la exposición a riesgos y amenazas cibernéticas. La implementación de medidas de seguridad de la información se vuelve crucial para proteger los activos digitales, garantizar la confidencialidad, integridad y disponibilidad de los datos, además, mantener la confianza de los clientes. La tecnología de la información es un componente clave en la gestión de la seguridad, y una tesis que aborde este aspecto ayudará a desarrollar estrategias y mejores prácticas para fortalecer la seguridad en una empresa de internet (Cesar & Yanza panta, 2019).

Justificación Institucional. - La justificación institucional para el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) en una empresa de internet se basa en la protección de información confidencial, el cumplimiento de regulaciones, la mejora de la confianza del cliente, la prevención de incidentes de seguridad y la obtención de una ventaja competitiva. Al implementar un SGSI, la empresa garantiza la protección de la información valiosa, cumple con las normativas legales, genera confianza en los clientes, previene amenazas de seguridad y se destaca en el mercado como una empresa confiable y segura (Torres, 2020.)

Justificación Metodológica. - La elección de utilizar MAGERIT como metodología para evaluar y gestionar los riesgos de seguridad en los sistemas de información se justifica debido a su enfoque integral. Se ha desarrollado específicamente para abordar los riesgos de seguridad en un contexto más amplio, considerando aspectos organizativos, tecnológicos y de gestión. Se obtiene un marco de trabajo sólido que permite a Pilar, como organización, identificar, analizar y tratar

adecuadamente los riesgos de seguridad, fortaleciendo su postura de seguridad y protegiendo sus sistemas de información de manera efectiva.

Esta metodología cuenta con reconocimiento y experiencia en seguridad de la información, lo que brinda confianza y credibilidad a los resultados obtenidos. Al implementar esta metodología, se podrá obtener una visión clara de los riesgos a los que está expuesta, tomar decisiones informadas para mitigarlos y mejorar la protección de su información de manera efectiva. Para validar la efectividad y viabilidad del SGSI se utilizará el método Delphi con la ayuda de dos expertos en el área los cuales evaluaran si es factible el usar el sistema propuesto en la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A. (MAGERIT: metodología práctica para gestionar riesgos | WeLiveSecurity, 2013.)

CAPITULO 1

Marco Teórico

1.1. Revisión de la literatura

La Revisión de la Literatura es el proceso por el cual se realiza un análisis, investigación con la finalidad de poder entender de una mejor forma y comprender como está estructurada la documentación que se ha encontrado, capaz de dar las respuestas a ciertas interrogantes el correcto procedimiento de determinados procesos

1.1.1. Análisis de investigación

El análisis de investigación es el factor central para recopilar información, evaluarla con el fin de utilizar la información más apta para responder las dudas o interrogantes que se tenga en el proceso, en este caso haciendo referencia al: Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma de seguridad ISO/IEC 27001-27002 para la empresa AIRMAXTELECOM Soluciones Tecnológicas S.A.

1.1.2. Preguntas de investigación

Se elaboraron preguntas de investigación (PI) específicas para cada objetivo en la Tabla 1, con la finalidad de tener una estructura para la revisión de la literatura basado en el tema de titulación.

Tabla 1 *Preguntas de Investigación*

No	Preguntas de investigación	Motivación
PI 1	¿Qué son los activos de información, datos sensibles y confidenciales?	Permitirá conocer de una mejor forma cuales son los activos sensibles que la empresa debe cuidar y mantener en confidencialidad que las personas han brindado por un servicio.
PI 2	¿Cuáles son los riesgos de seguridad de la información que está propensa una empresa?	Permitirá conocer cuáles son los riesgos a los cuales se encuentra vulnerable la información y tomar las medidas necesarias para controlarlo.
PI 3	¿Cuáles son las etapas de un Sistema de Gestión de Seguridad de la información?	Conocer y comprender los procesos que en cada etapa se deben aplicar de forma efectiva en las empresas, mejorando de forma continua la seguridad de la información.

PI 4	¿Cuál es la mejor forma de adoptar un SGSI en las empresas y mejorar su seguridad en la información?	Es un punto fundamental en el cual se tendrá un pilar para conocer como ha sido el proceso de adoptar un SGSI y que beneficios tiene para la seguridad de la información.

Nota. Elaboración propia

1.1.3. Búsqueda de documentos

La finalidad de la búsqueda de documentos es realizar la investigación de información que permita obtener más información correspondiente a las interrogantes de investigación. Se tomará información de bases de datos bibliográficas como: ScienceDirect, Scopus, IEEE Xplore, Google Scholar y diversos repositorios digitales. La cadena de búsqueda que se implementó para la búsqueda

> (“Information Security Management System”) AND (“Information AND Security AND Management AND System) AND (“ISO 27001” AND “ISO 27002”)

de información se presenta a continuación:

1.1.4. Selección de artículos

Como se visualiza en la Tabla 2, se realizó la búsqueda y selección de diferentes artículos y trabajos de investigación

Tabla 2 *Procesos de elección de artículos*

Tipo de documento	Etapa 1	Etapa 2
Artículos científicos.	43	20
Trabajos de investigación.	13	12
Total	56	32

Nota. Elaboración propia

Se realizó la búsqueda y selección de la documentación con un valor total de 32 documentos, los cuales tuvieron una mejor respuesta correspondientes a 20 artículos científicos y 12 trabajos de investigación como se muestra en la Tabla 3:

Tabla 3 *Documentos seleccionados*

Código	Título	Base de datos	Autor/es	Año
A1	Information security risk management models for cloud hosted systems: A comparative study	ScienceDirect	Irsheid A	2022
A2	Security and Privacy Controls for Information Systems and Organizations	Nistpubs	Task Force, Joint	2020
A3	Problems of Implementing Information Security Management Systems	IEEE Xplore	Svetlana V	2020
A4	Cyber-Secure SDN: A CNN-Based Approach for Efficient Detection and Mitigation of DDoS attacks	Scopus	Najar A	2024
A5	Information security management in ICT and non-ICT sector companies: A preventive innovation perspective	ScienceDirect	Mona M	2021
A6	Implementation of the Risk-based Approach Methodology in Information Security Management Systems	IEEE Xplore	Mark N	2021
A7	Assessment of Information Security in Integrated Systems	IEEE Xplore	Tatyana Y	2021
A8	Research on security management and control system of information system in IT governance	IEEE Xplore	Zhang J	2011
A9	Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private organizations in Sweden	Scopus	Kamil Y	2023
A10	The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector	Scopus	Kitsios F	2023
A11	Rationality constraints in cyber defense: Incident handling, attribution and cyber threat intelligence	ScienceDirect	Hinne H	2021
A12	Digital media system design and visual art analysis based on information security	ScienceDirect	Li k	2024

A13	The impact of information security management guide utilization on technological and institutional information security measures in university libraries in Türkiye	ScienceDirect	Kavak A	2023
A14	Improving the quality of information security management systems with ISO27000	Journal	Gillies A	2011
A15	Information Security Management System in Distributed Information Systems	IEEE Xplore	Pleskach V	2019
A16	Research on Information Security Protection System of Industrial Control System	IEEE Xplore	Zou Z	2020
A17	Methodology for the Synthesis of Acceptable Options for Organizational Functional Structure of the Security Management System of a Significant Object of Critical Information Infrastructure	IEEE Xplore	Valentin V	2022
A18	Information Systems and Technologies in Quality Management	IEEE Xplore	Svetlana	2020
A19	Advanced Information Security Management Evaluation System	Journal	Heasuk J	2011
A20	Development of a new IEC Technical Report on System Software Vulnerability Management and System Software End-Of-Life Management for I&C and Electrical Power Systems in Nuclear Power Plants	Scopus	Bochtler J	2023

Nota. Elaboración propia

En la Tabla 4 se encuentra la información seleccionada de los trabajos de investigación.

Tabla 4 *Trabajos de investigación*

Código	Título	Base de datos	Autor/es	Año
T1	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO	EndNote	YEZID C	2014

	27001 Y 27002 PARA LA UNIDAD DE INFORMÁTICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE NARIÑO			
T2	Diseño de auditoría de un SGSI – Sistema de Gestión de la Seguridad de la Información, basado en ISO 27001	Espol	Chang A	2017
T3	Análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001- sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros	UPS	Molina K	2015
T4	Metodología del SGSI según la norma ISO/IEC 27001 para el Gobierno Autónomo Descentralizado de San Miguel de Urcuquí	UTN	Valencia H	2016
T5	Sistema de gestión de seguridad de la información para Emel Norte prototipo: proceso de levantamiento de un nuevo cliente	UTN	Gordillo A	2017
T6	Sistema de gestión de seguridad de la información (SGSI) en el Comando Provincial de Policía Imbabura Nro. 12.	UTN	Diaz P	2013
T7	Diseño de un Sistema de Gestión de la Seguridad de la Información para el Departamento de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte basado en la Norma ISO/IEC 27001	UTN	Guzmán S	2023
T8	Auditoría de seguridad informática en la red interna de la Universidad Técnica del Norte según la metodología Offensive Security Professional Training and Tools For Security Specialists y planteamiento de políticas de seguridad basadas en la norma ISO/IEC 27001	UTN	León M	2017

T9	Estudio de la seguridad en big data, privacidad y protección de datos mediante la ISO/IEC 27007:2017- aplicado a los datos académicos de la Universidad Técnica del Norte	UTN	Hernández C	2019
T10	Elaboración e implementación del manual de políticas y normas de seguridad informática para la empresa Eléctrica Regional Norte S.A. - EMELNORTE	UTN	Orejuela A	2015
T11	Diseño de un plan de gestión de riesgos tecnológicos con la metodología MAGERIT V3 basada en la norma ISO/IEC 31000, para fortalecer la gestión de amenazas y riesgos en los Laboratorios de informática de la facultad de ingeniería en ciencias de la Universidad Técnica del Norte	UTN	Sevilla E	2023
T12	Estudio de la normativa ISO 27002:2017 para el desarrollo de una aplicación web de registro y seguimiento de mediciones antropométricas de deportistas para la Federación Deportiva de Imbabura	UTN	Trávez C	2019

Nota. Elaboración propia

1.2. Sistema de Gestión de Seguridad de la Información (SGSI)

Un sistema de gestión de seguridad de la información es un conjunto de políticas y normas de información en las que se utiliza recursos y actividades a nivel administrativo de una organización con la finalidad de proteger la información de los usuarios, tiene un enfoque en monitorizar y mejorar la seguridad de la información de una organización(Alvarado Claudia, 2021).

1.2.1. Definición de un SGSI

El Sistema de Gestión de Seguridad de la información (SGSI) es una parte fundamental para un sistema de gestión organizado, enfocándose en los riesgos que pueden presentarse en una organización principalmente en la seguridad de la información, este sistema no solo permite como punto

importante reducir los riegos que tienen relación con la información, también se puede tener una ventaja considerable y competitiva en el mercado ya que se diferenciará de las demás organizaciones(Aleksandrova , 2020).

Se define como modelos de seguridad los cuales proporcionan metodologías más adecuadas para la seguridad de la información, son procedimientos los cuales en cada paso ayudan a mejorar y fortalecer la seguridad de la información basados en evaluación de riesgos, vulnerabilidades, amenazas, establecimiento de políticas en las cuales se maneja la integridad y la disponibilidad de la información, garantizando que se encuentre segura en el lugar donde se encuentres almacenados ya sea en su forma física o lógica(Irsheid et al., 2022).

Se establece ciertos pasos los cuales vas desde el apoyo de la alta dirección, alcance del SGSI, inventario de activos de la información, incluyendo la información como bases de datos, copias de seguridad y repositorios, personal tanto financiero como lega, servidores, dispositivos de red, infraestructura, hardware, software, activos humanos como el talento humado, evaluación y tratamiento de riesgos, políticas de seguridad de la información, son pasos de los procesos fundamentales para plantear un esquema de seguridad de la información.

1.2.2. Beneficios e importancia de un SGSI

Este sistema está enfocado en la gestión de la seguridad de la información la cual es fundamental que las organizaciones adapten en su marco de trabajo, estableciendo procesos estructurados y debidamente documentados, este modelo es ha sido creado con la finalidad de monitorear, mantener y tener una mejora continua en la seguridad de la información, en la siguiente Tabla 5 y en la Figura 4 se muestra los beneficios que conlleva tener un SGSI en las organizaciones:

Tabla 5 *Beneficios de un SGSI*

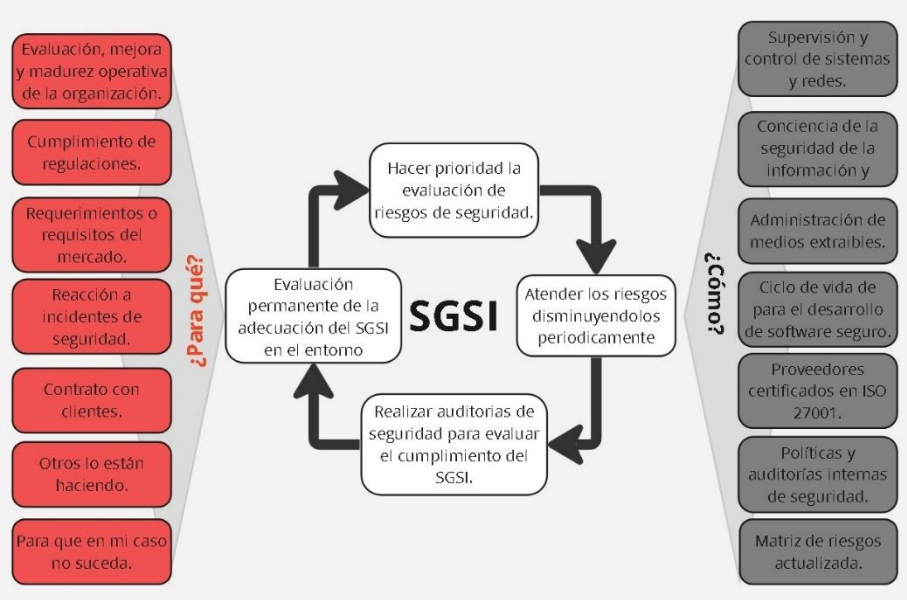
Involucrar a la Dirección en la seguridad de la información.
Desarrollar políticas de cumplimiento de cumplimiento obligatorio.
Conocer realmente de qué activos dispone la organización.
Cumplir con la legislación vigente ligada al proyecto.
Realizar análisis de riesgos para el desarrollo de la organización.
Introducción de contratos de niveles de servicio.
Reforzar la seguridad ligada al personal y a la información.
Disponer de planes de contingencia ante incidentes.
Disponer planes de continuidad del negocio y recuperación ante desastres.

Desarrollo de indicadores de desempeño del SGSI.

Disminución de riesgos a niveles aceptables.

Nota.: (Guerrero, 2014)

Figura 4 *Beneficios de un SGSI*



Nota: (Lopez, 2023)

1.2.3. Fases de un SGSI

En un SGSI el cuerpo se conforma de diversas etapas, las cuales pretenden mediante su proceso garantizar la seguridad de la información en donde quiera que se encuentre almacenada dentro de la organización, es importante establecer objetivos específicos centrándose en la seguridad de la información y también en los activos fijos, se establece la evaluación y monitoreo para generar políticas de seguridad de acuerdo al departamento en el que se encuentre y por consiguiente delegar responsables, los cuales son parte fundamental para que el SGSI funcione de manera óptima y mantener la seguridad y la integridad de la información.

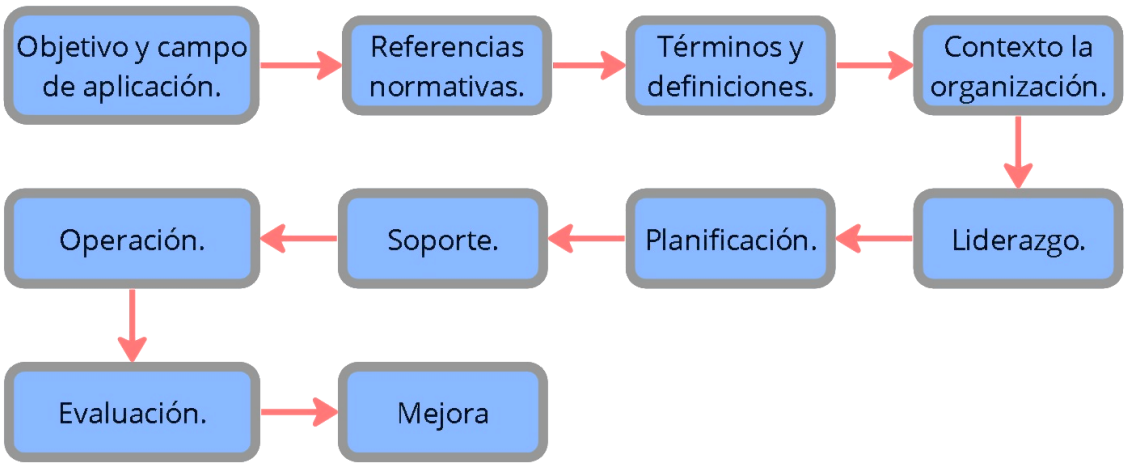
Además de establecer procedimientos de seguridad, es esencial mantener un estudio constante y análisis de la organización para una mejora continua a nivel organizacional contando con el apoyo y aprobación de la alta dirección. A continuación, en la Tabla 6 y en la Figura 5 se presenta los puntos generales de las fases de un SGSI:

Tabla 6 *Fases de un SGSI*

Fases	Contexto
Fase 1	Ámbitos de aplicación.
Fase 2	Referencias normativas.
Fase 3	Términos y definiciones.
Fase 4	Contexto de la organización.
Fase 5	Liderazgo.
Fase 6	Planificación.
Fase 7	Apoyo.
Fase 8	Operación.
Fase 9	Evaluación del funcionamiento.
Fase 10	Mejora.

Nota. Elaboración propia

Figura 5 *Fases del SGSI*



Nota: ISO/IEC 27000 (Edgar Leopoldo Martínez)

1.3. Norma ISO

Contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI) utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

1.3.1. Organización Internacional para la estandarización (ISO)

Las normas ISO son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización, se encargan de establecer estándares y guías relacionados con sistemas de gestión y aplicables a cualquier tipo de organización internacionales y mundiales, con el propósito de facilitar el comercio, facilitar el intercambio de información y contribuir a la transferencia de tecnologías.

1.3.2. Comisión Electrotécnica Internacional (IEC)

La Comisión Electrotécnica Internacional, es la encargada de diseñar y establecer las normas que ayudan a verificar la seguridad en las organizaciones en los diferentes dispositivos electrónicos en los cuales se maneja la información a nivel global, tiene como punto importante en la certificación de conformidad de los productos, asegurando que se cumplan a cabalidad los estándares que se imponen para su uso (Aula Mentor, 2016).

1.3.3. Norma ISO/IEC 27001:2022

La seguridad de la información, según la ISO 27001, se basa en la preservación de su confidencialidad, integridad y disponibilidad, así como la de los sistemas aplicados para su tratamiento.(Aula Mentor, 2016)

1.3.4. Norma ISO/IEC 27002:2022

Según (Normas ISO, 2005),Los requisitos de la Norma ISO 27001 norma nos aportan un Sistema de Gestión de la Seguridad de la Información (SGSI), consistente en medidas orientadas a

proteger la información, indistintamente del formato de esta, contra cualquier amenaza, de forma que garanticemos en todo momento la continuidad de las actividades de la empresa.

Los Objetivos del SGSI son preservar la:

Confidencialidad, Integridad y Disponibilidad de la Información.

Según (ISO/IEC, 2022) es una norma internacional que proporciona orientación para las organizaciones que buscan establecer, implementar y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) centrado en la ciberseguridad.

La ISO/IEC 27002 ofrece las mejores prácticas y objetivos de control relacionados con aspectos clave de ciberseguridad, como el control de acceso, la criptografía, la seguridad de los recursos humanos y la respuesta a incidentes. La norma sirve como un modelo práctico para las organizaciones que buscan salvaguardar eficazmente sus activos de información contra las amenazas cibernéticas. Siguiendo las directrices ISO/IEC 27002, las empresas pueden adoptar un enfoque proactivo para la gestión de riesgos de ciberseguridad y proteger la información crítica del acceso no autorizado y la pérdida, en la Figura 6 se muestra los puntos principales de la norma.(ISO/IEC, 2022)

Figura 6 *Puntos principales norma ISO 27002:2022*

Nota: (ICS, 2019)

1.3.5. Comprensión de los riesgos y amenazas a la seguridad de la información en el entorno actual.

Como se menciona en (Software Engineering Institute, 2023). Los riesgos y amenazas a la seguridad de la información son cada vez más sofisticados y cambiantes debido a la evolución tecnológica y la interconexión global. Algunos ejemplos de riesgos y amenazas incluyen ataques cibernéticos, malware, phishing, ingeniería social, robo o pérdida de dispositivos, desastres naturales y errores humanos. Es fundamental comprender estos riesgos para implementar controles adecuados y mitigarlos efectivamente.

1.3.6. Beneficios y objetivos estratégicos de contar con un SGSI.

Los beneficios de contar con un SGSI bien implementado incluyen:

- Un mayor nivel de protección de la información sensible y los activos críticos de la organización.
- Aumento en la confianza de los clientes, usuarios y socios comerciales.
- Fidelidad a los requerimientos legales y regulatorios relacionados con la protección de datos.
- Reducción de incidentes de seguridad y su impacto en la organización.
- Mayor capacidad de recuperación frente a desastres o incidentes de seguridad.

Los objetivos estratégicos del SGSI suelen alinearse con los objetivos generales de la organización, asegurando la sostenibilidad, competitividad y continuidad del negocio a largo plazo.(Force, 2020)

1.4. Políticas de seguridad de la información

Las políticas de información son lineamientos que contienen los recursos necesarios para el manejo en cuanto a la tecnología, información, activos físicos y lógicos se habla, son normativas las cuales hay que cumplir a cabalidad conforme sean establecidas por el personal responsable y capacitado, estando en conocimiento de todo lo que comprende la empresa en la que se está insertando políticas de seguridad, tiene la finalidad de tener un mejor control en el campo de organización y seguridad, maneja la gestión de incidentes, proteger la información que se maneja tanto interna como externa, realizar auditorías en las cuales se asegura que se esté cumpliendo paso a paso todas las normativas establecidas, deben ser de conocimientos para todo el personal que se encuentra involucrado en su ejecución y constante puesta en práctica.

1.4.1. Importancia de establecer el numero adecuado de políticas claras y coherentes para encaminar las buenas prácticas de seguridad de la información.

Según (Force, 2020) las políticas de seguridad de la información son el marco fundamental para establecer directrices y principios que guían las prácticas de seguridad dentro de una organización. Estas

políticas definen las reglas, responsabilidades y expectativas relacionadas con la protección de la información y los activos de la organización. Al establecer políticas claras y coherentes, se logra lo que se muestra en la Tabla 5 siguiente:

Tabla 7 *Importancia de las políticas de seguridad*

Importancia	Conceptos
Unificación de criterios	Las políticas aseguran que todos los miembros de la organización entiendan y apliquen las mismas prácticas de seguridad, lo que reduce la confusión y la inconsistencia en las acciones relacionadas con la protección de la información.
Mitigación de riesgos:	Al establecer reglas específicas y medidas de seguridad, las políticas ayudan a reducir las vulnerabilidades y los riesgos de seguridad de la información, protegiendo a la organización de posibles amenazas.
Cumplimiento normativo	Las políticas de seguridad ayudan a la organización a cumplir con los requisitos legales y normativos relacionados con la protección de datos y la privacidad.
Respuesta a incidentes	Las políticas proporcionan una base para abordar y resolver los incidentes de seguridad de manera eficiente y efectiva.

Nota: (Software Engineering Institute, 2023)

1.4.2. Contenido y estructura típica de las políticas de seguridad de la información.

Las políticas de seguridad de la información generalmente incluyen los siguientes elementos:

- Título y propósito: Define el objetivo general de la política y su alcance.
- Alcance: Describe a qué áreas o sistemas de la organización se aplica la política.
- Responsabilidades: Establece las responsabilidades de los empleados, gerentes y otros actores relacionados con la seguridad de la información.

- Definición de términos: Aclara los conceptos clave utilizados en la política.
- Políticas específicas: Enumera las reglas y directrices específicas relacionadas con la seguridad de la información, como el acceso a sistemas, el uso de contraseñas, el cifrado, la clasificación de datos, entre otros.
- Cumplimiento y consecuencias: Detalla las consecuencias del incumplimiento de las políticas y las medidas disciplinarias asociadas.
- Procedimiento de revisión: Especifica cómo se revisará y actualizará la política periódicamente.(NIST, 2023)

1.4.3. Proceso para desarrollar, aprobar, comunicar y revisar las políticas de seguridad.

- El proceso para desarrollar, aprobar, comunicar y revisar las políticas de seguridad de la información generalmente sigue estos pasos:
- Identificación de necesidades: Se determinan las áreas y temas clave que deben abordarse en las políticas de seguridad, basándose en los riesgos y requisitos específicos de la organización.
- Desarrollo y redacción: Se redactan las políticas en colaboración con expertos en seguridad y otras partes interesadas. Esto incluye definir los elementos estructurales mencionados en el punto anterior.
- Aprobación: Las políticas proceden a ser revisadas y aprobadas por la alta dirección y otros responsables para garantizar que estén alineadas con los objetivos de la organización.
- Comunicación: Una vez aprobadas, las políticas deben ser comunicadas clara y efectivamente a todos las partes interesadas relevantes.
- Revisión y actualización: Las políticas deben revisarse periódicamente y actualizarse según se considere pertinente para adaptarse a los cambios en el entorno de seguridad y los riesgos asociados.(CIBERSEGURIDAD, 2020 C.E.)

1.4.4. Relación entre las políticas de seguridad y otros componentes del SGSI, como procedimientos y directrices.

Para la importante relación (Perez Ramiro, 2023) menciona la importancia de destacar que cada organización puede tener estructuras y enfoques ligeramente diferentes para sus políticas de seguridad, como se muestra en Tabla 6. La adaptación de estos conceptos a la realidad específica de cada empresa es fundamental para garantizar una gestión efectiva de la seguridad de la información.

Tabla 8 *Relación entre políticas y un SGSI*

Políticas	SGSI
Las políticas de seguridad de la información son el nivel más alto de orientación y establecen los principios generales para la seguridad. Los procedimientos y directrices operativas, por otro lado, son más detallados y específicos, proporcionando instrucciones sobre cómo implementar las políticas en situaciones concretas.	Las políticas proporcionan el marco y la dirección para el desarrollo de procedimientos y directrices coherentes y consistentes. Estos tres componentes están interconectados y trabajan juntos para lograr una seguridad de la información efectiva y bien gestionada en toda la organización. Los procedimientos y directrices deben estar alineados con las políticas para asegurar que las prácticas de seguridad sean uniformes y estén alineados con los objetivos tácticos de la organización

Nota: (Seguridad de personas y bienes, 2017)

1.4.5. Organización de la seguridad de la información:

Roles y responsabilidades de los actores clave en la gestión de la seguridad de la información (por ejemplo, CISO, comité de seguridad, usuarios

- Chief Information Security Officer (CISO): El CISO es el responsable principal de la seguridad de la información en las organizaciones. Su función incluye desarrollar y supervisar la estrategia de seguridad, asegurando la protección de los activos de información, la gestión de riesgos, implementación de controles de seguridad. También es responsable de coordinar la respuesta a incidentes de seguridad y garantizar el cumplimiento de las políticas relacionadas con la seguridad de la información.
- Comité de Seguridad: El Comité de Seguridad es un grupo formado por representantes de diferentes áreas y niveles a nivel interno de una organización. Su objetivo es proporcionar asesoramiento y apoyo al CISO en la toma de decisiones que se relacionan con la seguridad de la información. El Comité revisa y aprueba las políticas, procedimientos de seguridad, así como los recursos y presupuestos asignados a la seguridad.(Manejo de información, 2022)
- Usuarios: Los usuarios son empleados, contratistas y cualquier otra persona que acceda a los sistemas y activos de información. Aunque no ocupan posiciones de liderazgo en la gestión de la seguridad, son actores clave en la implementación de las políticas y controles de seguridad. Su responsabilidad incluye el uso adecuado de los sistemas y datos, la protección de contraseñas y

credenciales, la notificación de incidentes de seguridad y la participación en programas de concienciación, capacitación y formación en temas relacionados con la seguridad.(DIRECTRICES DE SEGURIDAD DE LA INFORMACIÓN, 2018)

1.4.6. Gestión de activos

1.4.7. Identificación de los activos de información de la organización.

El primer paso que (Rodriguez Johanna, 2022) menciona, se realizan en la gestión de activos es identificar y clasificar los activos de información de la organización. Esto implica identificar todos los activos relevantes, como sistemas, bases de datos, aplicaciones, dispositivos, datos, documentos que contenga información valiosa para la organización. Luego, se deben clasificar los activos según su valor, importancia, sensibilidad y criticidad para el negocio.

Es importante asignar responsabilidades claras para la gestión y protección de cada activo específico. Esto implica designar propietarios y responsables que sean responsables de mantener y salvaguardar cada activo. Los propietarios deben comprender sus responsabilidades y estar empoderados para tomar decisiones relacionadas con la seguridad y el manejo del activo asignado. (IBM, 2023)

1.4.8. Procesos para el almacenamiento seguro, respaldo y disposición de activos de información.

La organización debe establecer procesos para garantizar el almacenamiento seguro, respaldo y disposición adecuada de los activos de información. Esto incluye:

- Almacenamiento seguro: Establecer medidas para proteger física y lógicamente los activos, como sistemas y dispositivos, de amenazas físicas y cibernéticas.
- Respaldo: Implementar rutinas regulares de copias de seguridad para garantizar que la información crítica esté protegida contra pérdidas o daños. Los datos respaldados deben almacenarse en ubicaciones seguras.
- Disposición segura: Desarrollar un proceso para la eliminación segura de activos que ya no se necesiten o estén fuera de uso. Esto puede implicar el borrado seguro de datos y el reciclaje adecuado de dispositivos.

1.4.9. Controles de acceso

La autenticación y autorización de usuarios y sistemas es esencial para garantizar que solo se permita el acceso autorizado, es fundamental proteger los activos de información. Los controles físicos incluyen el uso de tarjetas de acceso, cerraduras, vigilancia, y controles de ingreso a áreas sensibles. Los controles lógicos, por otro lado, involucran autenticación y autorización de usuarios en sistemas

informáticos mediante contraseñas, claves criptográficas, autenticación biométrica, entre otros. Estas medidas aseguran que solo personas autorizadas puedan ingresar a áreas físicas o acceder a recursos informáticos.

La autenticación según menciona (Poomas Das, 2022) es el proceso de verificar la identidad de un usuario o sistema, mientras que la autorización determina qué recursos o funciones están disponibles para ese usuario o sistema una vez autenticado. Se deben implementar mecanismos o procesos robustos de autenticación, dado el caso: contraseñas seguras, autenticación multifactor (MFA) o biometría, para asegurar que solo usuarios autorizados puedan acceder a los sistemas y datos sensibles. Además, la autorización debe establecer qué acciones específicas están permitidas para cada usuario o grupo de usuarios, con base en sus roles y responsabilidades.

El monitoreo y la auditoría de actividades de acceso son esenciales para detectar comportamientos sospechosos o intentos no autorizados de acceso. Mediante la implementación de soluciones de monitoreo de seguridad y auditoría, la organización puede registrar y analizar eventos relacionados con el acceso a sistemas y datos sensibles. Esto permite identificar posibles infracciones de seguridad, detectar comportamientos anómalos y responder rápidamente a incidentes de seguridad.(Suárez Mirella Bernal, 2023)

1.4.10. Criptografía – Cifrado y gestión de claves

Importancia de una gestión adecuada de claves para garantizar la integridad y disponibilidad de la información cifrada.

La gestión adecuada de claves es esencial para garantizar la integridad y accesibilidad de la información cifrada. Las claves criptográficas son componentes críticos del proceso de cifrado y descifrado. Una mala gestión de claves puede comprometer la seguridad de los datos cifrados. Es necesario implementar prácticas de gestión de claves seguras, como el almacenamiento seguro de las claves, rotación periódica de claves, y limitar el acceso a las claves solo a personal autorizado. La gestión adecuada de claves también es esencial para evitar la pérdida de acceso a la información en caso de que se pierdan o dañen las claves.(Revista IMG, 2023)

1.4.11. Respaldo y recuperación de claves

El respaldo y la recuperación de claves son aspectos críticos de la gestión de claves para evitar la pérdida de acceso a la información cifrada. La pérdida de claves puede dar como resultado la pérdida de información que se encuentre cifrada, es necesario realizar copias de seguridad de las claves y mantener una copia segura fuera del sitio. También se deben establecer procedimientos de recuperación para garantizar que, en caso de extravío o daño de las claves, haya un proceso para recuperarlas y permitir el acceso a la información cifrada.(Rocha Alex, 2021)

1.4.12. Seguridad en el manejo y almacenamiento de soportes físicos (papel, discos duros, cintas) que contienen información sensible.

El manejo y almacenamiento adecuado de soportes físicos que contienen información sensible es esencial para evitar pérdida o exposición de datos. Algunas prácticas recomendadas incluyen:

- Almacenamiento seguro: Mantener los soportes físicos en áreas seguras y restringidas con acceso controlado.
- Etiquetado y registro: Etiquetar y registrar los soportes físicos para rastrear su ubicación y contenido.
- Destrucción segura: Implementar procedimientos de destrucción segura para soportes físicos que ya no se necesiten, como la trituración de discos duros o el uso de servicios de destrucción certificados(S Blog, 2022)

1.4.13. Seguridad operacional

La seguridad operacional comprende la gestión y la aplicación de normativas adaptadas a la seguridad conforme sea necesario en una organización, garantizando en un alto porcentaje la protección de los activos que maneja la empresa, puede incluirse los procesos con los cuales se rigen, manteniendo un plan de continuidad y seguridad para seguir ofreciendo el servicio a los usuarios.

1.4.14. Implementación de directrices para prevenir y detectar malware y software malicioso.

La implementación de controles para la prevención y detección de malware y software malicioso es fundamental para proteger los sistemas y datos. Algunas medidas de control incluyen:

- Uso de software de seguridad: Implementar soluciones antivirus, antimalware y firewalls para proteger contra amenazas cibernéticas.
- Actualizaciones preventivas y correctivas de software: Mantener los sistemas y aplicaciones actualizados y habilitados los parches de seguridad.
- Filtrado de contenido web: Utilizar filtros de contenido o accesos web para bloquear el ingreso a sitios web maliciosos o inseguros.
- Educación y concienciación: Capacitar a los empleados para que sean conscientes de las amenazas de malware y cómo evitar ser víctimas de ataques.(Team Asana, 2022)

1.4.15. Planificación y pruebas de continuidad del negocio y recuperación ante desastres.

La planificación y las pruebas de continuidad del negocio y nivel de recuperación ante desastres son fundamentales para garantizar la agilidad de la organización para enfrentar y recuperarse de eventos catastróficos o interrupciones. Estas medidas incluyen:

- Identificación de riesgos: Identificar los riesgos potenciales y las amenazas que podrían afectar la continuidad del negocio.
- Planes de contingencia: Desarrollar planes de contingencia y recuperación que describan los procedimientos a seguir en caso de interrupciones o desastres.
- Pruebas y simulacros: Realizar pruebas y simulacros periódicos para asegurarse que los planes de contingencia sean efectivos y estén actualizados.(Manejo de información, 2022)
- Respaldo y recuperación de datos: Implementar sistemas de respaldo y recuperación de información para proteger y garantizar su recuperación en caso de pérdida.(Schwaker Eric, 2019)

1.4.16. Seguridad de las comunicaciones:

Se hace referencia a seguridad de las comunicaciones a las directrices o medidas que ayudan a fortalecer la seguridad con la finalidad de mantener la integridad de la información que se maneja, siempre y cuando se designen personas responsables en los diversos campos de la seguridad, puede comprender el tránsito de información, el almacenamiento de la misma, evitar en lo más posible la manipulación de información y que solamente esté disponible para personal autorizado, puesto que se debe contar con factores importantes como: Confidencialidad, integridad, disponibilidad, protección y cifrado, aspectos que se explican a continuación.

1.4.17. Uso de tecnologías seguras, como VPN y cifrado

El uso de tecnologías seguras, como las redes privadas virtuales (VPN) y el cifrado, es parte fundamental para mantener la integridad de la información transmitida por redes públicas o no confiables. Las VPN proporcionan un canal seguro y encriptado para la comunicación entre dispositivos y redes, lo que evita que terceros no autorizados accedan o intercepten los datos transmitidos. Además, el cifrado garantiza que los datos viajen en forma de texto cifrado y solo puedan ser descifrados por los destinatarios autorizados.(Innova Busines School, 2022)

- Uso de protocolos seguros: Utilizar protocolos de comunicación seguros, como HTTPS para sitios web, que utilizan cifrado para proteger la información transmitida.
- Firma digital: Utilizar firmas digitales para verificar la integridad y autenticidad de los datos transmitidos.

- Certificados de servidor: Implementar certificados de servidor para garantizar la identidad y autenticidad del servidor al que se está conectando.(CISCO, 2023)
- Autenticación sólida: Utilizar autenticación multifactor (MFA) para proteger las cuentas y datos almacenados en servicios en la nube.
- Encriptación de información de extremo a extremo: Utilizar aplicaciones de mensajería que admitan encriptar la información de extremo a extremo para proteger la integridad de las conversaciones.
- Evaluación de proveedores: Al seleccionar servicios en la nube, evaluar cuidadosamente los proveedores en términos de su seguridad, cumplimiento y medidas de protección de datos.(CISCO, 2023)

1.4.18. Identificación y corrección de vulnerabilidades mediante pruebas de seguridad y revisión de código.

Las pruebas de seguridad y la revisión de código mencionadas por (David Castañeda Echeverri & Adolfo Villegas Villegas, 2020) son prácticas esenciales para identificar y corregir vulnerabilidades en sistemas y aplicaciones. Las pruebas de seguridad en la construcción, como las pruebas de infiltración y las pruebas de vulnerabilidad, se utilizan para evaluar la resistencia del sistema ante intentos de explotación y para identificar posibles debilidades. Por otro lado, las revisiones de código implican la revisión minuciosa del código fuente por parte de desarrolladores y expertos en seguridad para identificar errores y vulnerabilidades de programación.

1.4.19. Conocimiento y cumplimiento de leyes, regulaciones y estándares relevantes basados en la seguridad de la información.

Es esencial que la empresa esté al tanto de las leyes, reglamentos y normas de seguridad de la información que apliquen. La Ley de Protección de Datos, el Reglamento General de Protección de Datos (GDPR) de Europa, la Ley de Privacidad del Consumidor de California (CCPA) de los Estados Unidos y la norma ISO 27001 para la gestión de seguridad de la información son algunos ejemplos de regulaciones y estándares comunes. Para proteger los datos de los clientes, empleados y socios comerciales y evitar posibles sanciones y responsabilidades legales, es esencial cumplir con estas leyes y estándares.(Auditool, 2023)

1.4.20. Realización de auditorías internas y externas.

Las auditorías internas y externas son importantes para evaluar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) y garantizar la ejecución y el cumplimiento de las reglas, procedimientos y estándares establecidos. Las auditorías externas son realizadas por terceros independientes, como empresas de auditoría o entidades certificadoras, mientras que las auditorías internas son realizadas por personal interno o equipos de auditoría de la organización. Estas auditorías

identifican factores físicos y lógicos de mejora, riesgos potenciales y oportunidades para mejorar la seguridad de la información.(En et al., 2014)

1.4.21. Mantenimiento de registros y documentación.

Es esencial mantener registros y documentación detallada sobre las actividades y controles implementados en el SGSI. Estos registros y documentos sirven como evidencia para demostrar el cumplimiento de leyes, regulaciones y estándares, y también para respaldar la efectividad de los controles implementados. La documentación también facilita las auditorías y evaluaciones internas y externas, ya que proporciona una visión clara de las prácticas de seguridad de la información y las acciones tomadas para proteger los activos de información.(ISO 27001, 2021)

1.5. Mejores formas de adopción de un SGSI.

En las empresas, cada que pasa el tiempo, se han vuelto vulnerables a ataques a su activo más valioso como lo es la información, cada vez más, han generado la necesidad de adoptar sistemas de gestión de seguridad de la información en las organizaciones, basándose en un estudio en Alemania, según (Berg y Niemeier, 2019), señala que el 70% de las organizaciones han recibito o ha sido atacadas digitalmente en el año 2019, es por ello que la adopción de un SGSI es de vital importancia, su finalidad es proteger los activos, la información y generar un plan para la gestión de riesgos, cumpliendo a cabalidad los principios de seguridad, basado en las normas ISO 27001 – 27002, uno de los marcos de gestión de seguridad reconocido como líder para la seguridad y su gestión, algunas de las ventajas de la adopción de un SGSI son las que se muestran en la Figura 7:

Figura 7 *Como implementar el SGSI paso a paso*

Nota: (OYARZÚN G, 2023)

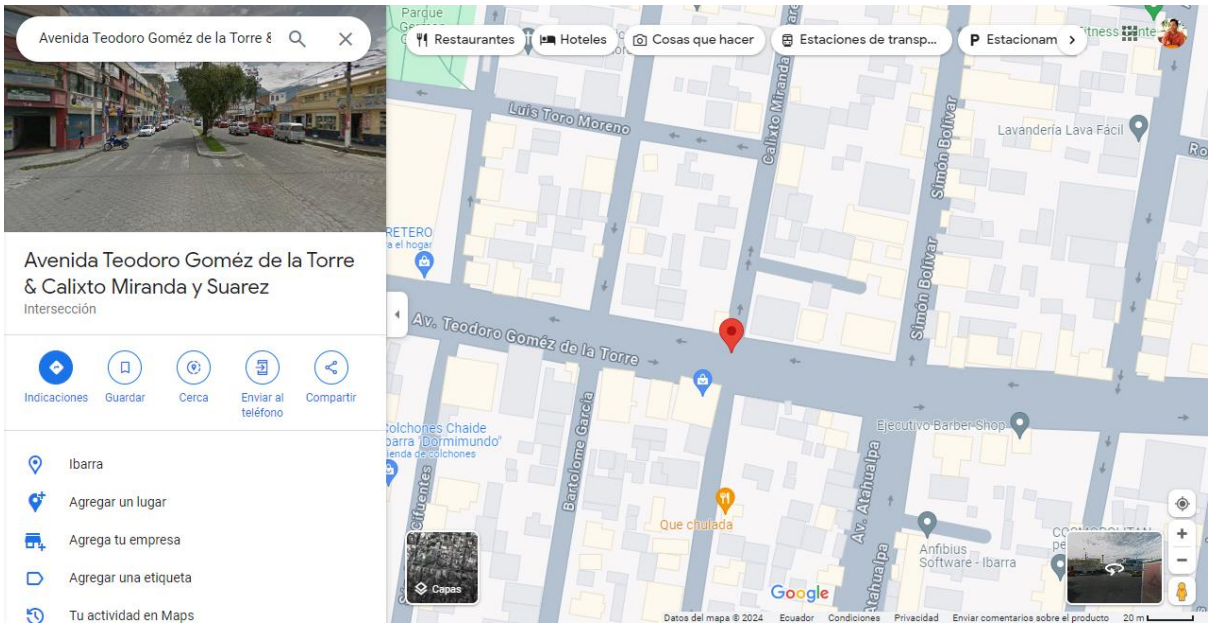
1.6. Análisis de la situación actual de la empresa

La empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A, es una empresa la cual presta el servicio de internet para la comunidad, cuenta con varios planes de internet accesibles para todo tipo de usuarios, cuenta con servicio al cliente, soporte técnico, y se encuentran innovando en su catálogo de ventas para aumentar productos relacionados con la comunicación, internet y seguridad.

Es una empresa dedicada a la prestación de servicios de telecomunicaciones y que a través de la implementación de la Norma ISO 9001:2015, atiende los requerimientos, necesidades de los clientes y normativa legal aplicable.

La empresa u Oficina Matriz se encuentra ubicada en las calles Avenida Teodoro Gómez de la Torre & Calixto Miranda y Suarez esquina como se muestra en la Figura 8.

Figura 8 *Ubicación actual de la empresa*



Nota.: (Google Maps, 2024)

1.6.1. Objetivos de calidad

- Mantener un adecuado nivel de satisfacción del cliente aplicable en el medio.
- Certificarnos con la Norma ISO 9001:2015 hasta abril 2024.
- Fomentar una cultura organizacional que priorice la satisfacción del cliente.
- Alcanzar un máximo de 0,52% de tasa de deserción de clientes con base a la cartera total en el 2026.

1.6.2. Misión

La empresa AIRMAXTELECOM tiene como misión conectarse al mundo a familias y empresas a través de servicios de telecomunicaciones innovadores y de calidad.

1.6.3. Visión

La empresa AIRMAXTELECOM tiene como visión ser la empresa referente de excelencia en atención al cliente, a través de la estandarización, automatización de procesos y protección de la información, con el fin de mejorar las expectativas de nuestras partes interesadas.

1.6.4. Valores

- Servicio: Mantenemos un alto sentido de colaboración hacia lo demás.
- Disciplina: El hábito que en la empresa generamos en base al compromiso y autocontrol.
- Integridad: Actuamos en base a nuestros principios.
- Calidad: Trabajamos para generar un servicio de mayor valor.
- Compromiso: Tomamos conciencia para cumplir los acuerdos.

1.6.5. Políticas

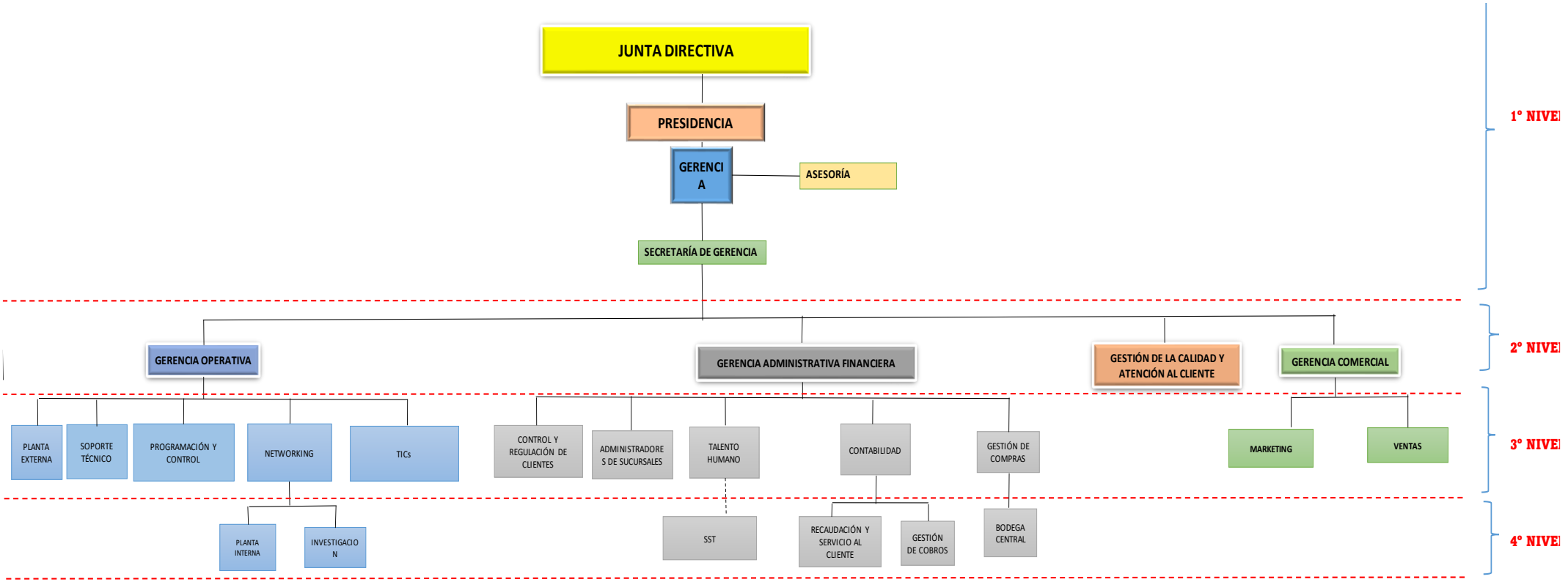
AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A. es una empresa dedicada a la prestación de servicios de telecomunicaciones y que a través de la implementación de la Norma ISO 9001:2015 atendemos los requerimientos, necesidades de los clientes y normativa legal aplicable.

Trabajamos de manera incansable y con procesos de mejora continua para proporcionar a nuestros clientes conectividad rápida, confiable y segura que les permita mejorar y facilitar su vida. Comunicamos la política de calidad a todas las partes interesadas.

En la Figura 9 se puede observar la estructura organizacional de la empresa por niveles con los departamentos que operan, dan funcionamiento y servicio al cliente.

1.6.6. Organigrama estructural

Figura 9 *Organigrama estructural*



Nota: AIRMAXTELECOM (2023). Organigrama estructural de la empresa

CAPÍTULO 2

Levantamiento de Activos y Evaluación de Riesgos de la Información

2.1. Generalidades

A continuación, se presenta los aspectos generales de la situación actual de la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A, la información que se abarca es de suma importancia y contiene puntos clave para conocer de mejor forma el contexto.

2.2. Tipo de Investigación

2.1.1. Investigación Aplicada

Esta investigación recopilo información del personal de la empresa, en cuanto se podía observar a simple vista y por experiencias propias en el establecimiento, se enfoca en conocer la situación actual de la empresa de internet ubicada en Ibarra.

2.1.2. Métodos de Investigación

Deductivo: Como punto de partida se dio el problema en el que se encontró la empresa, comenzar con la implementación de un SGSI para la empresa que planea certificarse en la norma ISO 27001 basada en la seguridad de la información, conociendo así sus activos de forma exacta y conocer sus vulnerabilidades y amenazas para realizar los procesos respectivos con cada uno.

Analítico: Al tener claros los activos con su respectivo análisis, se pudo determinar con más certeza los procesos a seguir para minimizar el riesgo, en su mayoría, disminuir la materialización y perderlos.

Exploratoria: Se realiza la exploración del campo y la información de la empresa en cuanto a la seguridad de la información con la finalidad de establecer preguntas de investigación y plantear hipótesis.

Cualitativa: Se enfoca en el análisis del factor social o humano, en este caso el personal que trabaja en la empresa para la recopilación de información que aporte a la mejora de la seguridad de la información.

Cuantitativa: Se enfoca en la recepción de datos representados en valores, valores referenciales para tener información más cercana a la realidad sobre la seguridad de la información.

2.3. Técnicas de Investigación

Como paso importante para el desarrollo continuo se adoptaron varias técnicas para recopilar la información, siendo estas: documentación de apoyo de la empresa, entrevistas con los encargados de los departamentos, observación de la situación en el campo se observa en la Tabla 9.

Tabla 9 *Técnicas de Investigación SGSI*

Técnicas	**Definición**
Revisión de Documentación	Al estar presente la documentación con base en los procesos o reglamentos implementados o implementándose en la empresa sobre el tratamiento de riesgos en la empresa. La documentación revisada que cuenta como más importante será el inventario de activos actualizado hasta la fecha de entrega, la información entregada por el encargado de sistemas en la cual se contaba con un acercamiento a la norma.
Entrevista	Se entrevistaron a los encargados de los departamentos que manejan información de la empresa interna y de los usuarios de forma externa, teniendo así una idea más clara de cómo es el manejo de la información, se abordó con preguntas específicas y enfocadas a la seguridad de la información, infraestructura, accesos.
Observación de Campo	La técnica se basa en la observación de lo físico en la infraestructura para obtener información de utilidad en cuanto a los activos disponibles en la empresa de internet, identificas si hay posibilidad de incidentes, amenazas que puedan comprometer la integridad de la información y a

la organización, se realizó la visita a los establecimientos en Ibarra con los que cuenta la empresa en la actualidad.

Nota: Elaboración Propia.

2.4. Directivos

Una vez realizada la entrevista con el personal, en este caso el asistente de gerencia de la empresa AIRMAXTELECOM se conforma de la siguiente manera como se presenta en la Tabla 10.

Tabla 10 *Nivel organizacional de la empresa*

	Nivel 2	Nivel 3	Nivel 4
Nivel 1	**Gerencia Operativa**	Planta Externa	
		Soporte Técnico	
		Programación y Control	
		Networking	Planta Interna
		Tics	Investigación
Junta Directiva			
Presidencia		Control y regulación de Clientes	
Gerencia			
Secretaría Gerencia	**Gerencia Administrativa Financiera**	Administradores de Sucursales	
		Talento Humano	SST
			Recaudación de Compras
		Contabilidad	
			Gestión de Cobros
		Gestión de compras	Bodega Central

Gestión de Calidad

Marketing

Gerencia Comercial

Ventas

Nota: AIRMAXTELECOM

2.5. Identificación del problema

La empresa AIRMAXTELECOM busca implementar la norma ISO 27001 en sus establecimientos funcionales. las calles Avenida Teodoro Gómez de la Torre & Calixto Miranda y Suárez esquina, empresa que cumple con el objetivo de proveer el servicio de calidad de internet para sus clientes, cuenta con una infraestructura adecuada para realizar sus funciones, ha implementado lugares físicos cercanos por el aumento de departamentos y personal de trabajo en su matriz Ibarra.

Busca llevar un control más minucioso con sus activos, instalaciones físicas, sistemas, buscando evitar, controlar, mitigar las vulnerabilidades y amenazas en el grado que sea posible, ya que es ciertos casos no siempre depende de la obra humana, puede haber escenarios medioambientales en los que será muy difícil llegar a un control adecuado, a este problema se le puede sumar los planes de recuperación o restablecimiento del servicio en el menor tiempo posible.

2.6. Introducción al Levantamiento de Activos

En el proceso de levantar información de los activos se encuentra información tal como se muestra en la Tabla 11.

Tabla 11 *Tipos de Activos y su descripción*

Tipos de Activos	Definición
Hardware	Componentes físicos de un sistema informático.
Software	Programas y aplicaciones informáticas que permiten el desarrollo de tareas específicas.
Infraestructura	Recursos y servicios indispensables para el desempeño de actividades.
Datos	Información que se almacena en sistemas informáticos como Data center, Nube, Unidades de almacenamiento.
Personas	Usuarios y trabajadores que comprenden la empresa para su funcionamiento.
Procesos	Flujos de trabajo, jerarquía, roles que están definidos para tareas específicas.

Nota. Elaboración propia

2.7. Importancia de Valoración e Identificación de Activos

La importancia que tiene un activo va de acuerdo con ciertos aspectos que en conjunto dan una idea más clara a si podría o no afectar a la seguridad de la información dentro de la empresa, a continuación, se presenta los aspectos que se evalúan:

- **Seguridad de la Información:** Los activos que se enfocan al almacenamiento y procesamiento de información basado en la seguridad de la información, accesos, información sensible, hardware, software, instalaciones, deben estar resguardadas, disminuyendo así posibles amenazas como daños, robos, entre otros.
- **Cumplimiento Normativo:** Debe estar sujetas y cumpliendo a cabalidad las normativas impuestas para la protección de datos en todos los aspectos que se maneje información.
- **Continuidad del Negocio:** Ciertos activos al verse comprometidos pueden causar que las actividades de la empresa no puedan desarrollarse con normalidad debido a su avería o perdida.
- **Protección de Reputación:** Información que al verse comprometida puede dañar la reputación del personal o la empresa como tal, provocando la pérdida de confianza en los usuarios.
- **Eficiencia Operativa:** Se enfoca en la gestión de los activos que maneja información en cuanto a su disponibilidad, criticidad, integridad dependiendo de cuál sea el caso.

2.8. Departamento de Tecnologías de la información

Las funciones del departamento de tecnologías son la organización de una empresa, encargada de la administración en el campo tecnológico, información y comunicación manteniendo la infraestructura, administrando los sistemas de información garantizando su seguridad y mejora continua, y el departamento también adquiere hardware y software para la gestión de proyectos, creación e implementación de políticas para la empresa.

2.8.1. Funciones Clave

Son funciones las cuales aportan valor y se enfocan en la habilidad estratégica de una empresa, con la finalidad de garantizar la continuidad de negocio de una organización, los más importantes con los que se cuenta en una empresa son los que se mencionan a continuación:

- **Redes:** Comprende el grupo de personas, unidades que se interrelacionan de forma electrónica o de forma física para tener un nivel de comunicación adecuado, con la mejora que ha tenido y ofrecido internet a sus usuarios mejorando y aumentando diversas formas de comunicarse como

puede ser, Face Time, Videollamadas, reuniones por Teams o Google Meet, manejo remoto de dispositivos con ayuda de aplicaciones como TeamViewer facilitan la labor desde los hogares.

- **Base de Datos:** Su funcionalidad es la de almacenamiento y procesamiento de datos y actividades en las cuales se maneja información importante y relevante, gestionando la información de la empresa de manera óptima, de forma que satisfaga las necesidades específicas de los usuarios autorizados a su manejo y control.
- **Sistema Contable:** La empresa tiene un sistema que controla todos los departamentos para operar local y remotamente disponible para dispositivos portátiles, móviles y celulares, actualmente la empresa está en proceso de migración a un nuevo sistema operativo para manejar información y procesos.

2.8.2. Niveles de seguridad

Es importante mencionar los niveles de seguridad para mantener la integridad y seguridad de la información, los niveles de seguridad pueden variar de acuerdo con cada organización, se presenta una Tabla 12 en la cual se clasifica los niveles de seguridad:

Tabla 12 *Niveles de Seguridad*

Nivel de Seguridad	Concepto
Seguridad Básica	Comprende la complejidad de las contraseñas, políticas de acceso, es un nivel que debe estar en cualquier organización.
Seguridad Física	Se refiere a la seguridad de las instalaciones físicas, controles de acceso al personal, alarmas, detectores de movimiento, cámaras, detectores de humo, seguridad en donde se manejen activos sensibles.
Seguridad Lógica	Controles de seguridad en los sistemas operativos, firewall, antivirus, protecciones ante amenazas o ataques cibernéticos.
Seguridad de la Red	La protección de la infraestructura de la red, cifrado y encriptación de la información, políticas de seguridad de la red que maneja la organización.
Seguridad de Datos	Protección de la integridad y confidencialidad de la información, clasificación y gestión de accesos.
Seguridad de Aplicaciones	Controles de seguridad, mantenimiento de aplicaciones, pruebas de seguridad, controles rutinarios
Seguridad Organizacional	Políticas, procedimientos en la organización, capacitaciones de seguridad de la información, gestión de riesgos, continuidad de negocio.

Nota. Elaboración propia

2.8.3. Controles Existentes

La empresa implementa en Ibarra ciertas normativas de control para controlar y minimizar los riesgos que puedan comprometer a los activos, las medidas que se manejan eficazmente dentro de la organización para continuar funcionando y proveer del servicio a sus clientes se especifica en la Tabla 13.

Tabla 13 *Controles en base a sus amenazas*

Amenazas	Controles	Efectividad
Físicas y medioambientales	• Permisos y controles por medio de un circuito cerrado de cámaras. • Backups.	• Si
Humanos	• Antivirus. • Firewall.	• Si
Personal	• Personal que brinda soporte.	• Si

Nota. Elaboración propia

2.9. Aspectos Iniciales

2.9.1. Alcance y Objetivos de SGSI

Es necesario definir alcances y objetivos acordados con la empresa AIRMAXTELECOM para la seguridad de la información.

Alcance del SGSI: El propósito para desarrollar este trabajo es Proponer un Sistema de Gestión de Seguridad de la Información para mitigar, asumir, transferir o eliminar las posibles amenazas que puedan comprometer la seguridad de la información en la empresa AIRMAXTELECOM Soluciones Tecnológicas S.A. El desarrollo de este SGSI, las actividades que serán fundamentales para asegurar el funcionamiento de la empresa y mantener la continuidad del negocio en la organización.

Objetivos específicos del SGSI:

- Obj 1: Levantamiento de activos y evaluación de riesgos de seguridad de la información a los que se enfrenta la empresa, considerando amenazas internas y externas, así como las posibles vulnerabilidades existentes en los sistemas y procesos.
- Obj 2: Garantizar la seguridad del sistema que maneja la empresa para el control de la información con la gestión de riesgos pertinente.
- Ojb 3: Definir medidas de seguridad óptimas para mantener segura la información y fortalecer el esquema de seguridad, confidencialidad, integridad y disponibilidad.

2.9.2. Partes Interesadas

Las partes interesadas que conforman el desarrollo de este Plan de SGSI se presentan en el siguiente orden:

Empresa de Interne AIRMAXTELECOM Soluciones Tecnológicas S.A.: Se ha notado una mejora continua en sus instalaciones, procesos y control, basado en experiencias anteriores compartidas con la empresa, ofreciendo servicios necesarios para el consumidor final. La empresa busca implementar las normas de seguridad de la información y no cuentan con un Sistema de Gestión de Seguridad de la Información (SGSI), controles, políticas de seguridad, que eleva la seguridad y planea actuar para enfrentar amenazas que comprometan la seguridad de activos e información.

Tics: Es el departamento que cuenta con más relación a la seguridad de la información, busca fortalecer el esquema de seguridad de la información en la empresa AIRMAXTELECOM Soluciones Tecnológicas S.A.

Autor del Trabajo: El estudiante cursante a la carrera de Ingeniería en Software de la Universidad Técnica del Norte, se encuentra en desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma de seguridad ISO/IEC 27001-27002 para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.

2.9.3. Requerimientos para el establecimiento de controles del SGSI

La empresa en todas sus áreas está en peligro de ataques en cuanto a la información, por lo que manejan una cantidad considerable de información del personal que conforma la empresa e información de los usuarios que contratan el servicio de la empresa. Para ello es necesario contar con un sistema que proteja la información el cual es considerado un activo critico e invaluable.

Implementar controles con un SGSI conformados por las Normas ISO 27001-27002: 2022, lleva a la empresa a un nivel de protección más alto para la información, manteniendo sus activos

seguros en su gran mayoría centrándose a los que manejar información. El Sistema de Gestión de Seguridad de la Información está basado en el control y valoración de activos, políticas de seguridad de acuerdo con la empresa, supliendo las necesidades que la empresa dispone en la organización.

El proceso para cumplir con el desarrollo de una Propuesta del Sistema de Gestión de Seguridad de la información (SGSI) se plantea gestionar de forma eficaz las amenazas y riesgos manteniendo una mejora continua en sus áreas, Los controles propuestos serás de gran ayuda para la empresa en resguardar la información gestionándola correctamente, tratando de mantener lo más segura posible la información.

2.9.4. Elementos Disponibles

Los elementos que se encuentran presentes para el desarrollo del Sistema de Gestión de Seguridad de la Información, enfocándose en los controles de la ISO/IEC 27002:2022, son los siguientes:

Cooperación de la Organización: La empresa brinda el respaldo al realizar el trabajo de titulación, las entidades que se encuentran en trabajo conjunto son:

- Gerencia
- Carrera de Software
- Responsables en la empresa AIRMAXTELECOM Soluciones Tecnológicas S.A.
- Respaldo Tutor de trabajo de Titulación

Metodología: La metodología que acompañara la mayor parte del proceso, basándose en investigaciones de varios autores, trabajos de grado, expertos en seguridad de la información, es un pilar muy importante para el desarrollo, la metodología a aplicar es muy amigable, fácil de usar, comprende y contiene componentes técnicos para la seguridad de la información, llevando a la persona que emplea esta tecnología, evaluar y gestionar los riesgos de los activos con los que cuenta la empresa:

- Metodología para Gestión de Riesgos (Magerit)

Herramienta: La herramienta idónea para gestionar los posibles riesgos, permitiendo abarcar una cantidad considerable de información de forma fácil y ágil, la cual maneja la metodología Magerit en conjunto con la herramienta.

- La herramienta seleccionada es Pilar, la cual hace que la gestión de riesgos sea más efectiva.

2.9.5. Metodología Magerit para la Gestión de Riesgos

En la etapa de gestión de riesgos, como herramienta precisa se tomó en cuenta Magerit, la cual está enfocada en la evaluación de las necesidades de la empresa AIRMAXTELECOM. Esta metodología se caracteriza por tener la capacidad de estimación de un valor específico de la información, activo o servicio, obteniendo el nivel de seguridad al que debe someterse.

La metodología incluye identificar, analizar y gestionar los riesgos que comprometen la seguridad de la información y los sistemas que la manejan, incluyendo la evaluación de amenazas y vulnerabilidades en los activos más cercanos al manejo de información y mitigar, asumir, transferir y eliminar los riesgos.

Lo que resalta en la metodología Magerit es que tiene un enfoque más centrado en los objetivos, incluye tiene objetivos más específicos que aumentan su grado de confiabilidad en cuanto a los resultados obtenidos en el levantamiento de activos:

- Fortalecer la gestión de información en los sistemas dentro de la organización.
- Determinar procesos óptimos para la identificación de riesgos dentro de la organización.
- Colaborar con la identificación y tratamiento y control de riesgos dentro de la organización.
- Preparar a la empresa para certificaciones en cuanto a seguridad de la información.

2.9.6. Software Pilar

Según (PILAR 2021.1 Manual de Usuario.) Pilar es conocido como un pilar fundamental de la metodología Magerit, es utilizada como objetivo principal hacer más fácil el proceso que se lleva a cabo para el análisis de datos, por consiguiente, tener una óptima gestión en cuanto a la seguridad de la información, tener una mejor visión en la toma de decisiones y tener un esquema adecuado de seguridad en la organización.

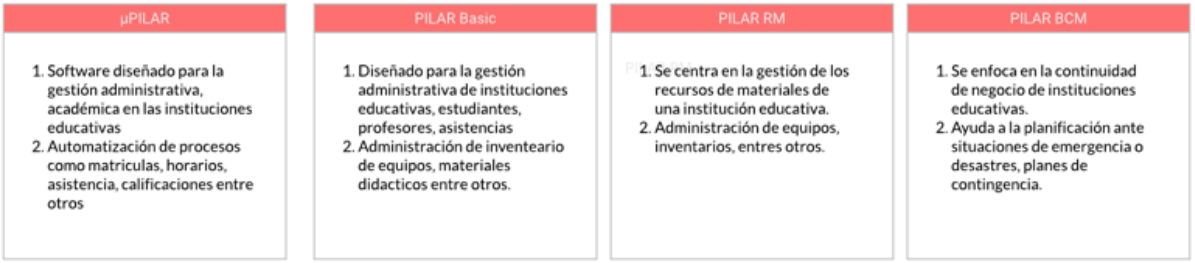
Analizar los riesgos es identificar los riesgos potenciales y residuales en un sistema de información y comunicaciones (CIS). Se denomina riesgo a la incertidumbre sobre lo que puede pasar.

El análisis de riesgos proporciona información para decidir sobre la asignación de recursos, ya sean técnicos o de otro tipo, para proteger organización. El análisis de riesgos requiere un enfoque metódico:

1. Identificar el valor que hay que proteger.
2. Identificar los elementos del sistema que soportan ese valor; es decir, aquellos donde los ataques pueden causar daño, establecer medidas de seguridad para protegernos contra los ataques y estimar indicadores de la posición de riesgo para ayudar a los que tienen que tomar decisiones.

En la Figura 10 se define los diferentes tipos de Software Pilar y características principales:

Figura 10 *Versiones del software Pilar*



Nota. Elaboración propia

2.10. Activos

2.10.1. Identificación de Activos

En el siguiente paso que es la identificación de activos críticos para la seguridad de la información en la empresa, se le da la definición de activo a los recursos que se encuentren en la empresa y que presenta un valor para la funcionalidad y continuidad del negocio, con los cuales se hace posible la disponibilidad del servicio a los usuarios, como metodología se utilizó Magerit en la cual se presenta los tipos de activos que puede haber como se muestra en la siguiente Tabla 14:

Tabla 14 *Clasificación de activos de acuerdo con la Metodología MAGERIT*

Tipos de Activos	Descripción
Datos/Información	Hace referencia a la información que se maneja dentro de la organización, tales como información personal de los empleados o usuarios, políticas, procesos, entre otros.
Servicios	Puede ser el soporte a la empresa, mantenimientos
Software	Herramientas, Bases de Datos, Servidores, entre otros Sistema Contable, Antivirus, Servicios en la Nube.

Hardware	La infraestructura de la organización, los componentes funcionales y de seguridad.
Redes de Comunicación	Permiten la comunicación entre todo el personal que conforma la empresa y sus clientes, tales como teléfonos, celulares, computadoras, servidores, entre otros.
Soportes de Información	Unidades de almacenamiento y procesamiento de información, respaldos, documentos, entre otros
Equipamiento Auxiliar	Apoyo para los equipos y sistemas que controlan la empresa, tales como, cargadores, teclados, adaptadores, entre otros.
Instalaciones	El o los lugares físicos donde operan los sistemas de información como establecimientos gerenciales, oficinas, transporte, entre otros.
Personal	El personal de planta que trabaja en la organización, como gerentes, auxiliares, jefes de departamentos, técnicos, entre otros.

Nota. Elaboración propia

La clasificación de la información de los activos se desarrolla conforma a una codificación la cual la metodología Magerit provee en el software Pilar y también se aplica para cada tipo de activo, en la siguiente Tabla 15 se muestra los activos y su codificación:

Tabla 15 *Identificación de activos y su código*

Tipos de Activos	Descripción	Codificación
Datos/Información	Bases de Datos	D0001
Servicios	Servidores	S0001
Software	Antivirus, Firewall, SO	SW0001
Hardware	Laptops, computadores, impresoras, Switch	HW0001
Redes de Comunicación	Redes de internet, teléfonos	COM0001
Soportes de Información	Electrónicos	MEDIA0001
Equipamiento Auxiliar	Rack, Regletas, Estanterías	AUX0001
Instalaciones	Casa Plus 1, 2, 3	L0001
Personal	Gerencias, personal de planta	P0001

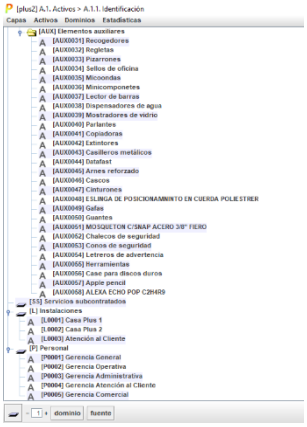
Nota. Elaboración propia

En la Figura 11 se puede visualizar el proceso de identificar los activos en el Software Pilar.

Figura 11 *Levantamiento de activos de la empresa AIRMAXTELECOM A, B, C*

A: Aplicaciones (SW)

B: Auxiliares (AUX)



C: Instalaciones (L) y Personal (P)

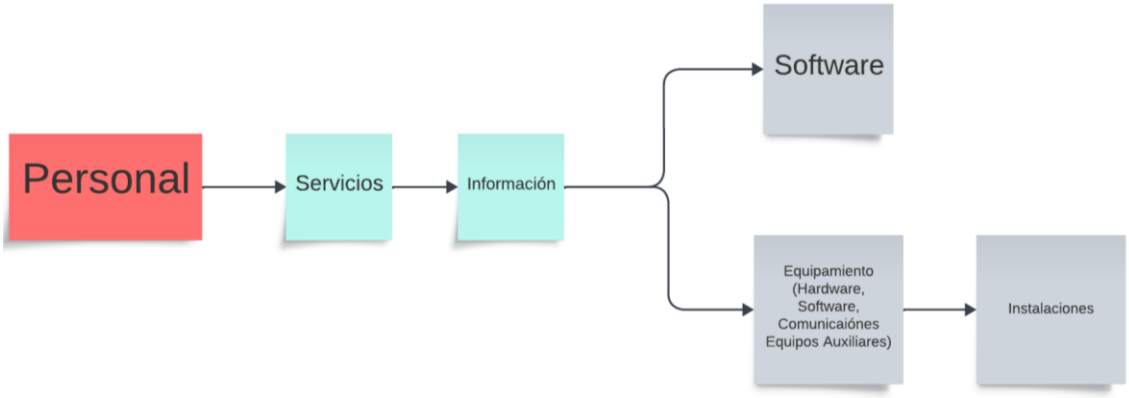
Nota: Elaboración Propia

2.10.2. Dependencia de Activos

Como paso siguiente, tras identificar los activos relacionados con el funcionamiento de la empresa de internet AIRMAXTELECOM Soluciones Tecnológicas S.A., hay que considerar sus relaciones de dependencia. Para poner en un contexto específico, un riesgo considerable en los activos no tan relevantes puede provocar la desestabilización de los activos con más o más importancia en cuanto al funcionamiento y seguridad de la información. El factor humano es de vital reconocimiento, es un activo por el que dependen los activos que funcionan en la empresa para operar, ya que si un activo esencial falla puede afectar de forma pequeña o masiva a la organización.

En la Figura 12 se muestra la categorización de los activos.

Figura 12 *Dependencia entre activos*



Nota. Elaboración propia

2.10.3. Valoración de Activos

La valoración de los activos enfocada en la seguridad de la información se puede realizar en la modalidad cuantitativa, contando con valores numéricos para tener una información o un resultado más acercado a la realidad. El análisis de literatura y documentación pertinente es un pilar fundamental para tener una mejor visión de los activos y cuál es su desempeño en la empresa. La metodología Magerit aporta con una evaluación con base en las dimensiones de los activos, como se muestra en la Tabla 16.

Tabla 16 *Definiciones de las dimensiones de valoración de activos*

Dimensión de Valoración	Definición
Disponibilidad (D)	Los activos y la información se encuentran disponibles siempre que sean necesarios para el desarrollo de actividades y que no comprometan a la empresa.
Integridad (I)	Garantizar que la información sea precisa, sin alteraciones ni modificaciones.
Confidencialidad (C)	La confidencialidad o protección que tengan los activos, la información para personal autorizado.

Nota. Elaboración propia

Para el proceso de valoración de los activos, se ha formulado las siguientes preguntas de acuerdo con la documentación de Magerit para obtener información más real en cuanto a los activos con los que cuenta la empresa.

- **Disponibilidad**

¿Qué importancia tendría el activo si no estuviera disponible?

¿Cuya inaccesibilidad no afecta la actividad normal de la Institución?

¿Cuya inaccesibilidad durante una semana podría ocasionar un perjuicio significativo para la Institución?

¿Cuya inaccesibilidad durante la jornada laboral podría impedir la ejecución de las actividades de la Institución?

¿Cuya inaccesibilidad durante una hora podría impedir la ejecución de las actividades de la Institución?

- **Integridad**

¿Qué importancia tendría que los datos fueran modificados fuera de control?

¿Cuya modificación no autorizada puede repararse fácilmente, o que no afecta a las actividades de la institución?

¿Cuya modificación no autorizada puede repararse, aunque podría ocasionar un perjuicio para la institución o terceros?

¿Cuya modificación no autorizada es de difícil reparación, y podría ocasionar un perjuicio significativo para la institución o terceros?

¿Cuya modificación no autorizada no podría repararse, impidiendo la realización de las actividades?

- **Confidencialidad**

¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?

¿Puede ser conocida y utilizada por cualquier persona, dentro o fuera de la institución?

¿Puede ser conocida y utilizada por cualquier persona, dentro de la institución?

¿Puede ser conocida y utilizada por un grupo de personas que la necesiten para realizar su trabajo?

¿Puede ser conocida y utilizada por un grupo muy reducido por personas, cuya divulgación podría ocasionar perjuicio a la institución o a terceros?

Según Magerit, para evaluar de forma cuantitativa se basa en los criterios que muestra la Tabla 17. En el Anexo 1 se muestra información acerca de los activos y cómo fueron evaluados, los valores son referenciales a la evaluación de impacto para la empresa en el caso hipotético de presentar daños en cierta dimensión.

Tabla 17 *Criterios de Valoración de activos*

Nivel	Valor	Criterio
10	Extremo	Daño catalogado como extremadamente grave.
9	Muy alto	Daño catalogado como muy grave.
6-8	Alto	Daño catalogado como grave.
3-5	Medio	Daño catalogado como importante.
1-2	Bajo	Daño catalogado como menor.
0	Despreciable	Daño catalogado como irrelevante

Nota. Elaboración propia

En la Tabla 18 se encuentran asignadas cada uno de los pilares que se centran en la seguridad (Disponibilidad, Integridad, Confidencialidad) y su respectiva valoración en la empresa de internet AIRMAXTELECOM.

Tabla 18 *Valoración de activos*

Tipo de Activo	Activo	Código	D	I	C	Peso ponderado	Amenaza	Valor
Datos/ Información	Base de Datos	D0001	10	10	10	10	[A.11] Acceso no autorizado	Extremo

	Datos de Acceso	D0002	10	10	10	10		[A.11] Acceso no autorizado	Extremo
	Detectores de Humo	D0003		9	1		7	[A.11] Acceso no autorizado	Alto
	Kit de seguridad	D0004	9	8	2		6	A.22] Manipulación de programas	Alto
	Electricidad	S0001	7	7	7		7	[A.23] Manipulación del hardware	Alto
Servicios	Internet	S0002	8	8	8		8	[A.23] Manipulación del hardware	Alto
	Mantenimiento	S0003	7	7	7		7	[A.11] Acceso no autorizado	Alto
	Correo	S0004	8	8	8		8	[A.11] Acceso no autorizado	Alto
	Sistema Contable	SW0001	9	10	9		9	[I.5.1] Avería de origen lógico	Muy alto
Software	Antivirus	SW0002	10	10	9		9		Muy alto
	Fusionadoras	HW0001	9	5	2		5	[A.23] Manipulación del hardware	Medio
	Cargadores	HW0002	8	5	2		7	[A.23] Manipulación del hardware	Alto
	Power Meter	HW0003	9	5	2		5	[A.23] Manipulación del hardware	Medio
	Sacabocados	HW0004	5	4	1		3	[A.23] Manipulación del hardware	Medio
	Taladros	HW0005	5	4	1		3	[A.23] Manipulación del hardware	Medio
Hardware	Etiquetadoras	HW0006	8	8	2		6	[A.23] Manipulación del hardware	Alto
	Cámaras Web	HW0007	9	8	6		8	[E.25] Pérdida de equipos	Alto
	Portátiles	HW0008	9	8	8		8	[E.25] Pérdida de equipos	Alto
	Cooler AMD	HW0009	8	9	1		6	[E.25] Pérdida de equipos	Alto
	CPUs	HW00010	10	10	1		7	[E.25] Pérdida de equipos	Alto
	Video Card	HW0011	9	9	2		7	[E.25] Pérdida de equipos	Alto
	Impresoras	HW0012	5	5	0		3	[A.11] Acceso no autorizado	Medio

Ipads Apple	HW0013	9	9	7	8	[A.11] Acceso no autorizado	Alto
MacBook Air	HW0014	8	9	8	8	[A.11] Acceso no autorizado	Alto
Monitores	HW0015	8	9	8	8	[E.25] Pérdida de equipos	Alto
Mouse	HW0016	8	9	1	8	[E.25] Pérdida de equipos	Alto
Servidor Dell	HW0017	10	10	9	9	[A.15] Modificación de la información	Muy alto
Tablet Lenovo	HW0018	9	10	7	9	[E.25] Pérdida de equipos	Muy alto
Teclados	HW0019	8	9	1	6	[E.25] Pérdida de equipos	Alto
TVs	HW0020	7	8	5	7	[E.25] Pérdida de equipos	Alto
Amplificadores	HW0021	8	9	3	7	[E.25] Pérdida de equipos	Alto
Aspiradoras	HW0022	9	2	1	4	[E.25] Pérdida de equipos	Medio
Lectores de huellas	HW0023	8	9	7	8	[A.11] Acceso no autorizado	Alto
Biométricos	HW0024	8	9	7	8	[A.11] Acceso no autorizado	Alto
Celulares	HW0025	8	9	5	7	[E.25] Pérdida de equipos	Alto
Micrófonos	HW0026	9	8	5	7	[E.25] Pérdida de equipos	Alto
Televisores	HW0027	7	8	5	6	[E.25] Pérdida de equipos	Alto
Alcancel	HW0028	8	9	1	6	[E.25] Pérdida de equipos	Alto
Estanterías	HW0029	9	8	8	8	[E.25] Pérdida de equipos	Alto
Rótulos	HW0030	9	8	2	6	[E.25] Pérdida de equipos	Alto
Rack	HW0031	9	9	7	8	[A.11] Acceso no autorizado	Alto
Implementos instalación internet	HW0032	9	8	5	7	[A.15] Modificación de la información	Alto
OLT Gpon	HW0033	8	9	7	8	[E.25] Pérdida de equipos	Alto
Unidades de almacenamiento	HW0034	9	9	8	9	[A.25] Robo de equipos	Muy alto

	Ofimática	HW0035	10	9	8	6	[E.25] Pérdida de equipos	Alto
Comunicaciones	Teléfonos IP 2 cuentas	COM00001	8	8	2	5	[E.25] Pérdida de equipos	Alto
	Escaleras	AUX0001	8	7	1	8	[A.11] Acceso no autorizado	Alto
	Generadores	AUX0002	9	9	7	6	[A.11] Acceso no autorizado	Alto
	Sillas	AUX0003	8	8	1	6	[E.25] Pérdida de equipos	Alto
	Balanza	AUX0004	8	9	2	7	[E.25] Pérdida de equipos	Alto
	Camilla	AUX0005	8	9	3	7	[E.25] Pérdida de equipos	Alto
	Linternas	AUX0006	9	8	1	6	[E.25] Pérdida de equipos	Alto
	Grapadoras	AUX0007	5	4	1	3	[E.25] Pérdida de equipos	Medio
	Perforadoras	AUX0008	5	4	1	3	[E.25] Pérdida de equipos	Medio
	Recogedores	AUX0009	9	2	1	4	[E.25] Pérdida de equipos	Medio
	Regletas	AUX0010	5	2	1	3	[E.25] Pérdida de equipos	Medio
	Pizarrones	AUX0011	5	5	1	4	[E.25] Pérdida de equipos	Medio
Auxiliares	Sellos de oficina	AUX0012	9	8	3	7	[E.25] Pérdida de equipos	Alto
	Microondas	AUX0013	8	0	0	3	[E.25] Pérdida de equipos	Medio
	Minicomponentes	AUX0014	7	5	1	4	[A.11] Acceso no autorizado	Medio
	Lector de barras	AUX0015	9	9	4	7	[A.11] Acceso no autorizado	Alto
	Dispensador de agua	AUX0016	5	4	1	3	[E.25] Pérdida de equipos	Medio
	Mostradores de vidrio	AUX0017	8	9	3	7	[E.25] Pérdida de equipos	Alto
	Parlantes	AUX0018	9	8	2	6	[E.25] Pérdida de equipos	Alto
	Copiadoras	AUX0019	9	8	6	8	[E.25] Pérdida de equipos	Alto
	Extintores	AUX0020	10	10	1	7	[A.11] Acceso no autorizado	Alto
	Casilleros metálicos	AUX0021	8	9	7	8	[A.11] Acceso no autorizado	Alto
	Data Fast	AUX0022	7	8	6	7	[A.11] Acceso no autorizado	Alto

	Arnés reforzado	AUX0023	9	9	1	6	[E.25] Pérdida de equipos	Alto
	Cascos	AUX0024	8	7	3	6	[E.25] Pérdida de equipos	Alto
	Cinturones	AUX0025	8	7	3	6	[E.25] Pérdida de equipos	Alto
	Eslinga de posicionamiento	AUX0026	8	7	2	6	[E.25] Pérdida de equipos	Alto
	Gafas	AUX0027	8	7	1	5	[E.25] Pérdida de equipos	Medio
	Guantes	AUX0028	8	7	1	3	[E.25] Pérdida de equipos	Medio
	Mosqueton	AUX0029	5	5	1	3	[E.25] Pérdida de equipos	Medio
	Chalecos	AUX0030	7	7	1	5	[E.25] Pérdida de equipos	Medio
	Conos de seguridad	AUX0031	5	5	1	7	[E.25] Pérdida de equipos	Alto
	Letreros de advertencia	AUX0032	9	9	2	7	[A.11] Acceso no autorizado	Alto
	Herramientas	AUX0033	10	9	1	7	[A.11] Acceso no autorizado	Alto
	Case para discos duros	AUX0034	9	9	4	7	[A.11] Acceso no autorizado	Alto
	Apple pencil	AUX0035	8	9	3	7	[A.25] Robo de equipos	Alto
	Alexa	AUX0036	8	9	3	7	[A.11] Acceso no autorizado	Alto
	Casa Plus 1	L0001	10	10	1	7	[A.30] Ingeniería social (picaresca	Alto
Instalaciones	Casa Plus 2	L0002	10	10	1	7	[A.30] Ingeniería social (picaresca	Alto
	Atención al Cliente	L0003	10	10	1	7	[A.30] Ingeniería social (picaresca	Alto
	Gerencia Operacional	P0001	5	5	5	5	[A.30] Ingeniería social (picaresca	Medio
	Gerencia Operativa	P0002	10	10	10	10	[A.30] Ingeniería social (picaresca	Extremo
Personal	Gerencia Administrativa	P0003	5	5	5	4	[A.30] Ingeniería social (picaresca	Medio
	Gerencia Atención al Cliente	P0004	4	4	4	4	[A.30] Ingeniería social (picaresca	Medio

Gerencia Comercial	P0005	5	5	5		5	[A.30] Ingeniería social (picaresca	Medio

Nota. Elaboración propia

2.10.4. Identificación de Amenazas

Después del análisis y valoración de activos, es necesario proceder con la identificación de las amenazas que pueden comprometer a los activos de la empresa. Es una parte fundamental en la cual se puede realizar la gestión de riesgos. Magerit nos proporciona en uno de sus dos libros en específico el libro número II, que trata sobre los catálogos de elementos y desglosa los tipos de amenazas existentes:

- Desastres Naturales (N)
- Origen Industrial (I)
- Errores y fallos no identificados (E)
- Ataques Intencionales (A)

En la Tabla 19 se menciona a detalle cada una de las amenazas a las cuales está propenso cada activo, se realizó el análisis y detección de amenazas en 94 activos de la empresa AIRMAXTELECOM Soluciones Tecnológicas S.A. las amenazas restantes se encuentran en el Anexo 2.

Tabla 19 *Identificación de amenazas por activos*

Activo	**Amenazas**
	Datos/Información
Base de Datos de los Sistemas Informáticos	[1.5.11 Avería de origen lógico
Base de Datos de los Sistemas Informáticos	[E.8] Difusión de software dañino
Base de Datos de los Sistemas Informáticos	[E.15] Alteración de la información
Base de Datos de los Sistemas Informáticos	[E,20] Vulnerabilidades de los programas (software)
Base de Datos de los Sistemas Informáticos	[E.21] Errores de mantenimiento I actualización de programas (software)
Base de Datos de los Sistemas Informáticos	[A.8] Difusión de software dañino
Base de Datos de los Sistemas Informáticos	[A.22] Manipulación de programas
Datos de acceso a servidores y sistemas	[1.5.11 Avería de origen lógico
Datos de acceso a servidores y sistemas	[E.81 Difusión de software dañino
Datos de acceso a servidores y sistemas	[E.20] Vulnerabilidades de los programas (software)

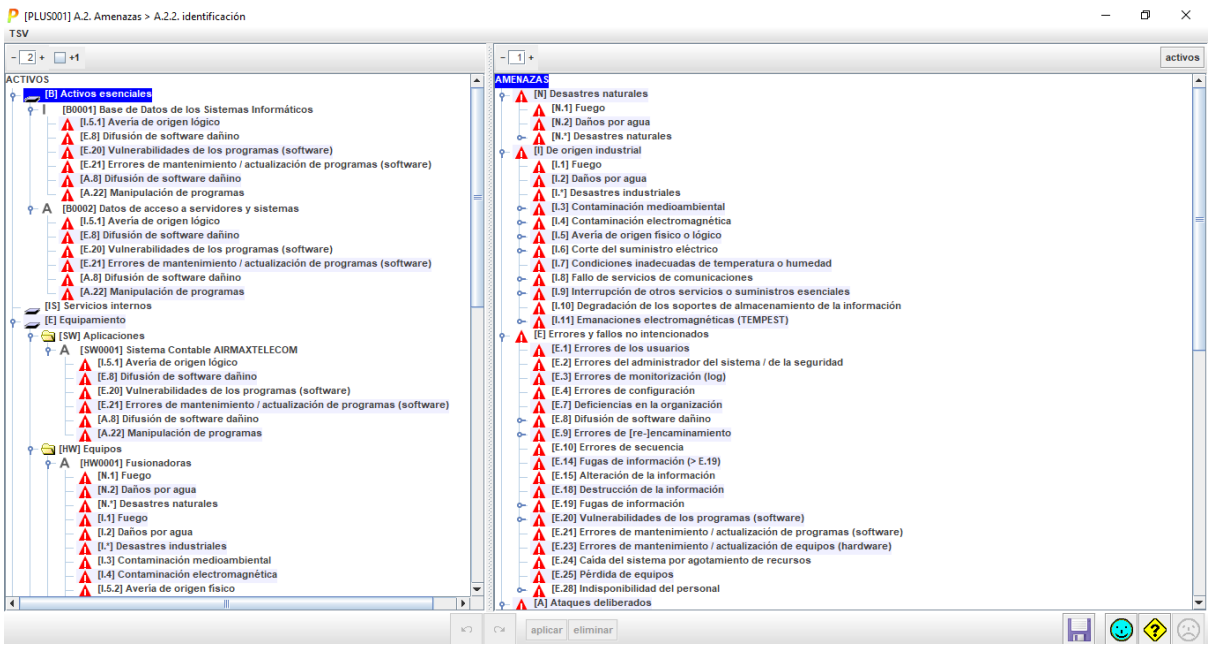
Datos de acceso a servidores y sistemas	[E.21] Errores de mantenimiento / actualización de programas (software)
Datos de acceso a servidores y sistemas	[A.8] Difusión de software dañino
Datos de acceso a servidores y sistemas	[A.221] Manipulación de programas
	Servicios
Electricidad	[E.2] Errores del administrador del sistema / de la seguridad
Electricidad	[E.15] Alteración de la información
Electricidad	[E.19] Fugas de información
Electricidad	[A.5] Suplantación de la identidad
Electricidad	[A.6] Abuso de privilegios de acceso
Electricidad	[A.7] Uso no previsto
Electricidad	[A.11] Acceso no autorizado
Electricidad	[A.15] Modificación de la información
Internet	[E.1] Errores de los usuarios
Internet	[E.2] Errores del administrador del sistema / de la seguridad
Internet	[E.15] Alteración de la información
Internet	[E.19] Fugas de información
Internet	[A.5] Suplantación de la identidad
Internet	[A.6] Abuso de privilegios de acceso
Internet	[A.7] Uso no previsto
Internet	[A.11] Acceso no autorizado
Internet	[A.15] Modificación de la información
Mantenimiento	[E.1] Errores de los usuarios
Mantenimiento	[E.2] Errores del administrador del sistema / de la seguridad
Mantenimiento	[E.15] Alteración de la información
Mantenimiento	[E.19] Fugas de información
Mantenimiento	[A.5] Suplantación de la identidad
Mantenimiento	[A.6] Abuso de privilegios de acceso
Mantenimiento	[A.7] Uso no previsto
Mantenimiento	[A.11] Acceso no autorizado
Mantenimiento	[A.15] Modificación de la información
Correo	[E.1] Errores de los usuarios

Correo	[E.2] Errores del administrador del sistema / de la seguridad
Correo	[E.15] Alteración de la información
Correo	[E.19] Fugas de información
Correo	[A.5] Suplantación de la identidad
Correo	[A.6] Abuso de privilegios de acceso
Correo	[A.7] Uso no previsto
Correo	[A.11] Acceso no autorizado
Correo	[A.15] Modificación de la información

Nota. Elaboración propia

La herramienta Pilar tiene la capacidad de identificar una a una las amenazas de forma automática para los activos, como se muestra en la Figura13.

Figura 13 *Identificación de amenazas por activos*



Nota: Elaboración Propia.

2.10.5. Valoración de Amenazas

Como paso importante, después de identificar las amenazas de los activos, continua la valoración de amenazas con dos elementos importantes, los cuales son:

Impacto o Degradación: Analiza los efectos que podría tener el activo si se materializa una amenaza relacionada. Esta evaluación se basa en la escala de la Tabla 20. Sin embargo, representar los valores de la herramienta Pilar es esencial para representar valores numéricos, con un intervalo de 0 a 100 en formato porcentual.

Tabla 20 *Escala Degradación del valor de un activo*

MA	100%	Muy Alta	Casi Seguro	Fácil
A	75%	Alta	Muy Alto	Medio
M	50%	Medio	Posible	Difícil
B	25%	Baja	Poco Probable	Muy Difícil
MB	0%	Muy Baja	Muy Raro	Extremadamente Difícil

Nota. Elaboración propia

Frecuencia o Probabilidad: Es la escala en la cual se mide la materialización de una amenaza, la misma que se calcula de forma anual como se muestra en la Tabla 21.

Tabla 21 *Valores de probabilidad de ocurrencia de una amenaza*

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

Nota. Elaboración propia

Para continuar con el proceso de valoración de amenazas se toma en cuenta los activos que facilito la empresa para ser valorados y se detalla en la siguiente Tabla 22 mostrando los aspectos de Frecuencia, Disponibilidad, Confidencialidad, Integridad, las amenazas restantes se encuentran en el Anexo 3.

Tabla 22 *Valoración de amenazas por activos*

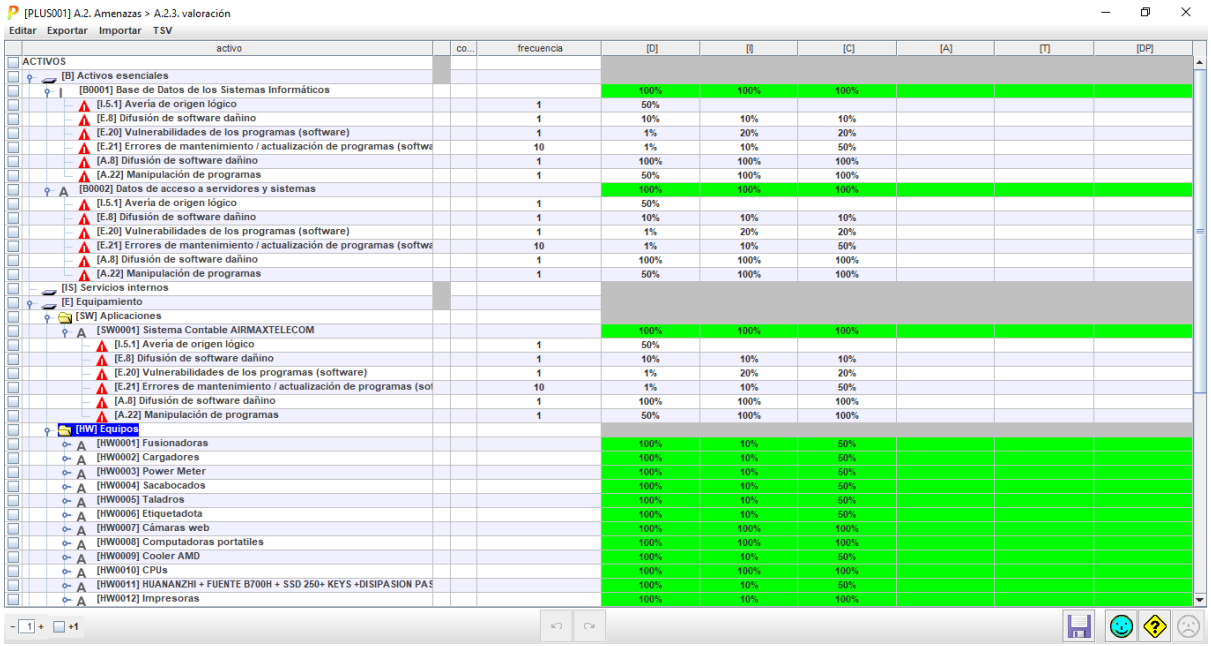
Activo	Amenazas		D	I	C
	Datos/Información				
Base de Datos	[1.5.11 Avería de origen lógico	50%			
Base de Datos	[E.8] Difusión de software dañino	10%	10%	10%	
Base de Datos	[E.15] Alteración de la información	1%	20%	20%	
Base de Datos	[E,20] Vulnerabilidades de los programas (software)				
Base de Datos	[E.21] Errores de mantenimiento / actualización (software)	1%	10%	50%	
Base de Datos	[A.8] Difusión de software dañino	100%	100%	100%	
Base de Datos	[A.22] Manipulación de programas	50%	100%	100%	
Base de Datos	[1.5.11 Avería de origen lógico	50%			
Base de Datos	[E.8] Difusión de software dañino	10%	10%	10%	
Base de Datos	[E.20] Vulnerabilidades de los programas (software)	1%	20%	20%	
Base de Datos	[E.21] Errores de mantenimiento / actualización (software)	1%	10%	50%	
Base de Datos	[A.8] Difusión de software dañino	100%	100%	100%	
Base de Datos	[A.221] Manipulación de programas	0%	5 00%	1 00%	1 00%
	Servicios				
Electricidad	[E.2] Errores del administrador del sistema / de la seguridad	0%	1 0%	1 0%	2 0%
Electricidad	[E.15] Alteración de la información			1 0%	1 0%
Electricidad	[E.19] Fugas de información		10%	10%	
Electricidad	[A.5] Suplantación de la identidad	50%	50%	50%	
Electricidad	[A.6] Abuso de privilegios de acceso	10%	10%	10%	

Electricidad	[A.7] Uso no previsto	10%	10%	10%
Electricidad	[A.11] Acceso no autorizado	10%	50%	10%
Electricidad	[A.15] Modificación de la información	50%		50%
Internet	[E.1] Errores de los usuarios		10%	10%
Internet	[E.2] Errores del administrador del sistema / de la seguridad	10%	20%	20%
Internet	[E.15] Alteración de la información		1%	10%
Internet	[E.19] Fugas de información	10%	10%	10%
Internet	[A.5] Suplantación de la identidad	10%	50%	50%
Internet	[A.6] Abuso de privilegios de acceso		10%	10%
Internet	[A.7] Uso no previsto	10%	10%	10%
Internet	[A.11] Acceso no autorizado	10%	50%	10%
Internet	[A.15] Modificación de la información	50%		50%
Mantenimiento	[E.1] Errores de los usuarios		10%	10%
Mantenimiento	[E.2] Errores del administrador del sistema / de la seguridad	10%	20%	20%
Mantenimiento	[E.15] Alteración de la información		1%	10%
Mantenimiento	[E.19] Fugas de información	10%	10%	10%
Mantenimiento	[A.5] Suplantación de la identidad	10%	50%	50%
Mantenimiento	[A.6] Abuso de privilegios de acceso		10%	10%
Mantenimiento	[A.7] Uso no previsto	10%	10%	10%
Mantenimiento	[A.11] Acceso no autorizado	10%	50%	10%
Mantenimiento	[A.15] Modificación de la información	50%		50%
Correo	[E.1] Errores de los usuarios		10%	10%
Correo	[E.2] Errores del administrador del sistema / de la seguridad	10%	20%	20%
Correo	[E.15] Alteración de la información		1%	10%
Correo	[E.19] Fugas de información	10%	10%	10%
Correo	[A.5] Suplantación de la identidad	10%	50%	50%
Correo	[A.6] Abuso de privilegios de acceso		10%	10%
Correo	[A.7] Uso no previsto	10%	10%	10%
Correo	[A.11] Acceso no autorizado	10%	50%	10%
Correo	[A.15] Modificación de la información	50%		50%

Nota. Elaboración propia

En la Figura 14 se puede visualizar las amenazas que se pueden presentar en base a la herramienta utilizada Pilar valorando la probabilidad en a que pueda suceder con estos activos.

Figura 14 *Valoración de amenazas por activos*



Nota: Elaboración Propia.

2.10.6. Evaluación de Riesgos

Tras finalizar las tareas en cuanto a su orden se impone levantar activos, evaluar sus amenazas en la empresa AIRMAXTELECOM Soluciones Tecnológicas S.A. Para calcular los riesgos, continuando los pasos presentados.

Impacto Potencial: Es la referencia a la estimación de los daños que puede darse como resultado de verse comprometidos los activos, Teniendo conocimiento de los activos en sus indicadores como (Disponibilidad, Integridad, Confidencialidad) y estando en contexto del grado de afección, se procede a calcular el impacto de los activos.

Criterios de Valoración

- **Muy Alto (10):** Si la amenaza llega a materializarse en los activos, obteniendo como consecuencia una perdida considerable para la empresa.
- **Alto (9):** Si la amenaza llega a materializarse, teniendo como resultado consecuencias considerables para la empresa.

- **Medio (6 - 8):** Si la amenaza llega a materializarse, teniendo como resultado consecuencias no tan grabes para la empresa.
- **Bajo (3 – 5):** Si la amenaza llega a materializarse, teniendo como resultado consecuencias bajas para la empresa.
- **Muy Bajo (1 - 2):** Si la amenaza llega a materializarse, teniendo como resultado consecuencias mínimas para la empresa.
- **Despreciable (0):** Si la amenaza llega a materializarse, no tendría efectos negativos para la empresa.

El proceso de evaluación de impacto tiene dos procesos por los que se puede tomar el camino óptimo.

Impacto Potencial Acumulado: Toma en cuenta el valor global de cada activo, acumulando sus valores en cuanto a las variables ya mencionadas, la evaluación de amenazas a las que está propenso.

Habiendo calculado el impacto de los activos con sus amenazas, se obtuvieron los siguientes resultados mostrados en la siguiente Tabla 23. El resultado de los restantes activos se encuentra en el Anexo 4.

Tabla 23 *Impacto potencial acumulado de afectación de activos*

Activo	Amenazas			Peso Ponderado
	Datos/Información			
Base de Datos	[1.5.11 Avería de origen lógico			9
Base de Datos	[E.8] Difusión de software dañino	0	0	9
Base de Datos	[E.15] Alteración de la información			4
Base de Datos	[E,20] Vulnerabilidades de los programas (software)			6
Base de Datos	[E.21] Errores de mantenimiento / actualización (software)			6
Base de Datos	[A.8] Difusión de software dañino	0	0	9
Base de Datos	[A.22] Manipulación de programas	0	0	9

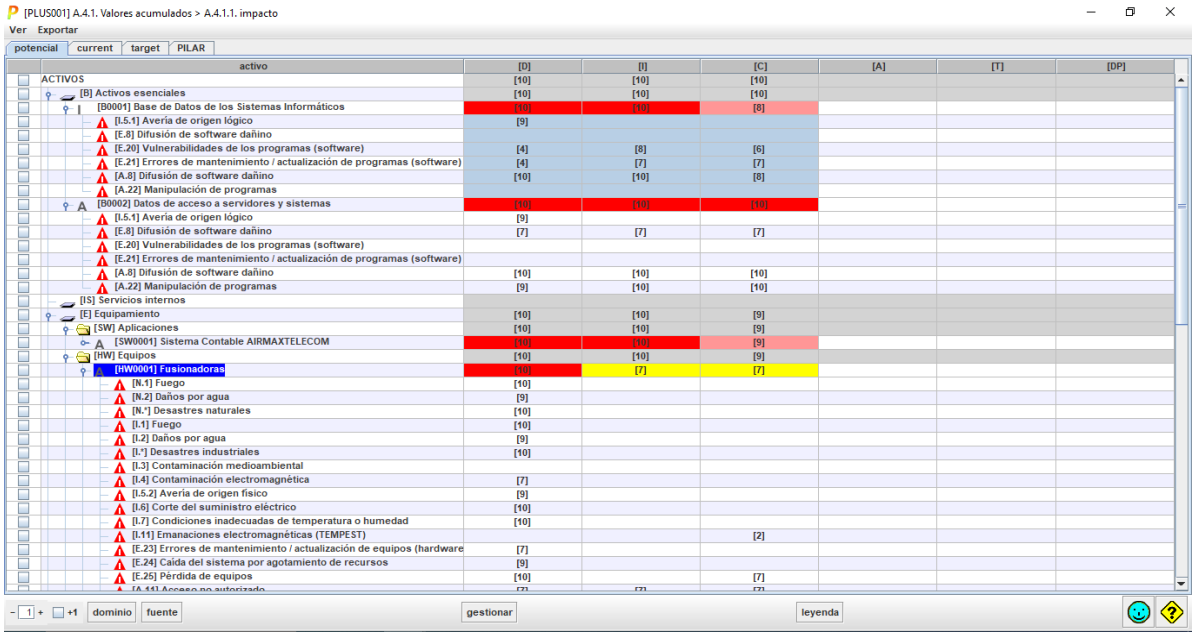
Base de Datos	[1.5.11 Avería de origen lógico			9
Base de Datos	[E.8] Difusión de software dañino	0	0	9
Base de Datos	[E.20] Vulnerabilidades de los programas (software)			4
Base de Datos	[E.21] Errores de mantenimiento / actualización (software)			6
Base de Datos	[A.8] Difusión de software dañino			6
Base de Datos	[A.221] Manipulación de programas	0	0	9
	Servicios			
Electricidad	[E.2] Errores del administrador del sistema / de la seguridad			6
Electricidad	[E.15] Alteración de la información			6
Electricidad	[E.19] Fugas de información			7
Electricidad	[A.5] Suplantación de la identidad			7
Electricidad	[A.6] Abuso de privilegios de acceso			6
Electricidad	[A.7] Uso no previsto			6
Electricidad	[A.11] Acceso no autorizado			7
Electricidad	[A.15] Modificación de la información			7
Internet	[E.1] Errores de los usuarios			6
Internet	[E.2] Errores del administrador del sistema / de la seguridad			6
Internet	[E.15] Alteración de la información			6
Internet	[E.19] Fugas de información			7
Internet	[A.5] Suplantación de la identidad			7
Internet	[A.6] Abuso de privilegios de acceso			6
Internet	[A.7] Uso no previsto			6
Internet	[A.11] Acceso no autorizado			7
Internet	[A.15] Modificación de la información			7
Mantenimiento	[E.1] Errores de los usuarios			6
Mantenimiento	[E.2] Errores del administrador del sistema / de la seguridad			6
Mantenimiento	[E.15] Alteración de la información			6
Mantenimiento	[E.19] Fugas de información			7

Mantenimiento	[A.5] Suplantación de la identidad	7
Mantenimiento	[A.6] Abuso de privilegios de acceso	6
Mantenimiento	[A.7] Uso no previsto	6
Mantenimiento	[A.11] Acceso no autorizado	7
Mantenimiento	[A.15] Modificación de la información	7
Correo	[E.1] Errores de los usuarios	6
Correo	[E.2] Errores del administrador del sistema / de la seguridad	6
Correo	[E.15] Alteración de la información	6
Correo	[E.19] Fugas de información	7
Correo	[A.5] Suplantación de la identidad	7
Correo	[A.6] Abuso de privilegios de acceso	6
Correo	[A.7] Uso no previsto	6
Correo	[A.11] Acceso no autorizado	7
Correo	[A.15] Modificación de la información	7

Nota. Elaboración propia

En la Figura 15 se puede apreciar el impacto que puede llegar a tener al estar comprometidos los activos en el software Pilar.

Figura 15 *Impacto potencia acumulada de afectación de activos*



Nota: Elaboración Propia.

Impacto Potencial Repercutido: En este tipo de impacto se toma en cuenta dos factores importantes, los cuales son el impacto directo activo, y las amenazas a las cuales estaría propenso los activos y los que dependen también.

En la Tabla 24 se puede visualizar el cálculo del impacto que puede tener los activos en el caso de que se encuentren comprometidos.

Tabla 24 *Impacto potencial repercutido de afectación de activos*

Activos	D	I	C	Peso Ponderado
Base de Datos	10	10	8	9
Datos de acceso	10	10	10	10
Detectores de Humo	10	9	1	7
Kit de Seguridad	9	8	2	6
Sistema Contable	10	10	9	10
Fusionadoras	10	7	7	8
Cargadores	10	7	7	8
Power Meter	10	7	7	8
Sacabocados	10	7	7	8
Taladros	10	7	7	8
Etiquetadoras	10	7	7	8
Cámaras Web	10	10	8	9
Computadoras Portátiles	10	10	8	9
Cooler AMD	10	7	7	8
CPU	10	10	9	10
Video Card	10	7	7	8
Impresoras	10	7	8	8
IPad Apple	10	10	8	9
MacBook Air	10	10	8	9
Monitores	10	10	8	9
Mouse	10	7	7	8
Server Dell	10	10	8	9
Tablet Lenovo	10	10	8	9
Teclados	10	7	7	8
TV	10	7	7	8

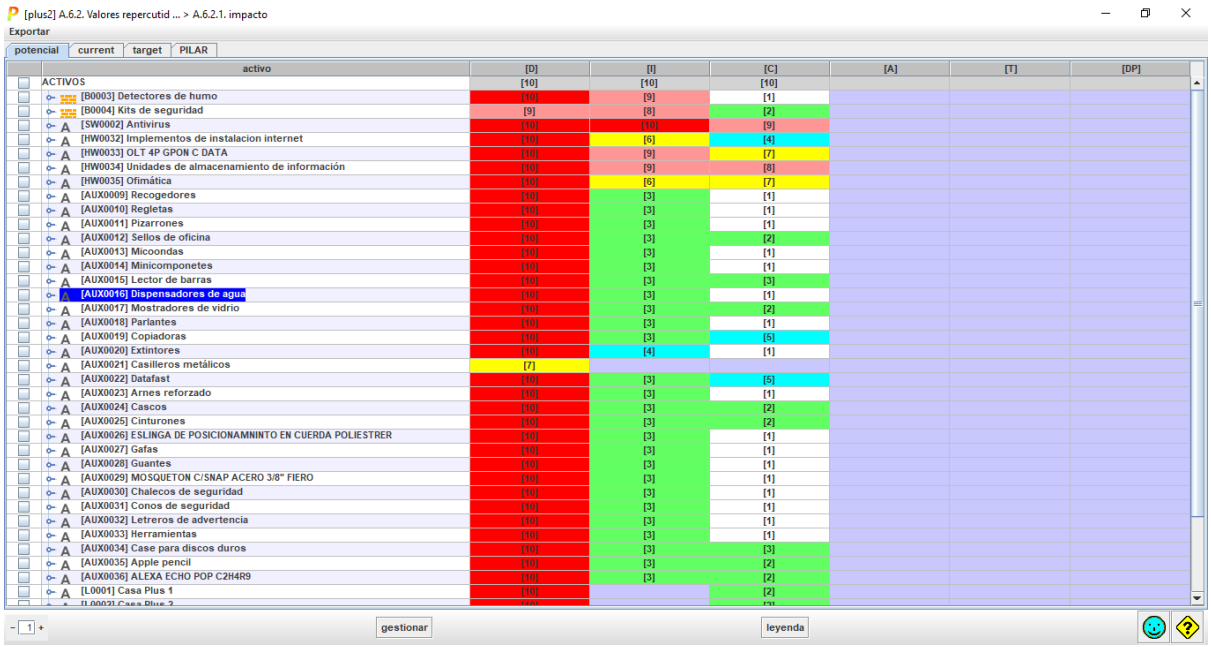
Amplificadores	10	7	7	8
Aspiradoras	10	7	7	8
Lectores de Huellas	10	10	8	9
Biométricos	10	7	7	8
Celulares	10	10	8	9
Micrófonos	10	7	7	8
Televisores	10	7	7	8
Alcancel	10	7	7	8
Estanterías	10	10	8	9
Rótulos	10	7	7	8
Rack	9	6	6	7
Instalación internet	10	6	4	7
OLT GPON	10	9	7	9
Unidades de Almacenamiento	10	9	8	9
Ofimática	10	6	7	8
Teléfonos IP 2 cuentas	9	8	7	8
Escaleras	10	4	7	7
Generadores	10			10
Sillas	10	4	7	7
Balanzas	10	4	7	7
Camilla	10	4	7	7
Linternas	9	2	0	4
Grapadoras	5	0	0	2
Perforadoras	5	0	0	2
Recogedores	10	3	1	5
Regletas	10	3	1	5
Pizarrones	10	3	1	5
Sellos de Oficina	10	3	2	5
Microondas	10	3	1	5
Minicomponente	10	3	1	5
Lectores de Barras	10	3	3	5
Dispensador de agua	10	3	1	5
Mostrador de vidrio	10	3	2	5
Parlantes	10	3	1	5
Copiadoras	10	3	5	6

Extintores	10	4	1	5
Casilleros metálicos	7			7
Data Fast	10	3	5	6
Arnés Reforzado	10	3	1	5
Cascos	10	3	2	5
Cinturones	10	3	2	5
Eslinga	10	3	1	5
Gafas	10	3	1	5
Guantes	10	3	1	5
Mosquetón	10	3	1	5
Chalecos	10	3	1	5
Conos de Seguridad	10	3	1	5
Letreros de Advertencia	10	3	1	5
Herramientas	10	3	1	5
Case para Discos Duros	10	3	3	5
Apple Pencil	10	3	2	5
Alexa	10	3	2	5
Casa Plus 1	10		2	6
Casa Plus 2	10		2	6
Atención al cliente				
Gerencia Operativa	9	8	4	7
Gerencia General	9	10	10	10
Gerencia Administrativa	9	8	4	7
Gerencia Atención al Cliente	9	8	2	6
Gerencia Comercial	9	8	3	7

Nota. Elaboración propia

En la Figura 13 se muestra el impacto que puede tener cada activo de la empresa AIRMAXTELECOM Soluciones Tecnológicas S.A. en base al software Pilar.

Figura 16 *Impacto potencial repercutido de afectación de activos*

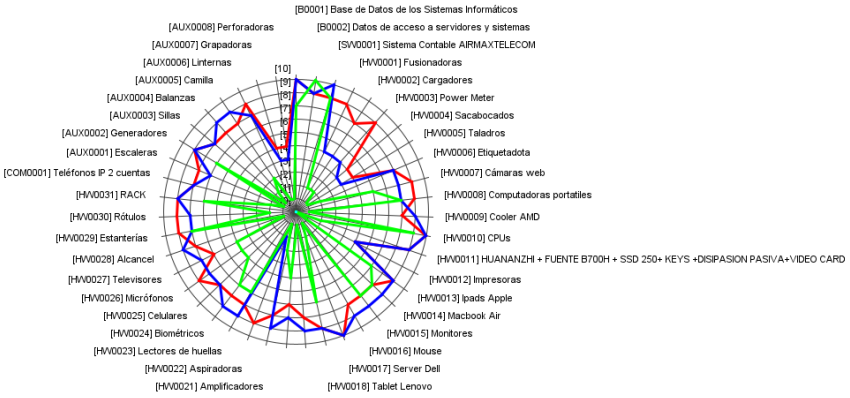


activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS	[10]	[10]	[10]			
[B0003] Detectores de humo	[10]	[9]	[1]			
[B0004] Kits de seguridad	[9]	[8]	[2]			
[SW0002] Antivirus	[10]	[10]	[9]			
[HW0032] Implementos de instalacion internet	[10]	[6]	[4]			
[HW0033] OLT 4P GPON C DATA	[10]	[9]	[7]			
[HW0034] Unidades de almacenamiento de información	[10]	[9]	[8]			
[HW0035] Ofimática	[10]	[6]	[7]			
[AUX0009] Recogedores	[10]	[3]	[1]			
[AUX0010] Regletas	[10]	[3]	[1]			
[AUX0011] Pizarrones	[10]	[3]	[1]			
[AUX0012] Sellos de oficina	[10]	[3]	[2]			
[AUX0013] Micoondas	[10]	[3]	[1]			
[AUX0014] Minicomponetes	[10]	[3]	[1]			
[AUX0015] Lector de barras	[10]	[3]	[3]			
[AUX0016] Dispensadores de agua	[10]	[3]	[1]			
[AUX0017] Mostradores de vidrio	[10]	[3]	[2]			
[AUX0018] Parlantes	[10]	[3]	[1]			
[AUX0019] Copiadoras	[10]	[3]	[5]			
[AUX0020] Extintores	[10]	[4]	[1]			
[AUX0021] Casilleros metálicos	[7]					
[AUX0022] Datafast	[10]	[3]	[5]			
[AUX0023] Arnes reforzado	[10]	[3]	[1]			
[AUX0024] Cascos	[10]	[3]	[2]			
[AUX0025] Cinturones	[10]	[3]	[2]			
[AUX0026] ESLINGA DE POSICIONAMNINTO EN CUERDA POLIESTRER	[10]	[3]	[1]			
[AUX0027] Gafas	[10]	[3]	[1]			
[AUX0028] Guantes	[10]	[3]	[1]			
[AUX0029] MOSQUETON C/SNAP ACERO 3/8" FIERO	[10]	[3]	[1]			
[AUX0030] Chalecos de seguridad	[10]	[3]	[1]			
[AUX0031] Conos de seguridad	[10]	[3]	[1]			
[AUX0032] Letreros de advertencia	[10]	[3]	[1]			
[AUX0033] Herramientas	[10]	[3]	[1]			
[AUX0034] Case para discos duros	[10]	[3]	[3]			
[AUX0035] Apple pencil	[10]	[3]	[2]			
[AUX0036] ALEXA ECHO POP C2H4R9	[10]	[3]	[2]			
[L0001] Casa Plus 1	[10]		[2]			

Nota. Elaboración propia

En la Figura 17 se puede apreciar el impacto acumulado de cada uno de los activos levantados en la empresa, los valores se delimitan por la línea roja, los valores que se marcan con el color azul son los calores recomendados por el software Pilar.

Figura 17 *Gráfico de valores de impacto potencial acumulado de los activos*



Nota. Elaboración propia

Como se ha demostrado en el proceso del desarrollo del SGSI es importante considerar el evaluar el impacto que pueden tener las amenazas en cuestión de los activos de la empresa y lograr

gestionar de mejor forma. Con este análisis más centrado en la realidad conlleva a tener un análisis adecuado para plantearse controles necesarios en base a las posibles consecuencias que pueden tener los activos en caso de materializarse en la empresa.

2.10.7. Determinación de Riesgos Potenciales

Continuando con el análisis y evaluación de riesgos conforme al impacto potencial, se determinó a los posibles riesgos evaluando que sea el caso hipotético de que suceda. La Tabla 25 muestra una relación proporcional directa entre la magnitud del riesgo y tanto el impacto como la probabilidad asociada

.

Tabla 25 *Nivel de riesgo*

		PROBABILIDAD		
		Bajo	**Medio**	**Alto**
IMPACTO	**Alto**	**3**	**6**	**9**
	Medio	**2**	**4**	**6**
	Bajo	**1**	**2**	**3**

Nota. Elaboración propia

Basándonos en la tabla y en la información mencionada con anterioridad, se desarrolló el análisis y el cálculo de los activos que existen en la empresa, evaluando las amenazas que el software Pilar nos ofrece en todas sus dimensiones.

Riesgo Potencial Acumulado: Se realiza el análisis del impacto que puede tener una amenaza en los activos, paralelamente se calcula la probabilidad de amenaza que puede tener los activos:

Riesgo Potencial Acumulado = Probabilidad de Amenaza x Valor Acumulado del Impacto

La continuación del análisis se puede encontrar en el Anexo 5 donde se muestra las amenazas en cada uno de los activos restantes, en la siguiente Tabla 26 se puede mostrar como es el proceso de valoración con base en variables de evaluación poniéndose en contexto de los riesgos potenciales acumulados.

Tabla 26 *Riesgo potencial acumulado de afectación de activos*

Activo	Amenazas	D R	I P	C A	Peso Ponderado
	Datos/Información	8,0	7,4	6,8	7,4
Base de Datos	[1.5.11 Avería de origen lógico	8,0	7,4		7,7
Base de Datos	[E.8] Difusión de software dañino	5,1	5,1	3,9	4,7
Base de Datos	[E.15] Alteración de la información	3,3	5,1	5,1	4,5
Base de Datos	[E,20] Vulnerabilidades de los programas (software)	8,0	5,6	4,4	6,0
Base de Datos	[E.21] Errores de mantenimiento / actualización (software)	8,0	8,0		8,0
Base de Datos	[A.8] Difusión de software dañino	6,8	6,8	5,7	6,4
Base de Datos	[A.22] Manipulación de programas	6,3	6,8	5,7	6,3
Base de Datos	[1.5.11 Avería de origen lógico	8,0			8,0
Base de Datos	[E.8] Difusión de software dañino	5,1	5,1	3,9	4,7
Base de Datos	[E.20] Vulnerabilidades de los programas (software)	8,0	5,6	4,4	6,0
Base de Datos	[E.21] Errores de mantenimiento / actualización (software)	8,0	8,0		8,0
Base de Datos	[A.8] Difusión de software dañino	6,8	6,8	5,7	6,4

Base de Datos	[A.221] Manipulación de programas	6,3	6,8	5,7	6,3
	Servicios		6,0	6,3	6,2
Electricidad	[E.2] Errores del administrador del sistema / de la seguridad	4,5	4,4	5,6	4,8
Electricidad	[E.15] Alteración de la información		2,1		2,1
Electricidad	[E.19] Fugas de información			5,1	5,1
Electricidad	[A.5] Suplantación de la identidad		5,1	6,3	5,7
Electricidad	[A.6] Abuso de privilegios de acceso		3,9	5,1	4,5
Electricidad	[A.7] Uso no previsto		3,9	5,1	4,5
Electricidad	[A.11] Acceso no autorizado		3,9	6,3	5,1
Electricidad	[A.15] Modificación de la información		6,0		6,0
Internet	[E.1] Errores de los usuarios	4,5	3,9	5,1	4,5
Internet	[E.2] Errores del administrador del sistema / de la seguridad	5,0	4,4	5,6	5,0
Internet	[E.15] Alteración de la información	2,1	2,1		2,1
Internet	[E.19] Fugas de información		5,3		5,3
Internet	[A.5] Suplantación de la identidad	5,7	5,1	6,3	5,7
Internet	[A.6] Abuso de privilegios de acceso	4,5	5,1	3,9	4,5
Internet	[A.7] Uso no previsto	4,5	5,1	3,9	4,5
Internet	[A.11] Acceso no autorizado	5,1	6,3	3,9	5,1

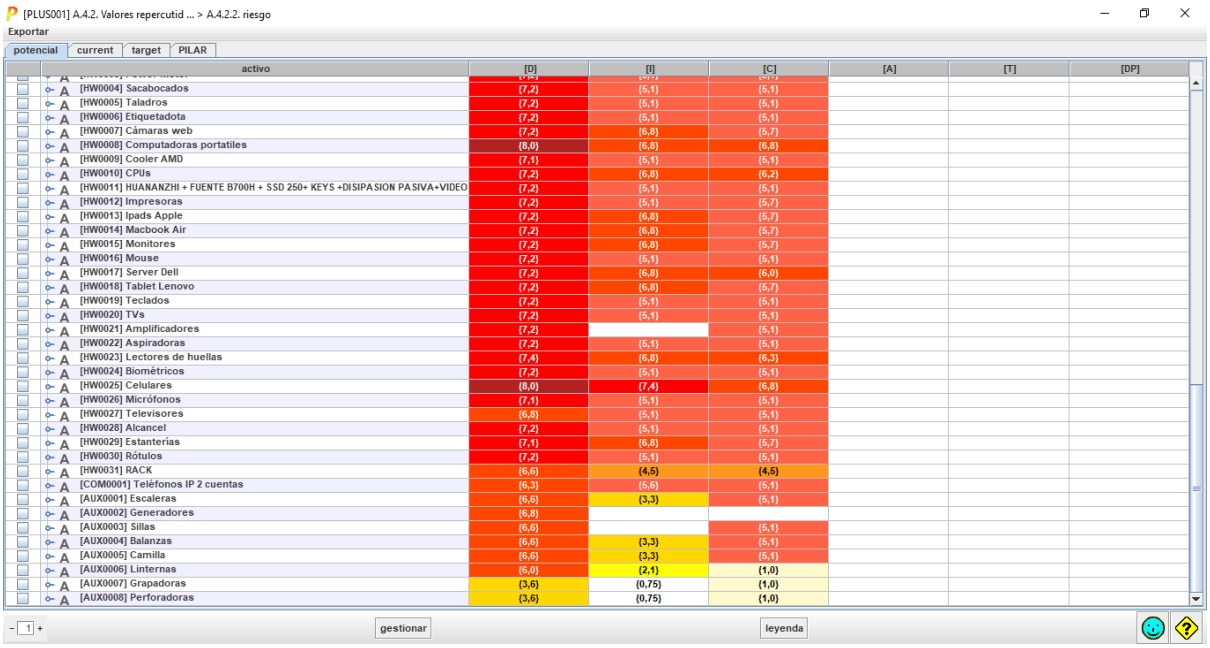
Internet	[A.15] Modificación de la información		6,0		6,0
Mantenimiento	[E.1] Errores de los usuarios	3,3	3,3	3,3	3,3
Mantenimiento	[E.2] Errores del administrador del sistema / de la seguridad	3,8	3,8		3,8
Mantenimiento	[E.15] Alteración de la información		1,5		1,5
Mantenimiento	[E.19] Fugas de información		3,3	3,3	3,3
Mantenimiento	[A.5] Suplantación de la identidad		4,5	4,5	4,5
Mantenimiento	[A.6] Abuso de privilegios de acceso		3,3	3,3	3,3
Mantenimiento	[A.7] Uso no previsto		3,3	3,3	3,3
Mantenimiento	[A.11] Acceso no autorizado		3,3	4,5	3,9
Mantenimiento	[A.15] Modificación de la información		5,4		5,4
Correo	[E.1] Errores de los usuarios	3,3	3,3	3,3	3,3
Correo	[E.2] Errores del administrador del sistema / de la seguridad	3,8	3,8		3,8
Correo	[E.15] Alteración de la información		1,5		1,5
Correo	[E.19] Fugas de información		3,3	3,3	3,3
Correo	[A.5] Suplantación de la identidad		4,5	4,5	4,5
Correo	[A.6] Abuso de privilegios de acceso		3,3	3,3	3,3
Correo	[A.7] Uso no previsto		3,3	3,3	3,3

Correo	[A.11] Acceso no autorizado	3,3	4,5	3,9
Correo	[A.15] Modificación de la información	5,4		5,4

Nota. Elaboración propia

En la Figura 18 se puede observar la información del riesgo potencial acumulado gracias al software Pilar, se puede visualizar de mejor forma el riesgo que podría tener los activos, con esta información se puede llegar a un análisis más a fondo y más preciso en caso de presentarse riesgos a los activos de la empresa.

Figura 18 *Riesgo potencial acumulado de afectación de activos*



Nota. Elaboración propia

Riesgo Potencial Acumulado: Se tiene en cuenta la magnitud del impacto que tiene una amenaza sobre un activo y la probabilidad de que ocurra. La siguiente es la fórmula utilizada para realizar este cálculo:

Riesgo Potencial Repercutido = Probabilidad de Amenaza x Valor Repercutido de Impacto

En la Tabla 27 se muestra el cálculo de los activos que han sido levantados realizando la operación con base en el riesgo potencial repercutido.

Tabla 27 Riesgo potencial repercutido de afectación de activos

Activos	D R	I P	C R	Peso Ponderado
Base de Datos	8,0	7,4	6,8	7,4
Datos de acceso	6,8	6,8	7,2	6,9
Detectores de Humo	8,0	6,2	2,4	5,5
Kit de Seguridad	7,4	5,7	3,0	5,4
Sistema Contable	6,3	6,8	6,2	6,4
Fusionadoras	7,2		5,1	6,2
Cargadores	7,2	5,1	5,1	5,8
Power Meter	7,2	5,1	5,1	5,8
Sacabocados	7,2		5,1	6,2
Taladros	7,2	5,1	5,1	5,8
Etiquetadoras	7,1		5,1	6,1
Cámaras Web	7,2	6,8	5,7	6,6
Portátiles	8,0	6,8	6,8	7,2
Cooler AMD	7,2			7,2
CPU	7,2	6,8	6,2	6,7
Video Card	7,2	5,1	5,1	5,8
Impresoras	7,2	5,1	5,7	6,0
iPad Apple	7,2	6,8	5,7	6,6
MacBook Air	7,2	6,8	5,7	6,6
Monitores	7,2	6,8	5,7	6,6
Mouse	7,2	5,1	5,1	5,8
Server Dell	7,2	6,8	6,0	6,7
Tablet Lenovo	7,2	6,8	5,7	6,6
Teclados	7,2	5,1	5,1	5,8
TV	7,2	5,1	5,1	5,8
Amplificadores	7,1	5,1	5,1	5,8
Aspiradoras	7,2	5,1	5,1	5,8
Lectores de Huellas	7,4	6,8	6,3	6,8
Biométricos	7,2		5,1	6,2
Celulares	8,0	7,4	6,8	7,4
Micrófonos	7,2		5,1	6,2
Televisores	7,1		5,1	6,1
Alcancel	7,1	5,1	5,1	5,8

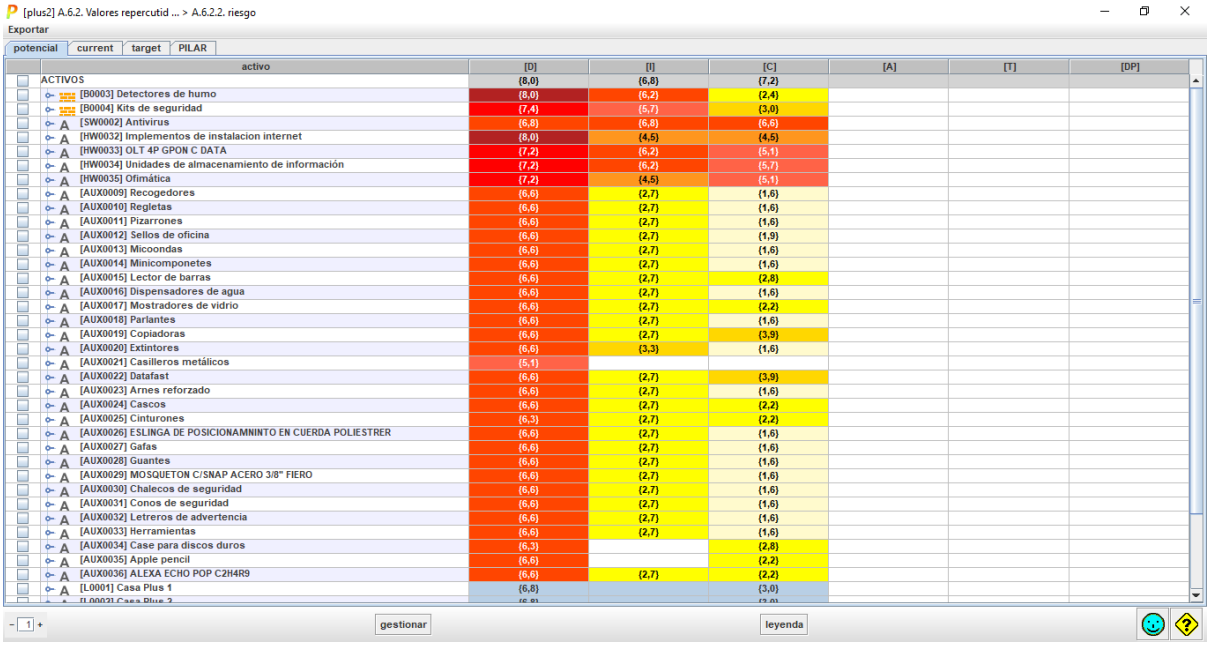
Estanterías	7,2	6,8	5,7	6,6
Rótulos	7,2	5,1	5,1	5,8
Rack	6,6	4,5	4,5	5,2
Instalación internet	8,0	4,5	4,5	5,7
OLT GPON	7,2	6,2	5,1	6,2
Almacenamiento	7,2	6,2	5,7	6,4
Ofimática	7,2	4,5	5,1	5,6
Teléfonos IP 2 cuentas	7,2	5,6	5,1	6,0
Escaleras	6,6	3,3	5,1	5,0
Generadores	6,6			6,6
Sillas	6,6	3,3	5,1	5,0
Balanzas	6,6	3,3	5,1	5,0
Camilla	6,6	3,3	2,1	4,0
Linternas	6,0	2,1	0,9	3,0
Grapadoras	3,6	0,8	1,0	1,8
Perforadoras	3,6	0,8	1,0	1,8
Recogedores	6,6	2,7	1,6	3,6
Regletas	6,6	2,7	1,6	3,6
Pizarrones	6,6	2,7	1,6	3,6
Sellos de Oficina	6,6	2,7	1,9	3,7
Microondas	6,6	2,7	1,6	3,6
Minicomponente	6,6	2,7	1,6	3,6
Lectores de Barras	6,6	2,7	2,8	4,0
Dispensador de agua	6,6	2,7	1,6	3,6
Mostrador de vidrio	6,6	2,7	2,2	3,8
Parlantes	6,6	2,7	1,6	3,6
Copiadoras	6,6	2,7	3,9	4,4
Extintores	6,6	3,3	1,6	3,8
Casilleros metálicos	5,1			5,1
Data Fast	6,6	2,7	3,9	4,4
Arnés Reforzado	6,6	2,7	1,6	3,6
Cascos	6,6	2,7	2,2	3,8
Cinturones	6,3	2,7	2,2	3,7
Eslinga	6,6	2,7	1,6	3,6
Gafas	6,6	2,7	1,6	3,6

Guantes	6,6	2,7	1,6	3,6
Mosquetón	6,6	2,7	1,6	3,6
Chalecos	6,6	2,7	1,6	3,6
Conos de Seguridad	6,6	2,7	1,6	3,6
Letreros Advertencia	6,6	2,7	1,6	3,6
Herramientas	6,6	2,7	1,6	3,6
Case Discos Duros	6,3		2,8	4,6
Apple Pencil	6,6		2,2	4,4
Alexa	6,6	2,7	2,2	3,8
Casa Plus 1	6,8		3,0	4,9
Casa Plus 2	6,8		3,0	4,9
Atención al cliente				
Gerencia Operativa	6,0	5,7	4,2	5,3
Gerencia General	6,3	6,8	7,2	6,8
Gerencia Administrativa	6,0	5,7	4,2	5,3
Gerencia Atención al Cliente	6,0	5,7	2,1	4,6
Gerencia Comercial	6,0	5,7	3,5	5,1

Nota. Elaboración propia

Como se puede visualizar en la Figura 19 se detalla los valores a los que se encuentra referido cada activo en cuanto al riesgo que pueda tener, gracias al software Pilar, nos muestra una información más clara y real en cuanto a la evaluación de riesgos en la empresa.

Figura 19 *Riesgo potencial repercutido de afectación de activos*

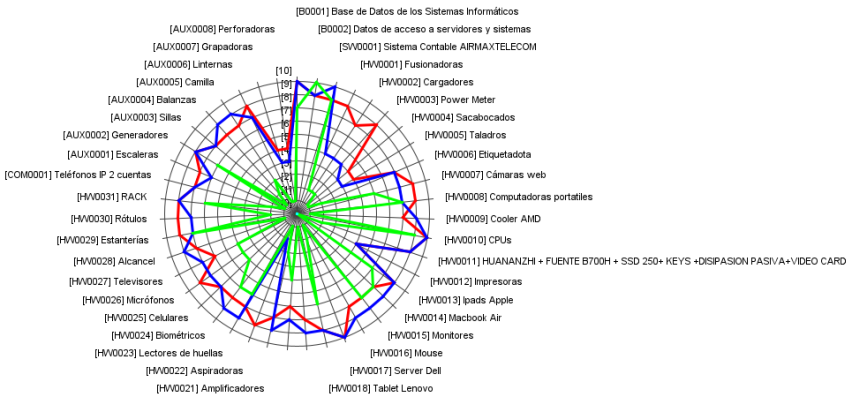


activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS	{8,0}	{6,8}	{7,2}			
[B0003] Detectores de humo	{8,0}	{6,2}	{2,4}			
[B0004] Kits de seguridad	{7,4}	{5,7}	{3,0}			
[SW0002] Antivirus	{6,8}	{6,8}	{6,6}			
[HW0032] Implementos de instalacion internet	{8,0}	{4,5}	{4,5}			
[HW0033] OLT 4P GPON C DATA	{7,2}	{6,2}	{5,1}			
[HW0034] Unidades de almacenamiento de información	{7,2}	{6,2}	{5,7}			
[HW0035] Ofimática	{7,2}	{4,5}	{5,1}			
[AUX0009] Recogedores	{6,6}	{2,7}	{1,6}			
[AUX0010] Regletas	{6,6}	{2,7}	{1,6}			
[AUX0011] Pizarrones	{6,6}	{2,7}	{1,6}			
[AUX0012] Sellos de oficina	{6,6}	{2,7}	{1,9}			
[AUX0013] Micoondas	{6,6}	{2,7}	{1,6}			
[AUX0014] Minicomponetes	{6,6}	{2,7}	{1,6}			
[AUX0015] Lector de barras	{6,6}	{2,7}	{2,8}			
[AUX0016] Dispensadores de agua	{6,6}	{2,7}	{1,6}			
[AUX0017] Mostradores de vidrio	{6,6}	{2,7}	{2,2}			
[AUX0018] Parlantes	{6,6}	{2,7}	{1,6}			
[AUX0019] Copiadoras	{6,6}	{2,7}	{3,9}			
[AUX0020] Extintores	{6,6}	{3,3}	{1,6}			
[AUX0021] Casilleros metálicos	{5,1}					
[AUX0022] Datafast	{6,6}	{2,7}	{3,9}			
[AUX0023] Arnes reforzado	{6,6}	{2,7}	{1,6}			
[AUX0024] Cascos	{6,6}	{2,7}	{2,2}			
[AUX0025] Cinturones	{6,3}	{2,7}	{2,2}			
[AUX0026] ESLINGA DE POSICIONAMNINTO EN CUERDA POLIESTRER	{6,6}	{2,7}	{1,6}			
[AUX0027] Gafas	{6,6}	{2,7}	{1,6}			
[AUX0028] Guantes	{6,6}	{2,7}	{1,6}			
[AUX0029] MOSQUETON C/SNAP ACERO 3/8" FIERO	{6,6}	{2,7}	{1,6}			
[AUX0030] Chalecos de seguridad	{6,6}	{2,7}	{1,6}			
[AUX0031] Conos de seguridad	{6,6}	{2,7}	{1,6}			
[AUX0032] Letreros de advertencia	{6,6}	{2,7}	{1,6}			
[AUX0033] Herramientas	{6,6}	{2,7}	{1,6}			
[AUX0034] Case para discos duros	{6,3}		{2,8}			
[AUX0035] Apple pencil	{6,6}		{2,2}			
[AUX0036] ALEXA ECHO POP C2H4R9	{6,6}	{2,7}	{2,2}			
[L0001] Casa Plus 1	{6,8}		{3,0}			

Nota. Elaboración propia

En la Figura 20 se puede apreciar el impacto acumulado de cada uno de los activos levantados en la empresa, los valores se delimitan por la línea roja, los valores que se marcan con el color azul son los valores recomendados por el software Pilar.

Figura 20 *Gráfico de valores de riesgo acumulado de los activos*



Nota. Elaboración propia

El proceso de gestión de riesgos facilita la identificación de las medidas de protección al calcular el riesgo potencial acumulado sobre el valor total de los activos del sistema. Sin embargo, al

calcular el riesgo potencial que afecta el valor intrínseco de los activos, solo se pueden evaluar los efectos de incidentes relacionados con amenazas específicas.

2.10.8. Tratamiento de Riesgos

En cuanto a tratamiento de riesgos se refiere, se toma en cuenta la identificación, la evaluación de los activos para tener una mejor visión para tomar medidas en las cuales se pueda mitigar, transferir o aceptar los riesgos que pueden suceder en la empresa con la finalidad de reducir el impacto en los activos que están relacionados con la seguridad de la información. Para ello es necesario establecer medidas o procesos para el tratamiento de riesgos apropiadamente para los activos vulnerables y evitar escenarios los cuales comprometan la integridad de la empresa.

2.10.9. Pasos para el Tratamiento de Riesgos

Después de haber establecido lo que es el identificar los activos con sus riesgos con los cuales se asocian las posibles amenazas que podrían comprometer los activos de la empresa en cuanto a información se refiere, se establece lineamientos para poder tener un grado de aceptación de ciertos riesgos. Estos criterios son de gran ayuda para clasificar los riesgos y establecer controles adecuados para los activos, para comprender de mejor forma se muestra la información en la Tabla 28.

Tabla 28 *Niveles de Tratamiento de riesgos*

Zona de Riesgo Residual	**Nivel de Riesgo**	**Tratamiento Para Seguir**	**Ejemplo**
Riesgo Aceptable	Aceptable	Asumir/Aceptar	Fortalecer, Conservar, Mantener
Riesgo Tolerable	Aceptable	Asumir/Aceptar	Infraestructura Actores locales Movilidad
Riesgo No Tolerable	No Aceptable	Reducir/Mitigar	Usuarios Vulnerables Medidas correctivas

Nota. Elaboración propia

- **Aceptar:** Se puede tomar la decisión de asumir el riesgo y las posibles consecuencias sin la necesidad de establecer alguna medida para controlarlo.

- **Transferir:** Se puede tomar la decisión de transferir a otro departamento o a otra entidad tales como aseguradoras.
- **Reducir:** Se puede tomar la decisión de asumir el impacto que pueda tener ese riesgo.
- **Evitar:** Se puede tomar la decisión de eliminar por completo el riesgo o la amenaza.

Es un pilar fundamental en el que la empresa debe enfocarse y evaluarse ante los riesgos inminentes, como se muestra en el Anexo 6, facilita el tratamiento que se puede amenazar y estar preparados para el futuro ante cualquier inconveniente que se pueda presentar y manteniendo la mejora continua. En la Tabla 29 se muestra una matriz en la cual se puede apreciar el tratamiento de riesgos.

Tabla 29 *Matriz de tratamiento de riesgos*

Activos	Amenazas de Activos	Peso	Tratamiento
Base de Datos	[A.11] Acceso no autorizado	7,4	Reducir
Datos de acceso	[A.11] Acceso no autorizado	6,9	Reducir
Detectores de Humo	[A.11] Acceso no autorizado	5,5	Reducir
Kit de Seguridad	A.22] Manipulación de programas	5,4	Reducir
Sistema Contable	[I.5.1] Avería de origen lógico	6,4	Aceptar
Fusionadoras	[A.23] Manipulación del hardware	6,2	Evitar
Cargadores	[A.23] Manipulación del hardware	5,8	Evitar
Power Meter	[A.23] Manipulación del hardware	5,8	Evitar
Sacabocados	[A.23] Manipulación del hardware	6,2	Evitar
Taladros	[A.23] Manipulación del hardware	5,8	Evitar
Etiquetadoras	[A.23] Manipulación del hardware	6,1	Evitar
Cámaras Web	[E.25] Pérdida de equipos	6,6	Reducir
Computadoras Portátiles	[E.25] Pérdida de equipos	7,2	Reducir
Cooler AMD	[E.25] Pérdida de equipos	7,2	Reducir
CPU	[E.25] Pérdida de equipos	6,7	Reducir
Video Card	[E.25] Pérdida de equipos	5,8	Reducir
Impresoras	[A.11] Acceso no autorizado	6,0	Reducir
iPad Apple	[A.11] Acceso no autorizado	6,6	Reducir
MacBook Air	[A.11] Acceso no autorizado	6,6	Reducir
Monitores	[E.25] Pérdida de equipos	6,6	Reducir
Mouse	[E.25] Pérdida de equipos	5,8	Reducir
Server Dell	[A.15] Modificación de la información	6,7	Reducir
Tablet Lenovo	[E.25] Pérdida de equipos	6,6	Reducir

Teclados	[E.25] Pérdida de equipos	5,8	Reducir
TV	[E.25] Pérdida de equipos	5,8	Reducir
Amplificadores	[E.25] Pérdida de equipos	5,8	Reducir
Aspiradoras	[E.25] Pérdida de equipos	5,8	Reducir
Lectores de Huellas	[A.11] Acceso no autorizado	6,8	Evitar
Biométricos	[A.11] Acceso no autorizado	6,2	Evitar
Celulares	[E.25] Pérdida de equipos	7,4	Reducir
Micrófonos	[E.25] Pérdida de equipos	6,2	Reducir
Televisores	[E.25] Pérdida de equipos	6,1	Reducir
Alcancel	[E.25] Pérdida de equipos	5,8	Reducir
Estanterías	[E.25] Pérdida de equipos	6,6	Reducir
Rótulos	[E.25] Pérdida de equipos	5,8	Reducir
Rack	[A.11] Acceso no autorizado	5,2	Reducir
Instalación internet	[A.15] Modificación de la información	5,7	Reducir
OLT GPON	[E.25] Pérdida de equipos	6,2	Reducir
Unidades de Almacenamiento	[A.25] Robo de equipos	6,4	Reducir
Ofimática	[E.25] Pérdida de equipos	5,6	Reducir
Teléfonos IP 2 cuentas	[E.25] Pérdida de equipos	6,0	Reducir
Escaleras	[A.11] Acceso no autorizado	5,0	Evitar
Generadores	[A.11] Acceso no autorizado	6,6	Evitar
Sillas	[E.25] Pérdida de equipos	5,0	Reducir
Balanzas	[E.25] Pérdida de equipos	5,0	Reducir
Camilla	[E.25] Pérdida de equipos	4,0	Reducir
Linternas	[E.25] Pérdida de equipos	3,0	Reducir
Grapadoras	[E.25] Pérdida de equipos	1,8	Reducir
Perforadoras	[E.25] Pérdida de equipos	1,8	Reducir
Recogedores	[E.25] Pérdida de equipos	3,6	Reducir
Regletas	[E.25] Pérdida de equipos	3,6	Reducir
Pizarrones	[E.25] Pérdida de equipos	3,6	Reducir
Sellos de Oficina	[E.25] Pérdida de equipos	3,7	Reducir
Microondas	[E.25] Pérdida de equipos	3,6	Reducir
Minicomponente	[A.11] Acceso no autorizado	3,6	Evitar
Lectores de Barras	[A.11] Acceso no autorizado	4,0	Evitar
Dispensador de agua	[E.25] Pérdida de equipos	3,6	Evitar
Mostrador de vidrio	[E.25] Pérdida de equipos	3,8	Evitar

Parlantes	[E.25] Pérdida de equipos	3,6	Evitar
Copiadoras	[E.25] Pérdida de equipos	4,4	Evitar
Extintores	[A.11] Acceso no autorizado	3,8	Evitar
Casilleros metálicos	[A.11] Acceso no autorizado	5,1	Evitar
Data Fast	[A.11] Acceso no autorizado	4,4	Evitar
Arnés Reforzado	[E.25] Pérdida de equipos	3,6	Evitar
Cascos	[E.25] Pérdida de equipos	3,8	Evitar
Cinturones	[E.25] Pérdida de equipos	3,7	Evitar
Eslinga	[E.25] Pérdida de equipos	3,6	Evitar
Gafas	[E.25] Pérdida de equipos	3,6	Evitar
Guantes	[E.25] Pérdida de equipos	3,6	Evitar
Mosquetón	[E.25] Pérdida de equipos	3,6	Evitar
Chalecos	[E.25] Pérdida de equipos	3,6	Evitar
Conos de Seguridad	[E.25] Pérdida de equipos	3,6	Evitar
Letreros de Advertencia	[A.11] Acceso no autorizado	3,6	Evitar
Herramientas	[A.11] Acceso no autorizado	3,6	Evitar
Case para Discos Duros	[A.11] Acceso no autorizado	4,6	Evitar
Apple Pencil	[A.25] Robo de equipos	4,4	Evitar
Alexa	[A.11] Acceso no autorizado	3,8	Reducir
Casa Plus 1	[A.30] Ingeniería social (picaresca	4,9	Evitar
Casa Plus 2	[A.30] Ingeniería social (picaresca	4,9	Evitar
Atención al cliente	[A.30] Ingeniería social (picaresca	4,9	Evitar
Gerencia Operativa	[A.30] Ingeniería social (picaresca	5,3	Evitar
Gerencia General	[A.30] Ingeniería social (picaresca	6,8	Evitar
Gerencia Administrativa	[A.30] Ingeniería social (picaresca	5,3	Evitar
Gerencia Atención al Cliente	[A.30] Ingeniería social (picaresca	4,6	Evitar
Gerencia Comercial	[A.30] Ingeniería social (picaresca	5,1	Evitar

Nota. Elaboración propia

2.11. Controles la Norma ISO/IEC 27002:2022

Según la Norma ISO/IEC 27002:2022, que proporciona ciertos parámetros para buenas prácticas al establecer y mantener un Sistema de Gestión de Seguridad de la Información en una organización, en este caso la empresa de Internet AIRMAXTELECOM Soluciones Tecnológicas S.A. para contrarrestar los riesgos y amenazas si comprometen la seguridad de la información.

Para la selección de los controles ante los activos, se ha evaluado uno por uno con base en lo establecido en la norma y los 93 controles que contiene.

2.11.1. Controles para Implementar en la Empresa AIRMAXTELECOM

Mediante el análisis de la Norma y los controles, se puede designar mediante las amenazas de cada activo de la organización para reducir, mitigar, transferir, aceptar según el nivel de riesgo, como se visualiza en la Tabla 30.

Tabla 30 *Identificación de dominios, Objetivos, controles*

Activos	Amenazas de Activos	Dominios	Objetivos	Controles
Base de Datos	[A.11] Acceso no autorizado	Planificación	9.1 Requisitos de negocio para el control de accesos	9.1 Requisitos de negocio para el control de accesos
Datos de acceso	[A.11] Acceso no autorizado	Apoyo	9.1 Requisitos de negocio para el control de accesos	8.2 Derechos de acceso privilegiados
Detectores de Humo	[A.11] Acceso no autorizado	Apoyo	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos
Kit de Seguridad	A.22] Manipulación de programas	Apoyo		13.2 Control de cambios técnicos
Sistema Contable	[I.5.1] Avería de origen lógico	Planificación	12.6 Gestión de la vulnerabilidad técnica.	8.2 Derechos de acceso privilegiados
Fusionadoras	[A.23] Manipulación del hardware	Apoyo	13. Control de cambio.	14.2 Gestión de proveedores de servicios
Cargadores	[A.23] Manipulación del hardware	Apoyo	12. Control de operaciones.	14.2 Gestión de proveedores de servicios
Power Meter	[A.23] Manipulación del hardware	Apoyo	14. Seguridad de la información relacionada con proveedores.	14.2 Gestión de proveedores de servicios

Sacabocados	[A.23] Manipulación del hardware	Apoyo	14. Seguridad de la información relacionada con proveedores.	14.2 Gestión de proveedores de servicios
Taladros	[A.23] Manipulación del hardware	Apoyo	14. Seguridad de la información relacionada con proveedores.	14.2 Gestión de proveedores de servicios
Etiquetadoras	[A.23] Manipulación del hardware	Apoyo	14. Seguridad de la información relacionada con proveedores.	14.2 Gestión de proveedores de servicios
Cámaras Web	[E.25] Pérdida de equipos	Apoyo	14. Seguridad de la información relacionada con proveedores.	11.1 Responsabilidad de los activos
Computadoras Portátiles	[E.25] Pérdida de equipos	Planificación	14. Seguridad de la información relacionada con proveedores.	11.1 Responsabilidad de los activos
Cooler AMD	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
CPU	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	Control (Código)
Video Card	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	9.1 Requisitos de negocio para el control de accesos

Impresoras	[A.11] Acceso no autorizado	Apoyo	Objetivo (Código)	11.1 Responsabilidad de los activos
iPad Apple	[A.11] Acceso no autorizado	Apoyo	9. Control de accesos.	11.1 Responsabilidad de los activos
MacBook Air	[A.11] Acceso no autorizado	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Monitores	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Mouse	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Server Dell	[A.15] Modificación de la información	Planificación	11. Gestión de activos de la organización.	9.1 Requisitos de negocio para el control de accesos
Tablet Lenovo	[E.25] Pérdida de equipos	Planificación	11. Gestión de activos de la organización.	9.1 Requisitos de negocio para el control de accesos
Teclados	[E.25] Pérdida de equipos	Apoyo	9. Control de accesos.	11.1 Responsabilidad de los activos
TV	[E.25] Pérdida de equipos	Apoyo	9. Control de accesos.	11.1 Responsabilidad de los activos
Amplificadores	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos

Aspiradoras	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Lectores de Huellas	[A.11] Acceso no autorizado	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Biométricos	[A.11] Acceso no autorizado	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Celulares	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	9.1 Requisitos de negocio para el control de accesos
Micrófonos	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	12.1 Procesos y procedimientos operativos
Televisores	[E.25] Pérdida de equipos	Apoyo	9. Control de accesos.	11.1 Responsabilidad de los activos
Alcancel	[E.25] Pérdida de equipos	Apoyo	12. Control de operaciones.	11.1 Responsabilidad de los activos
Estanterías	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Rótulos	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Rack	[A.11] Acceso no autorizado	Apoyo	11. Gestión de activos de la organización.	9.1 Requisitos de negocio para el control de accesos

Instalación internet	[A.15] Modificación de la información	Planificación	11. Gestión de activos de la organización.	9.1 Requisitos de negocio para el control de accesos
OLT GPON	[E.25] Pérdida de equipos	Planificación	9. Control de accesos.	11.1 Responsabilidad de los activos
Unidades de Almacenamiento	[A.25] Robo de equipos	Planificación	9. Control de accesos.	11.1 Responsabilidad de los activos
Ofimática	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Teléfonos IP 2 cuentas	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Escaleras	[A.11] Acceso no autorizado	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Generadores	[A.11] Acceso no autorizado	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Sillas	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Balanzas	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Camilla	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos

Linternas	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Grapadoras	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Perforadoras	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	9.1 Requisitos de negocio para el control de accesos
Recogedores	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	9.1 Requisitos de negocio para el control de accesos
Regletas	[E.25] Pérdida de equipos	Apoyo	9. Control de accesos.	11.1 Responsabilidad de los activos
Pizarrones	[E.25] Pérdida de equipos	Apoyo	9. Control de accesos.	11.1 Responsabilidad de los activos
Sellos de Oficina	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Microondas	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Minicomponente	[A.11] Acceso no autorizado	Apoyo	11. Gestión de activos de la organización.	9.1 Requisitos de negocio para el control de accesos
Lectores de Barras	[A.11] Acceso no autorizado	Apoyo	11. Gestión de activos de la organización.	9.1 Requisitos de negocio para el control de accesos
Dispensador de agua	[E.25] Pérdida de equipos	Apoyo	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos

Mostrador de vidrio	[E.25] Pérdida de equipos	Apoyo	9. Control de accesos.	11.1 Responsabilidad de los activos
Parlantes	[E.25] Pérdida de equipos	Apoyo	9. Control de accesos.	11.1 Responsabilidad de los activos
Copiadoras	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Extintores	[A.11] Acceso no autorizado	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Casilleros metálicos	[A.11] Acceso no autorizado	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Data Fast	[A.11] Acceso no autorizado	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Arnés Reforzado	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Cascos	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Cinturones	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	11.1 Responsabilidad de los activos
Eslinga	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	9.1 Requisitos de negocio para el control de accesos
Gafas	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	9.1 Requisitos de negocio para el control de accesos

Guantes	[E.25] Pérdida de equipos	Apoyo	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos
Mosquetón	[E.25] Pérdida de equipos	Apoyo	9. Control de accesos.	11.1 Responsabilidad de los activos
Chalecos	[E.25] Pérdida de equipos	Apoyo	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos
Conos de Seguridad	[E.25] Pérdida de equipos	Apoyo	11. Gestión de activos de la organización.	16.1 Gestión de incidentes y mejoras
Letreros de Advertencia	[A.11] Acceso no autorizado	Apoyo	9. Control de accesos.	16.1 Gestión de incidentes y mejoras
Herramientas	[A.11] Acceso no autorizado	Apoyo	16. Gestión de incidentes de seguridad de la información	16.1 Gestión de incidentes y mejoras
Case para Discos Duros	[A.11] Acceso no autorizado	Apoyo	16. Gestión de incidentes de seguridad de la información	16.1 Gestión de incidentes y mejoras
Apple Pencil	[A.25] Robo de equipos	Apoyo	16. Gestión de incidentes de seguridad de la información	16.1 Gestión de incidentes y mejoras
Alexa	[A.11] Acceso no autorizado	Apoyo	16. Gestión de incidentes de seguridad de la información	16.1 Gestión de incidentes y mejoras
Casa Plus 1	[A.30] Ingeniería social (picaresca	Apoyo	16. Gestión de incidentes de seguridad de la información	16.1 Gestión de incidentes y mejoras
Casa Plus 2	[A.30] Ingeniería social (picaresca	Apoyo	16. Gestión de incidentes de seguridad de la información	16.1 Gestión de incidentes y mejoras

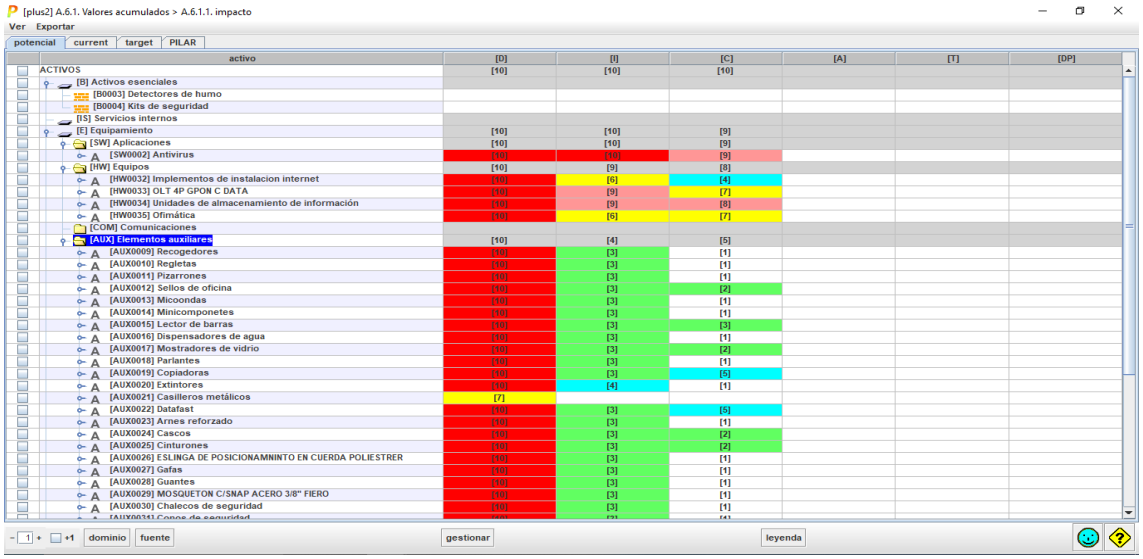
Atención al cliente	[A.30] Ingeniería social (picaresca	Apoyo	16. Gestión de incidentes de seguridad de la información	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Gerencia Operativa	[A.30] Ingeniería social (picaresca	Liderazgo y Compromiso	16. Gestión de incidentes de seguridad de la información	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Gerencia General	[A.30] Ingeniería social (picaresca	Liderazgo y Compromiso	7.2 Durante la contratación	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Gerencia Administrativa	[A.30] Ingeniería social (picaresca	Liderazgo y Compromiso	7.2 Durante la contratación	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Gerencia Atención al Cliente	[A.30] Ingeniería social (picaresca	Liderazgo y Compromiso	7.2 Durante la contratación	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Gerencia Comercial	[A.30] Ingeniería social (picaresca	Liderazgo y Compromiso	7.2 Durante la contratación	7.2.2 Concienciación, educación y capacitación en seguridad de la información

Nota. Elaboración propia

2.11.2. Estimación de Impacto Residual

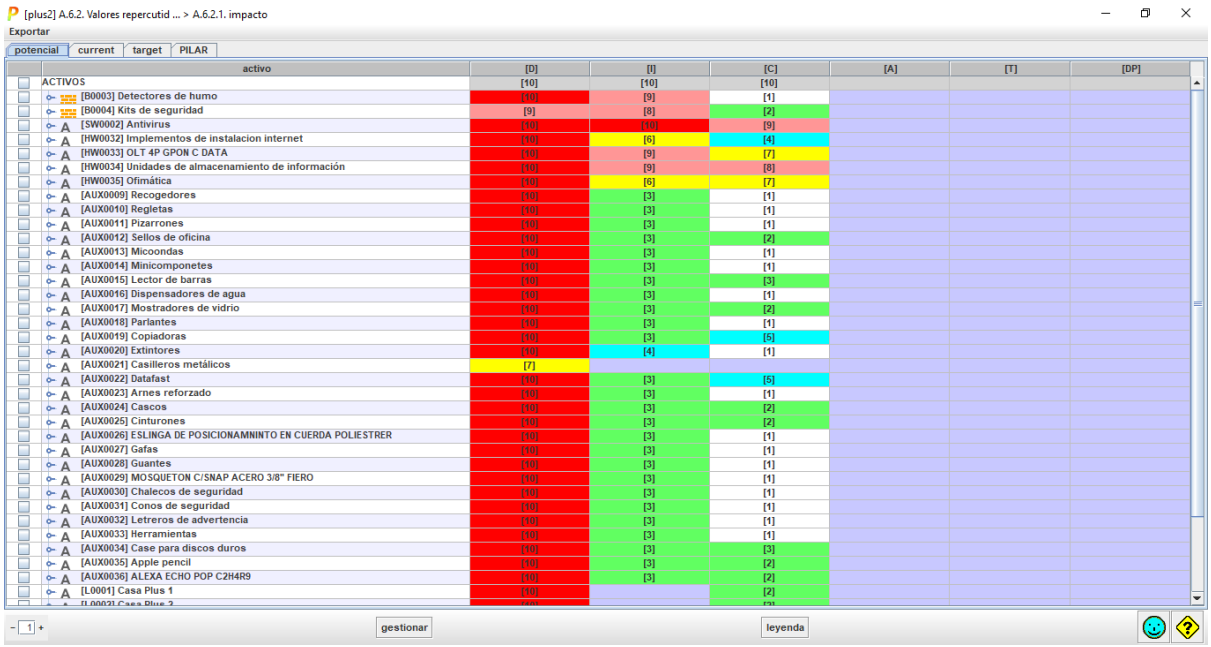
El sistema cambia su impacto potencial inicial a un impacto residual si se realiza las acciones que sugiere el software Pilar para llevar a cabo los controles. Esto se debe al hecho de que esta herramienta simula la implementación de controles y ofrece una evaluación del impacto residual acumulado y sus consecuencias, como se puede observar en la Figura 21 la acumulación del impacto residual y la Figura 22 se puede visualizar como se refleja o afecta este impacto residual.

Figura 21 *Impacto residual acumulado de los activos*



Nota. Elaboración propia

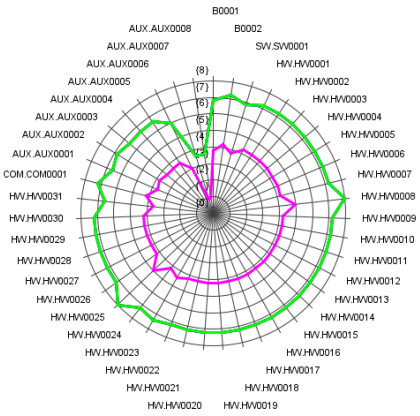
Figura 22 *Impacto Residual Repercutido de los Activos*



Nota. Elaboración propia

Como se observa en la Figura 23, son los valores que el software Pilar sugiere se encuentren dentro de los parámetros establecidos.

Figura 23 *Gráfico de valores de impacto de activos*



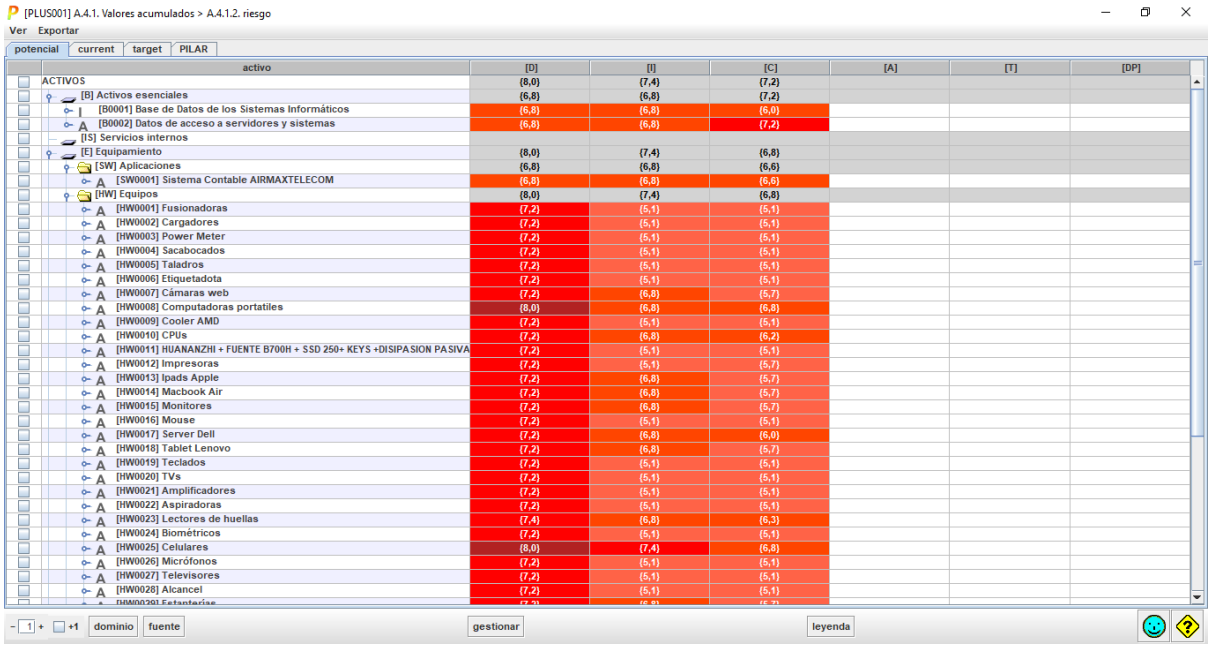
Nota. Elaboración propia**.**

2.11.3. Estimación de Impacto Residual

El software Pilar hace la simulación en cuanto a los controles y proporciona una evaluación de riesgos residual acumulado y el riesgo residual repercutido.

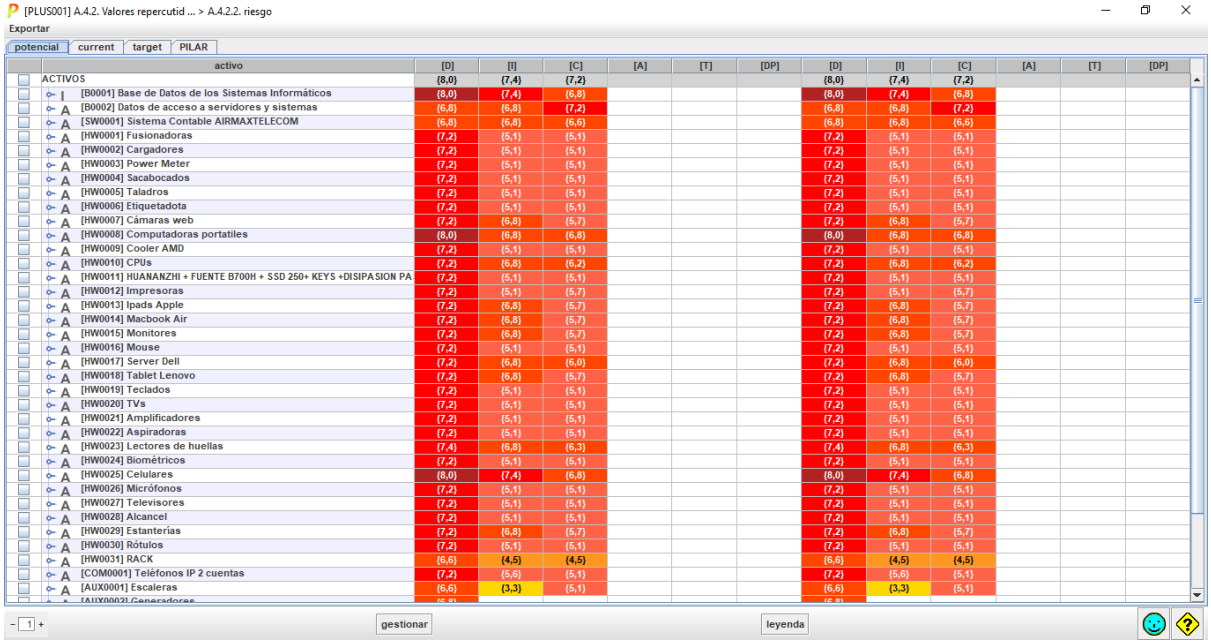
Como se puede visualizar en la Figura 24 se aprecia la acumulación del riesgo residual, mientras que en la Figura 25 se aprecia la manifestación del riesgo residual.

Figura 24 *Riesgo residual acumulado de afectación de activos*



Nota: Elaboración Propia

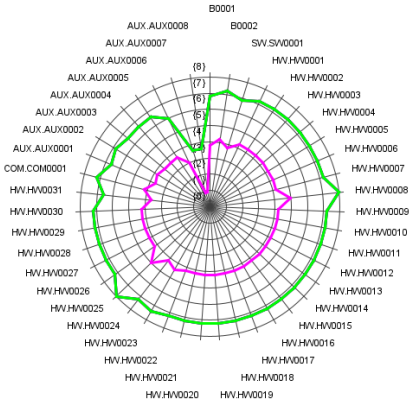
Figura 25 Riesgo residual repercutido en el caso de afectar los activos



Nota. Elaboración propia

Como se puede apreciar en la Figura 26 se puede visualizar la gráfica donde se muestra los riesgos potenciales actuales con base en el análisis del software Pilar

Figura 26 *Gráfico de valores de riesgo de activos del sistema financiero*



Nota. Elaboración propia

2.12. Políticas de Seguridad

2.12.1. Objetivos de las Políticas de Seguridad

Como parte vital de toda empresa para tener procesos, lineamientos, directrices, leyes a las cuales debe acatarse las personas que comprenden la organización, es necesario determinar políticas para tener un mejor desempeño en este caso en la Empresa AIRMAXTELECOM Soluciones Tecnológicas S.A. comprometiéndose a mantener seguros los activos que se encuentran relacionados con la información, normas que deben ser asumidas con respeto y a cabalidad, las cuales no deberán ser modificadas o alteradas a excepción que los altos mandos así lo requieran, no deberán ser divulgados con personas externas, manteniendo su integridad y confidencialidad.

La seguridad de la información en este caso las políticas son más conocidos por ser documentos redactados y presentados formalmente, estableciendo lineamientos a seguir tal como las dicta la persona responsable de establecerlas con el propósito mayor que es la seguridad de la información, las políticas conforman un esquema de seguridad el cual busca habiendo analizado ya la situación de la empresa mitigar los riesgos, es por ello que estableciendo lineamientos específicos se puede lograr un nivel de seguridad óptimo para la empresa y su información.

En el contexto, en cuanto a las políticas de seguridad, se deben enfocar en sus riesgos y amenazas ya detectadas en el análisis de cada uno de los activos levantados en la empresa, las políticas de seguridad de la información dan una ventaja a la empresa al momento de ponerlas en vigencia, a continuación, se detalla algunas de las ventajas que brindan las políticas.

- Protección de activos: Contribuyen a la protección de los activos con los que cuenta la empresa tales como, información confidencial, sistemas de información, personal que maneja información, establecimiento en donde se realizan las actividades, reduciendo a un nivel considerable la posibilidad de que se vea comprometida de seguridad.
- Cumplimiento legal y regulatorio: Toda empresa viene respaldada no solo por políticas, sino también por leyes y regulaciones, las cuales deben ser cumplidas en la organización, evitando escenarios que comprometan la integridad de la empresa, su privacidad y confidencialidad.
- Reducción de riesgos: Lograr identificas los riesgos y amenazas a los que se encuentra la empresa y sus activos para ser gestionados de forma óptima con la finalidad de reducir su nivel de incidencia y consecuencias dentro de la empresa.
- Mejora en la confianza: La empresa puede generar y ganar la confianza tanto de las personas que lo conforman como la de sus clientes por medio de políticas que brinden seguridad, siendo un punto clave para ganar clientes y elevando sus ingresos.
- Protección de la reputación: Las políticas evitan que la empresa se ve a comprometida ante la exposición pública y los incidentes que pueden comprometer la reputación de la empresa y sus clientes.
- Eficiencia operativa: Al establecer lineamientos en cuanto al manejo de información y su seguridad, se puede mantener una eficiencia laboral optimizando los recursos.
- Cultura de seguridad: Es un punto importante dentro de la empresa, puesto que es una buena práctica en cuanto a cultura de seguridad de la información, en donde las personas que conforman la empresa tengan el conocimiento de la importancia de la seguridad de la información y se comprometan a ejercerlas a diario.

2.12.2. Responsabilidad

Debe estar al frente una persona capacitada que tenga conocimiento de la situación de la empresa y que tenga conocimiento acerca de políticas y seguridad de la información cumpliendo ciertas actividades:

- Ser responsable y liderar las actividades propuestas con el fin de ser cumplidas por todos los miembros que conforman la empresa AIRMAXTELECOM Soluciones Tecnológicas S.A.
- Gestionar el mantenimiento de la infraestructura de hardware, software, redes de comunicación, bases de datos, infraestructura de la red.
- Estar en conocimiento continuo, no solo de un departamento, sino de los que conforman la empresa, conociendo sus necesidades y proveer soluciones óptimas.
- Administrar de forma responsable la infraestructura de la red, bases de datos y todo lo que comprenda y maneje información.
- Planificación y ejecución de las normas de seguridad.
- Poner en conocimiento las políticas de seguridad, en caso de realizarse cambios o incrementar políticas, informar y capacitar al personal.

2.12.3. Políticas de Seguridad de la Información

Como se puede visualizar en la Tabla 31, se plantean políticas de seguridad que se encuentran en el Anexo 7 con sus procedimientos, los cuales deben ser cumplidos, tal cual lo dicta cada una de estas para garantizar el buen funcionamiento de la empresa. En conjunto, estos lineamientos aseguran en un gran porcentaje que se disminuirá la posibilidad de riesgos ante los activos de la empresa.

Tabla 31 *Políticas de la seguridad de la información*

Dominio	Resumen de Objetivo y Control	Detalles de Políticas
1. Políticas de Seguridad	1.1 Directrices de la Dirección en Seguridad de la Información 1.1.1. Conjunto de políticas que estén a favor de la seguridad de la información. 1.1.2. Revisión de políticas de seguridad	Políticas generales. Definición de la documentación dentro de los requisitos legales y regulatorios en vigencia. Definir procesos para identificar, evaluar y mitigar los riesgos de seguridad de la información.
2. Aspectos Organizativos	**2.1 Organización interna**	La empresa debe tener personal capacitado en seguridad de la información en la empresa de

	2.1.1 Asignación de responsables 2.1.2 Asignación de tareas 2.1.3 Seguridad de la información en la gestión de proyectos **2.2 Dispositivos para trabajo remoto** 2.2.1 Dispositivos y red que permita el desempeño de labores de forma remota.	internet AIRMAXTELECOM Soluciones Tecnológicas S.A. con la finalidad de periódicamente establecer políticas de seguridad de la información, capacitar al personal y asignar roles y actividades para lograr tener un óptimo desempeño.
3. Seguridad en RRHH	**3.1 Antes de contratar** 3.1.1 Entrevista y revisión de antecedentes. 3.1.2 Términos y condiciones **3.2 Durante el contrato** 3.2.1 Responsabilidad en la gestión. 3.2.2 Conocimiento de la formación en su vida académica.	La empresa debe realizar el proceso de capacitación en cuanto a los lineamientos y políticas relevantes.
4. Gestión de activos	**4.1 Responsabilidad de activos** 4.1.1 Realizar periódicamente el levantamiento de activos. 4.1.2 Utilizar de forma adecuada los activos. 4.1.3 Realizar el análisis de riesgos y amenazas para	El personal encargado de realizar la gestión de activos debe comprender la importancia de tener un inventario de los activos de la empresa con la finalidad de ser analizados ante los posibles riesgos. Establecer manuales para la gestión de activos, administrar

	contrarrestarlas periódicamente.	las instalaciones, realizar backups de la información, monitorear los sistemas.
	4.2 Manejo de almacenamiento	
	4.2.1 Gestión de almacenamiento de los activos.	
	4.2.2 Almacenar de forma segura los activos, con cerraduras adecuadas.	
	5.1 Requerimientos de acceso.	
	5.1.1 Políticas de control de acceso.	
	5.1.2 Portar las credenciales de la empresa para conceder el acceso.	
	5.2 Gestión de acceso de usuarios.	Establecer manuales para el control de acceso.
5. Controles de acceso	5.2.1 Manejo y uso correcto de la información de acceso y autenticación.	Políticas que delimiten el acceso al personal de acuerdo con el área de trabajo.
	5.3 Control de accesos a sistemas.	Revisión de accesos de usuario.
	5.3.1 Restringir el acceso no autorizado.	
	5.3.2 Delimitar el acceso al personal solamente al área designada para desarrollar sus tareas.	

	5.3.3 Procedimientos de acceso seguro e inicios de sesión.	
6. Cifrado	**6.1 Controles criptográficos** 6.1.1 Gestión de claves 6.1.2 Cambio periódico de claves de acuerdo con pautas en las que debe estar una contraseña.	Definir estándares en los cuales debe ir una contraseña tales como: • Mayúsculas • Minúsculas • Números • Caracteres. • No usar contraseñas como fechas o nombres de la empresa.
7. Seguridad física	**7.1 Áreas seguras.** 7.1.1 Protección en los ingresos al establecimiento. 7.1.2 Delimitar el acceso a ciertas áreas solo a personal autorizado. 7.1.3 Mantener aseguradas las áreas en donde se resguarda información. 7.1.4 Mantener los gabinetes y estanterías con puertas y candados. **7.2 Seguridad de los activos** 7.2.1 Protección segura para los activos.	Establecer y delimitar normativas en las cuales se garantice el orden y cuidado de los activos. Delimitar el acceso a las áreas sensibles en el caso de personal que no pertenezca a la empresa o practicantes.

	7.2.2 Mantenimiento preventivo y correctivo de los equipos.	
	7.2.3 Auditorias constantes a los activos físicos e instalaciones**.**	
	8.1 Responsabilidad operacional	
	8.1.1 Documentación en regla de los procesos empresariales.	
	8.2 Registro de actividades.	
8. Seguridad operativa	8.2.1 Monitoreo y registro continuo de actividades del personal de la empresa ya sea de las actividades que se realizan a nivel operativo y de sistemas.	Determinar políticas de seguridad operacional para constante monitoreo de actividades en hardware y software.
	8.3 Gestión de vulnerabilidades	Revisión de licencias adecuadas en los sistemas que se utilizan en la empresa.
	8.3.1 Restricción de software o instalación de licencias no autorizadas.	
	8.3.2 Mantener las licencias de los dispositivos en condiciones óptimas, Office, Antivirus.	
	8.3.3 Auditorias a los sistemas.	
	9.1 Gestión de comunicación	Políticas de seguridad de intercambio de información.
9. Seguridad en telecomunicaciones	9.1.1 Controles de servicios en la red.	Controles y protección de datos a los cuales se tiene acceso.

	9.2 Intercambio de información. 9.2.1 Políticas y procedimientos que controlen el intercambio de información. 9.2.2 Clausulas de acuerdos de confidencialidad. 9.2.3 Cifrado de extremo a extremo. 9.2.4 Pautas de uso seguro de dispositivos. 9.2.5 Principios de protección en base a la ingeniería en sistemas. 9.2.6 Pruebas de correcta funcionalidad.	Limitar la información que se puede informas a personas externas de la empresa. Pruebas de funcionalidad y confidencialidad en la comunicación de la empresa.
10. Mantenimiento de sistemas de información	**10.1 Seguridad en los sistemas de información** 10.1.1 Establecer parámetros de seguridad. 10.1.2 Protección de transacciones. 10.1.3 Contraseñas estandarizadas y su protección. 10.1.4 Pruebas de ataques al sistema y reforzar la seguridad periódicamente. 10.1.5 Licencias y antivirus originales.	Garantizar la protección de datos, realizando pruebas periódicamente a los sistemas, controlando que no haya perdida o alteración de información. Garantizar la confidencialidad e integridad de la información sensible para el acceso en áreas no autorizadas.

10.1.6 Seguridad en el entorno de desarrollo.
10.1.7 Mejora continua.

Nota. Elaboración propia

2.13. Mejora Continua

EL proceso de mejora continua del SGSI que se realizó con las Normas de Seguridad ISO/IEC 27001 – 27002: 2022 como punto importante conlleva la revisión de los controles, políticas y lineamientos para adaptarlos a la empresa basándose en la situación actual. Este proceso tiene como finalidad dar el tratamiento correcto a los riesgos y mitigarlos. Se incentiva a crear nuevas actividades y ponerlas en práctica para contrarrestar las posibles amenazas y riesgos de manera óptima para la empresa en cuanto a los activos levantados y tener un esquema de seguridad favorable para la información.

- Se recomienda hacer auditorias periódicamente del SGSI para poder tener un control constante y mejorar conforme va pasando el tiempo y detectando posibles riesgos.
- Controlar que las políticas se estén acatando a cabalidad en las áreas designadas por el personal de la empresa, que todos los miembros de la empresa tengan conocimiento de las políticas actualizadas para garantizar la seguridad de la información.
- Mantener periódicamente el levantamiento y evaluación de los activos para tener un inventario más actualizado y controlar las amenazas instaurando los controles pertinentes.
- Capacitar de forma regular y continua a los miembros que conforman la empresa para mantener y garantizar la seguridad de la información.
- Auditorías tanto internas como externas con personal capacitado, ayudan a tener un mejor control en la empresa, es una medida que se recomienda en las empresas para tener una mejor visión de la situación de la empresa y lograr controlar el riesgo y amenazas.
- Dar a conocer la importancia y los beneficios que trae a la empresa el implementar un SGSI para la seguridad de activos e información.

2.14. Plan de Gestión de Riesgos

Para identificar, evaluar y gestionar los riesgos de seguridad de la información en una organización, es necesario un plan de gestión de riesgos basado en las normas ISO 27001 y 27002:2022.

Para crear un plan de gestión de riesgos que cumpla con estas normas, aquí está un resumen de los pasos esenciales que se deben seguir:

1. **Establecimiento del contexto:**

   - Determine el alcance y los objetivos del plan de gestión de riesgos.
   - Determine las normas para evaluar el riesgo y la tolerancia al riesgo.

2. **Identificación de activos:**

   - Identificar y clasificar todos los activos de información de la organización, incluidos sistemas, datos, infraestructura y procesos.

3. **Identificar los peligros y las vulnerabilidades:**

   - Identificar las amenazas potenciales para los activos de información.

4. **Análisis de riesgos:**

   - Evaluar la probabilidad de que ocurran las amenazas identificadas y su impacto potencial en los activos de información.
   - Calcule el riesgo inherente de cada amenaza y vulnerabilidad.

5. **Evaluación de riesgos:**

   - Aplicar los controles existentes para determinar el nivel de riesgo residual.
   - Evaluar el riesgo residual en comparación con los estándares de tolerancia al riesgo establecidos anteriormente.

6. **Tratamiento de riesgos:**

   - Desarrolle métodos de tratamiento de riesgos que reduzcan, transfieran, eviten o acepten los riesgos.
   - Clasificar las medidas de tratamiento de riesgos en función de su eficacia y costo.

Todo este procedimiento se puede realizar con la ayuda del Software Pilar y el documento de Excel de Gestión de Riesgos.

7. **Implementación de controles:**

- Elegir e implementar los controles de seguridad de la información apropiados para reducir los riesgos.
- Asegurarse de que los controles implementados sean efectivos y cumplan con las normas ISO 27001 y 27002.

8. **Seguimiento y revisión:**

- Mantener un seguimiento continuo de los riesgos de seguridad de la información y de la eficacia de los controles implementados.
- Realizar revisiones regulares del plan de gestión de riesgos para asegurarse de que sea relevante y actualizado.

9. **Mejora continua:**

- Identificar oportunidades para mejorar los controles de seguridad de la información y la gestión de riesgos.
- Implementar proactivamente medidas correctivas y preventivas para mejorar la seguridad de la información.

2.15. Plan de Implementación

Se ha desarrollado una serie de lineamientos en los cuales la empresa AIRMAXTELECOM Soluciones Tecnológicas S.A. debe basarse para su implementación, como se muestra en la Tabla 32.

Tabla 32 *Lineamientos para implementación de SGSI*

Implementación del Sistema de Gestión de seguridad de la Información	
Poner en práctica los controles que se definieron en la Norma ISO 27001 – 27002: 2022, conforme a las políticas de seguridad que se establecieron en el desarrollo del SGSI	Para garantizar que la puesta en práctica e implementación en cuanto a las políticas ya mencionadas anteriormente y en el documento que se las clasifica, es necesario que la empresa lo ejecute con responsabilidad para así evitar percances Como recomendación principal a la empresa, se incita a la revisión previa de la documentación, con la metodología de CheckList y análisis de activos, levantando

	activos y verificando amenazas, plan en caso de riesgos y como responder ante una situación vulnerable, controles y políticas de seguridad en aspectos físicos y lógicos de los activos.
Implementación de Controles	Como paso principal para empezar el SGSI se realizó el levantamiento de activos e información de la empresa AIRMAXTELECOM Soluciones Tecnológicas S.A. para valorar sus riesgos y amenazas y delimitar el tratamiento en caso de verse comprometido, con toda esta información se logra definir los controles del SGSI. Se recomienda detallar los controles que se va a utilizar para delimitar que recursos van a intervenir, logrando un desarrollo óptimo. Designar personal capacitado y encargado específicamente al área de seguridad de la información, delegando responsabilidades y actividades calendarizadas para consiguiente poner en prácticas los controles que se detallan en el documento.
Ejecución del Plan de Gestión de Incidentes	Es importante que el personal a cargo lleve registros de incidentes que se hayan suscitado en la empresa con la finalidad de reducir, controlar, transferir o eliminar los riesgos recurriendo a las políticas de seguridad. Designar responsables en la organización según la empresa crea conveniente con el conocimiento de habilidades de sus integrantes. Crear planes de contingencia ante posibles situaciones que comprometan a la empresa. Realizar la documentación respectiva en cuanto a reportes de actividades.

Manejo de Recursos para el Plan de SGSI	Para mantener un manejo eficaz del SGSI se requiere asignar o proveer los recursos necesarios para desarrollarlo de forma óptima. Cumplir con responsabilidad y conciencia las políticas y normativas de seguridad, controles en base a las normas ISO 27001 – 27002: 2022.
Revisión, Evaluación, Aprobación de Desarrollo del Plan de SGSI por el personal a cargo	El departamento y personal encargado recibirá la documentación que dé como resultado al desarrollo del SGSI.

Nota. Elaboración propia

2.16. Socialización y Capacitación

En la etapa de socialización es importante dar a conocer lo que conlleva la implementación de un SGSI en la empresa, comunicar su importancia y hacer conocer sus beneficios.

- Dar a conocer la importancia y los beneficios que trae a la empresa el implementar un SGSI para la seguridad de activos e información.
- Dar a conocer las actividades que se han designado a acatar en cuanto al SGSI se ha establecido para cada uno de los integrantes de la empresa.
- Detallar cada una de las normas de seguridad, políticas y planes de acción desarrollados para la empresa que se han destinado a la mitigación y control de riesgos.
- Mantenerse siempre informados acerca del SGSI promoviendo su práctica y la mejora continua.
- Tener manuales al alcance de los miembros de la organización para poder suplir dudas, ser aclaradas y continuar con las actividades.

Se realizó material de ayuda que servirá para socializar el contexto del SGSI en el Anexo 8 donde se busca cautivar la atención de las partes interesadas y los altos mandos de la empresa AIRMAXTELECOM Soluciones Tecnológicas S.A. se estima que la capacitación durará 1 hora.

Se facilita de igual forma el desarrollo de gestión de riesgos y Plan de Sistema de Gestión de Seguridad de la información (Archivo Excel).

La empresa debe utilizar medios por los cuales se evalúe la eficacia, eficiencia y nivel satisfactorio de las actividades referentes a la concientización. Las preguntas que se elaboraron en el Anexo 9 colaboraran como preguntas de sondeo para la empresa.

CAPÍTULO 3

Diseño de la Propuesta de un Sistema de Gestión de Seguridad de la Información

3.1. Consideraciones Generales

Después de realizar el proceso de levantamiento de activos, validando sus amenazas, vulnerabilidades y por consiguiente sugerir controles los cuales ayudarán a mantener una seguridad óptima para los activos de la información, en esta sección se desarrollará, la propuesta con la cual la empresa puede realizar su futura gestión de riesgos e implementación en cuanto a las normativas, controles, políticas y lineamientos ya aplicadas para la empresa.

Para ello se sugiere el paso a paso a seguir en cuanto a el proceso de gestión de riesgos y controles basados en las Normas ISO/IEC 27001 y 27002: 2022.

Como punto importante para el desarrollo e implementación de un SGSI en la empresa es necesario convencer a la alta gerencia de la efectividad en cuanto a la seguridad de la información, es el punto de partida en el cual se basa, si la alta gerencia no acepta o no tiene la iniciativa o el conocimiento de un SGSI y sus beneficios no se logrará implementar un sistema de seguridad en la empresa.

3.2. Metodología para Gestión de Riesgos

Como metodología para el levantamiento de activos se recomienda utilizar la metodología Magerit con la cual se desarrolló este proyecto, Magerit ayuda a la evaluación de los activos de forma específica de cada activo en la empresa, es importante resaltar que se debe estar al tanto de sus tres libros en los cuales da las normativas, lineamientos, preguntas que se debe hacer para valorar los activos en cuanto a los factores importantes que son: Disponibilidad, Integridad y Confidencialidad.

Como principal objetivo es el levantamiento de activos físicos y lógicos en la empresa para identificar a que amenazas pueden estar propensos y con ello evaluar y plantear las mejores opciones para mitigar, transferir o aceptar los riesgos, esta metodología aporta bases fundamentales que fortalecen el SGSI como se muestra en la Tabla 33:

Tabla 33 *Beneficios de implementar un SGSI en la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.*

Objetivos	Definición
Fortalecer	Ayuda a apalancarse de forma segura y capacitada en cuanto a la gestión de riesgos.

Determinar	Se establece procesos para identificar los riesgos y amenazas a los que se puede estar propensos los activos de la organización.
Colaborar	Identificar y determinar controles de riesgos en base a las normas de seguridad, llevando a los activos a un riesgo bajo
Mejora Continua	La empresa estará preparada en caso de ocurrir algún evento que comprometa la seguridad de la información, la mejora constante en el esquema de seguridad.

Nota: Elaboración Propia

3.3. Pilar

Pilar es una herramienta la cual se maneja con la metodología Magerit, es fácil de usar y amigable con el usuario, facilita el levantamiento de activos, la herramienta brinda las amenazas a las que puede estar propenso un activo, se establece por niveles, brinda gráficas y también recomienda los valores en los que debería estar un activo bajo la seguridad que se le establezca en base a las normativas y políticas con ello se puede establecer una gestión de riesgos efectiva.

3.4. Efectividad de la Gestión de Riesgos y SGSI en la empresa

Al momento en que se realizó el levantamiento de los activos en cuanto al riesgo potencial y el impacto se puede observar los valores críticos en ciertos casos en los que se encontraban los activos relacionados con la información, en esta etapa se encuentran en un porcentaje de 7,6 de 10 en nivel de riesgo, para ello se muestra en la Tabla 34.

Tabla 34 *Valores de riesgo sin aplicar y aplicando controles, políticas de seguridad en la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.*

	Sin Gestión de Riesgos	Con Gestión de Riesgos
Activos	**Peso Ponderado**	**Peso Ponderado**
Alexa	5	3
Apple Pencil	5	3
Case para Discos Duros	5	3
Extintores	5	3
Mostrador de vidrio	5	3
Parlantes	5	3
Sellos de Oficina	5	3
Casa Plus 1	6	4
Casa Plus 2	6	4
Copiadoras	6	4

Gerencia Atención al Cliente	6	4
Kit de Seguridad	6	3
Atención al cliente	7	5
Casilleros metálicos	7	5
Detectores de Humo	7	4
Gerencia Administrativa	7	5
Gerencia Comercial	7	5
Gerencia Operativa	7	5
Instalación internet	7	5
Rack	7	5
Etiquetadoras	8	3
Cooler AMD	8	3
Biométricos	8	6
Fusionadoras	8	3
Impresoras	8	3
Mouse	8	3
Ofimática	8	4
Teléfonos IP 2 cuentas	8	4
Video Card	8	3
Base de Datos	9	6
Cámaras Web	9	3
Celulares	9	5
Computadoras Portátiles	9	4
IPad Apple	9	5
Lectores de Huellas	9	4
MacBook Air	9	5
Monitores	9	3
OLT GPON	9	4
Server Dell	9	6
Tablet Lenovo	9	5
Unidades de Almacenamiento	9	5
CPUs	10	4
Datos de acceso	10	6
Generadores	10	6
Sistema Contable	10	6
Gerencia General	10	6

Nota: Elaboración Propia

Al realizar la gestión de riesgos de los activos conforme a la metodología y las Normas ISO/IEC 27001 y 27002: 2022, políticas de seguridad de la información, se logra reducir el riesgo y el impacto de los activos relacionados con la información estando en este punto con un valor de 4,3 de 10 en nivel de riesgo como se muestra en la Tabla 34.

Se puede observar un cambio notable al aplicar las normativas de seguridad en los activos de la empresa para hacer una comparativa se muestra en la Tabla 35 el valor que disminuye en cuanto al riesgo aplicando las normativas, lineamientos y buenas prácticas de seguridad de la información basadas en las Normas ISO/IEC 27001 y 27002:2022.

Tabla 35 *Valores de mejora aplicando normativas de seguridad en la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A*

Sin aplicar Gestión de Riesgos	Aplicando Gestión de Riesgos
7,6	4,2
Valor de mejora	3,3

Nota: Elaboración Propia

3.5. Diseño de un Sistema de Gestión de Seguridad de la Información

Para la gestión de riesgos de debe seguir la serie de pasos que se muestran en la Tabla 36.

Tabla 36 *Gestión de riesgos de activos para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.*

Definición	Contexto
Establecimiento del contexto	• Determine el alcance y los objetivos del plan de gestión de riesgos. • Determine las normas para evaluar el riesgo y la tolerancia al riesgo.
Identificación de activos	• Identificar y clasificar todos los activos de información de la organización, incluidos sistemas, datos, infraestructura y procesos.
Identificar los peligros y las vulnerabilidades	• Identificar las amenazas potenciales para los activos de información.
Análisis de riesgos	• Evaluar la probabilidad de que ocurran las amenazas identificadas y su impacto potencial en los activos de información.

	• Calcule el riesgo inherente de cada amenaza y vulnerabilidad.
Evaluación de riesgos	• Aplicar los controles existentes para determinar el nivel de riesgo residual. • Evaluar el riesgo residual en comparación con los estándares de tolerancia al riesgo establecidos anteriormente.
Tratamiento de riesgos	• Desarrolle métodos de tratamiento de riesgos que reduzcan, transfieran, eviten o acepten los riesgos. • Clasificar las medidas de tratamiento de riesgos en función de su eficacia y costo.
Políticas de Seguridad	• Establecer políticas de seguridad para los activos para mitigar los riesgos. • Actualizar las políticas de seguridad periódicamente cuando sea necesario.

Nota: ***Todo este procedimiento se puede realizar con la ayuda del Software Pilar y el documento de Excel de Gestión de Riesgos*** Elaboración Propia.

Para la implementación de controles se debe seguir la serie de pasos que se muestran en la Tabla 37.

Tabla 37 *Implementación de controles de seguridad en la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.*

Definición	Contexto
Implementación de controles	• Elegir e implementar los controles de seguridad de la información apropiados para reducir los riesgos.

	• Asegurarse de que los controles implementados sean efectivos y cumplan con las normas ISO 27001 y 27002.
Seguimiento y revisión	• Mantener un seguimiento continuo de los riesgos de seguridad de la información y de la eficacia de los controles implementados. • Realizar revisiones regulares del plan de gestión de riesgos para asegurarse de que sea relevante y actualizado.
Mejora continua	• Identificar oportunidades para mejorar los controles de seguridad de la información y la gestión de riesgos. • Implementar proactivamente medidas correctivas y preventivas para mejorar la seguridad de la información.

Nota: Elaboración Propia

Para la implementación del SGSI en la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A. se debe acudir a los siguientes pasos elaborados en base a las Normas de Seguridad ISO/IEC 27001 Y 27002: 2022 como se muestran en la Tabla 38.

Tabla 38 *Implementación del SGSI en la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.*

Implementación del Sistema de Gestión de seguridad de la Información	
Poner en práctica los controles que se definieron en la Norma ISO 27001 – 27002: 2022, conforme a las políticas de seguridad que se establecieron en el desarrollo del SGSI	Para garantizar que la puesta en práctica e implementación en cuanto a las políticas ya mencionadas anteriormente y en el documento que se las clasifica, es necesario que la empresa lo ejecute con responsabilidad para así evitar percances

	Como recomendación principal a la empresa, se incita a la revisión previa de la documentación, con la metodología de CheckList y análisis de activos, levantando activos y verificando amenazas, plan en caso de riesgos y como responder ante una situación vulnerable, controles y políticas de seguridad en aspectos físicos y lógicos de los activos.
Implementación de Controles	Como paso principal para empezar el SGSI se realizó el levantamiento de activos e información de la empresa AIRMAXTELECOM Soluciones Tecnológicas S.A. para valorar sus riesgos y amenazas y delimitar el tratamiento en caso de verse comprometido, con toda esta información se logra definir los controles del SGSI. Se recomienda detallar los controles que se va a utilizar para delimitar que recursos van a intervenir, logrando un desarrollo óptimo. Designar personal capacitado y encargado específicamente al área de seguridad de la información, delegando responsabilidades y actividades calendarizadas para consiguiente poner en prácticas los controles que se detallan en el documento.
Ejecución del Plan de Gestión de Incidentes	Es importante que el personal a cargo lleve registros de incidentes que se hayan suscitado en la empresa con la finalidad de reducir, controlar, transferir o eliminar los riesgos recurriendo a las políticas de seguridad. Designar responsables en la organización según la empresa crea conveniente con el conocimiento de habilidades de sus integrantes.

	Crear planes de contingencia ante posibles situaciones que comprometan a la empresa. Realizar la documentación respectiva en cuanto a reportes de actividades.
Manejo de Recursos para el Plan de SGSI	Para mantener un manejo eficaz del SGSI se requiere asignar o proveer los recursos necesarios para desarrollarlo de forma óptima.
	Cumplir con responsabilidad y conciencia las políticas y normativas de seguridad, controles en base a las normas ISO 27001 – 27002: 2022.
Revisión, Evaluación, Aprobación de Desarrollo del Plan de SGSI por el personal a cargo	El departamento y personal encargado recibirá la documentación que dé como resultado al desarrollo del SGSI.

Nota: Elaboración Propia

3.6. Cronograma de Desarrollo

Para cumplir con el desarrollo e implementación de este sistema se seguridad de la información se debe realizar la calendarización de actividades delegando responsables como se muestra en el documento de Políticas de Seguridad de Información sección Lineamientos en el apartado 2 y como paso primordial construir un comité de seguridad o departamento de seguridad de la información.

Se puede ayudar con herramientas para llevar un calendario estructurado tales como las que se muestran en la Tabla 39.

Tabla 39 *Herramientas para calendarizar actividades de gestión de riesgos*

Herramientas	Definición
Microsoft Excel	• Calendarios. • Plantillas. • Actividades de Gestión de Riesgos con fechas límites y recordatorios.
Google Calendar	• Crear y gestionar eventos.

	• Programar actividades con otros usuarios. • Asignar responsabilidades y recibir notificaciones.
Software de Gestión de Proyectos	• Microsoft Project. • Asana. • Trello. • Jira.
Software de Gestión de Riesgos	• RiskWare. • ARMATURE. • LogicManager.
Plantillas de Calendario	• Plantillas de calendario diseñadas en Word, Excel o PDF.

Nota: Elaboración Propia

3.7. Implementación y Evaluación

3.7.1. Implementación del Sistema

Se debe detallar como se llevará a cabo la implementación del sistema en todas sus etapas, tiempos, calendarios, responsables, presupuestos, configuraciones de herramientas, capacitación del personal en seguridad de la información y gestión de riesgos.

3.7.2. Evaluación de Sistema

Se debe evaluar el nivel de efectividad del sistema implementado a base de las normas de seguridad, políticas, rendimiento del sistema, gestión de riesgos con la ayuda de la matriz que fundamentado en la aplicación de controles y políticas puede dar el valor de riesgos, aplicar simulacros con los trabajadores de la organización.

3.8. Resultados

Se evalúa en base a todo el proceso realizado si se logró llegar o acercar a los resultados esperados teniendo conocimiento ya de las normas, políticas y procesos que se deben seguir a cabalidad

logrando alcanzar la seguridad esperada en la información de la organización con la ayuda del Sistema de Gestión de Seguridad de la Información.

Realizar los aportes y observaciones que en base a la experiencia y pruebas se haya recolectado para mantenerse en una mejora continua en los procesos y lineamientos de seguridad de la información, colaborar con los integrantes de la empresa con el conocimiento adquirido, capacitar, incentivar y promover la seguridad de la información dentro y fuera de la empresa.

CAPÍTULO 4

Validar la propuesta del Sistema de Gestión de Seguridad de la Información para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.

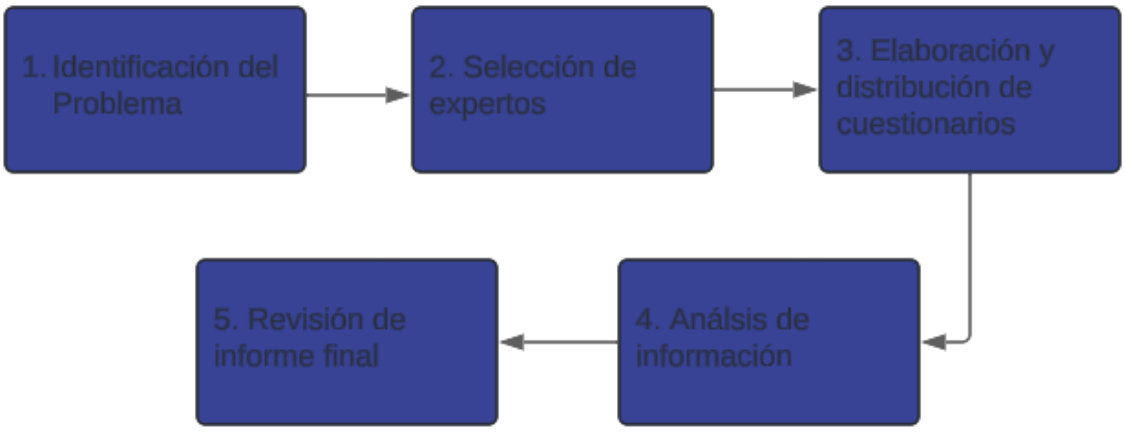
4.1. Evaluación de Desarrollo del Sistema de Gestión de Seguridad de la Información con el método Delphi.

Después de realizar el proceso de Diseñar un Sistema de Gestión de Seguridad de la Información, como parte fundamental y no menos importante es el validar la eficiencia y eficacia en cuanto a las normativas, lineamientos y políticas establecidas para la empresa, esta validación se apalanca en el método Delphi (por expertos). En la que se recibe apoyo de expertos en seguridad de la información y asegurando que el trabajo será útil para la seguridad de la empresa.

La metodología Delphi se contextualiza en la evaluación y consultoría con expertos en la que se analiza que llevará a conclusiones en común, los expertos responden las preguntas del cuestionario realizado sobre el trabajo realizado para llegar a los resultados esperados de eficiencia.

Para hacer uso del método de validación Delphi, se debe seguir los pasos mostrados en la Figura 27.

Figura 27 *Fases del método Delphi*



Nota: Elaboración Propia

4.1.1. Identificación del Problema

Como primer paso se realiza el análisis e identificación del problema o en su defecto el objetivo de estudio lo cual dicta el método Delphi, tiene como finalidad evaluar el desempeño y eficiencia del

Sistema de Gestión de Seguridad de la Información para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A. documentación realizada en base a la metodología Magerit sin dejar a un lado lo que dicta las Normas ISO/IEC 27001 y 27002: 2022 en cuestión del análisis y gestión de riesgos de la información.

4.1.2. Selección de expertos

Se realizar la selección del personal experto en el área de seguridad de la información para la validación, deben tener amplio conocimiento en las normas actuales, procesos y políticas de seguridad, la participación es voluntaria emitir los criterios.

4.1.3. Elaboración de cuestionarios

Al completar los objetivos para la investigación aplicada de seguridad de la información, se desarrolló un cuestionario que contiene 12 preguntas como se puede visualizar en el Anexo 10 enfocadas a las metodologías de desarrollo, las políticas de seguridad y observaciones que se deban tomar en cuenta en el Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27001 y 27002: 2022. Este cuestionario se encuentra disponible en el Anexo 10. El método de recolección de la información fue vía correo electrónico a cada uno de los expertos en Seguridad de la Información. El tiempo estimado para el envío y recepción de las respuestas por parte de los expertos fue de aproximadamente dos semanas debido a la revisión de los documentos complementarios, la misma que fue enviada a los expertos en formato de vinculo compartido del Sistema de Gestión de Seguridad de la Información, adjunto de igual forma un vínculo en la plataforma Microsoft Forms que contiene el cuestionario.

Las preguntas propuestas se pueden responder en base a la escala de Likert de 5 puntos, la pregunta 12 se encuentra estructurada en formato de opinión y recomendación, para mejor comprensión se detalla en la Tabla 40.

Tabla 40 *Ecala de Likert Cuestionario*

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

Nota: Elaboración Propia

4.1.4. Análisis de información

La siguiente información basada en metodologías investigativa, descriptiva, cualitativa y cuantitativa se someten a un análisis para comprender de mejor forma los resultados obtenidos.

Para obtener el valor o índice de validez de cada elemento se realiza con la fórmula que se muestra a continuación:

$$CIV = \frac{número\ de\ respuestas\ positivas}{número\ total\ de\ respuestas}$$

$$CIVTotal = \frac{número\ de\ respuestas\ positivas}{(número\ de\ expertos\ x\ número\ de\ items)}$$

En cuanto a la investigación aplicada que se revisó, en cuanto a valores de validez mediante la evaluación tomando en cuenta el factor de índice de validez de contenido (IVC). Para que cada ítem se encuentre en el rango de validez establecido debe ser igual o superior al 90%, cada proyecto debe tener un valor de CVI mayor o igual a un valor de 78%. Si los resultados obtenidos en esta investigación se encuentran referentes a los valores indicados, se considera que existe una igualdad, en caso de no estar dentro del rango establecido se puede realizar la admisión de recomendaciones o propuestas que ayuden a mejorar, fortalecer, inclusive eliminar ítems.

Como método de apoyo se acudió a las técnicas o métodos como:

Estadística Descriptiva: La cual se encarga de la recolección de información, organizándola como datos de manera informativa, utiliza como operaciones principales la media, la moda, la mediana, desviación estándar, gráficos o histogramas para el análisis más amigable de la información en un conjunto de datos.

Alfa de Cronbach: Este método se encarga de evaluar la efectividad de un conjunto de ítems de un cuestionario, en este caso la encuesta de validación, que tenga coherencia en las respuestas por parte de los expertos. Los valores del Alfa de Cronbach que se acercan a un valor de 1 son el indicador de fiabilidad, de lo contrario los valores bajo este nivel son valores atípicos que no concuerdan en este grupo. Los valores mínimos que se aceptan se encuentran en el rango de entre 0,70 7 0,90.

Para empezar con el análisis de efectividad de las 12 preguntas con las respuestas de los expertos se muestra los valores con los que se va a trabajar en la siguiente Tabla 41.

Tabla 41 *Cuestionario enviado a los expertos para validación*

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12
E1	1	2	2	2	2	3	1	2	2	2	1	Ninguno
E2	1	2	1	1	2	1	2	2	2	2	2	No tengo observaciones.
E3	1	2	1	2	1	1	1	1	2	2	2	Por cuestiones económicas, las empresas no disponen de recursos suficientes para contratar un Director de Seguridad de la Información.
E4	1	2	1	2	1	1	1	1	2	2	2	Ser más amigable en políticas de sanciones.

Nota: La tabla que se muestra son los datos que se tabularon en el cuestionario. Elaboración propia

Con fines didácticos para la evaluación enfocada a la validez del SGSI, se muestra en la Tabla 42 y en la Figura 28 una matriz la cual cuenta con el valor de las preguntas en su escala de Likert para una mejor comprensión.

Tabla 42 *Tabulación de respuestas equivalentes a los valores de sus preguntas*

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

Nota: TA: Totalmente de acuerdo, A: Acuerdo, N: Neutro, D: Desacuerdo, TD: Totalmente desacuerdo, P: Preguntas de cuestionario. Elaboración propia

Figura 28 *Respuestas por ítem del cuestionario de validación*

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

Después de realizar el cálculo de los Índices de Validez de acuerdo con las fórmulas mencionadas se puede visualizar en la Tabla 43.

Tabla 43 *Índice de Validez de Contenido*

	TD	D	N	A	TA	IVC ÍTEM
1: ¿Considera usted que es muy imprescindible el Diseño de un Sistema de Gestión de Seguridad de la Información con la ISO/27001 y 27002:2022 en el departamento de Tecnología de la Información de la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A?	-	-	-	-	100%	100%
2: ¿Cómo evalúa el Diseño de un Sistema de Gestión de Seguridad de la Información con la ISO/27001 y 27002:2022 para la	-	-	-	100%	-	100%

empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A., es un informe comprensible?						
3: ¿Está de acuerdo con la elección de la Metodología Magerit y la ISO/27001 y 27002:2022 para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.?	-	-	-	25%	75%	100%
4: ¿Considera usted que los procedimientos realizados en el Diseño de un Sistema de Gestión de Seguridad de la Información para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A., fueron los necesarios?	-	-	-	75%	25%	100%
5: ¿A su criterio el informe de Diseño de un Sistema de Gestión de Seguridad de la Información con la ISO/ 27001 y 27002:2022 para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A., Tiene la información necesaria?	-	-	-	75%	25%	100%
6: ¿Considera usted que la herramienta Pilar y la hoja de cálculo de Excel son eficientes para el desarrollo de un Sistema de Gestión de Seguridad de la información para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.?	-	-	25%		-	75%	100%
7: ¿En su opinión las tareas propuestas para el control y mitigación de riesgos en el desarrollo de un Sistema de Gestión de Seguridad de la	-	-	-	25%	75%	100%

información para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A., fueron adecuadas?						
8: ¿Considera usted que las políticas de seguridad para el Sistema de Gestión de Seguridad de la Información para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A. fueron las más adecuadas?	-	-	-	75%	25%	100%
9: ¿Considera usted que el número de políticas establecidas en el Sistema de Gestión de Seguridad de la Información para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A. son las óptimas para la empresa?	-	-	-	-	100%	100%
10: ¿Considera usted que las políticas de seguridad descritas para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A., cubren todos los aspectos de seguridad de la información?	-	-	-	-	100%	100%
11: ¿Considera usted que ha recibido suficiente información para seguir y entender las políticas de seguridad de la información para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.?	-	-	-	75%	25%	100%
					Total IVC	100%

Nota: TA: Totalmente de acuerdo, A: Acuerdo, N: Neutro, D: Desacuerdo, TD: Totalmente desacuerdo, IVC: índice de Validez de Contenido. Elaboración propia

En relación con las preguntas y respuestas analizadas para la validación se pudo alcanzar un Índice de Validez de Contenido (IVC) Valor Total de 90,10%. En mención a la literatura es un puntaje apropiado para la validez del cuestionario enviado a los expertos. En las preguntas con más alto grado de importancia o aceptación se encuentran en valores iguales o superiores a 75% realizando los cálculos con las respuestas de los expertos, se puede concluir que no se requieren ajustes ni declinar ítems.

Para evaluar la validez del cuestionario, se aplicó el método estadístico d fiabilidad conocido como el Alfa de Cronbach la cual se maneja con la siguiente fórmula:

$$\mathrm{a} = \frac{K}{K-1}\, x\, [1 - \frac{SVi}{Vt}]$$

En donde

α = Alfa de Cronbach

K = Número de ítems

Vi = Varianza de cada ítem

Vt = Varianza total

Los valores de varianza se muestran a detalle en la Tabla 44 y los cálculos del Alfa de Cronbach en la Tabla 45.

Tabla 44 *Varianza de ítems del cuestionario a expertos*

	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**	**P11**	**Sumatoria**
E1	1	2	2	2	2	3	1	2	2	2	1	20
E2	1	2	1	1	2	1	2	2	2	2	2	18
E3	1	2	1	2	1	1	1	1	2	2	2	16
E4	1	2	1	2	1	1	1	1	2	2	2	16
Varianza	0	0	0,25	0,08	0,17	0,50	0,08	0,17	0	0	0,25	70

Nota: P: Número de pregunta, E: Número de Experto. Elaboración propia

Tabla 45 *Alfa de Cronbach cuestionario expertos*

Variables	Valores
K	4
Suma Varianzas (Vi)	1,5
Varianza Total (Vt)	5,51
Cronbach	0,73

Nota: Elaboración propia

El resultado del Alfa de Cronbach nos muestra un valor de 0,73, un rango aceptable en cuanto a la validez del cuestionario enviado a los expertos. Según la literatura, los valores referenciales de excelencia están entre 0,72 y 0,99, lo que indica que el instrumento es confiable.

Para el ítem 12 referente a la pregunta abierta en cuanto a recomendaciones o posibles cambios que se puedan realizar en el Desarrollo de un Sistema de Gestión de Seguridad de la Información. Las sugerencias propuestas por los expertos se encuentran en la Tabla 46.

Tabla 46 *Comentarios de los expertos en la pregunta abierta del cuestionario.*

11: ¿Haría ajustes a algún elemento del Desarrollo de un Sistema de Gestión de Seguridad de la Información para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS SA.?	
Expertos	Respuestas
E1	Ninguno
E2	No tengo observaciones
E3	Por cuestiones económicas, las empresas no disponen de recursos suficientes para contratar un Director de Seguridad de la Información
E4	No tengo recomendaciones

Nota: E: número de expertos. Elaboración propia

En esta etapa de validación se obtiene la colaboración de 4 expertos, el experto 1 sugiere el factor económico dificulta la conformación del Comité de Seguridad o contratar un Director de Seguridad de la Información, los tres expertos restantes con sus comentarios elevan la eficacia del Plan de Gestión de Riesgos para la Seguridad de la Información.

Para sustentar de forma aceptable las observaciones del experto, se presenta una propuesta para mejorar el SGSI:

1. **Recursos suficientes para contratación de Director de Seguridad de la Información**: Para solventar esta problemática que por temas económicos no sea posible contratar a una persona que se enfoque solamente a Seguridad de la Información, se sugiere:
    - Certificar a cierta parte del personal que esté más empapada del tema.
    - Capacitar al personal en cuanto a Seguridad de la Información.
    - Hacer simulacros en cuanto a posibles casos de vulnerabilidad.
    - Realizar revisiones del Sistema de Gestión de Seguridad de la información.
    - Mantenerse actualizado en las políticas de Seguridad
    - Monitorear continuamente los procesos que se manejan en la empresa
    - Tener planes de contingencia ante posibles catástrofes.
    - Realizar ajustes necesarios en la empresa.
    - Colaborar con los integrantes de la empresa para la seguridad de los activos.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. La revisión en cuanto a la literatura y la bibliografía es un proceso fundamental en el cual se logra comprender y entender de mejor forma los procesos a realizar en cuanto a la seguridad de la información, en especial las Normas ISO y Metodología Magerit.
2. En la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A. debe implementar los controles, normas, lineamientos y políticas establecidos en el Sistema de Gestión de Seguridad de la Información para poder elevar la seguridad en su organización en aspectos físicos y lógicos, se logrará mitigar en su mayoría los peligros a los que pueda estar propensa la organización.
3. El uso de la metodología Magerit para la Gestión de Riesgos juega un papel muy importante en el desarrollo del SGSI en cuanto a la valoración e identificación de activos, vulnerabilidades y amenazas, genera un nivel de confianza tanto a los integrantes de la organización como a los clientes que utilizan sus servicios, fortalece la seguridad en la empresa de internet.
4. La puesta en marcha de las políticas de seguridad basado en las Normas ISO 27001 y 27002: 2022 garantizan un nivel de seguridad y confianza para la organización, depende del cumplimiento que le den los integrantes de la organización en sus áreas y roles que desempeñan.
5. En el análisis y validación del Sistema de Gestión de Seguridad de la Información con el Alfa de Cronbach, se obtuvo un resultado de 0,73, lo que se encuentra en un valor aceptable en cuanto a la literatura, los resultados obtenidos elevan la confiabilidad del instrumento.

Recomendaciones

1. Es importante realizar evaluaciones periódicamente de los activos de la empresa para mantenerse al tanto de la situación en que se encuentre la empresa, manejar la Gestión de Riesgos de forma adecuada con el personal especifico encargado de la seguridad de la información.
2. La utilidad de la metodología Magerit y la herramienta Pilar para la gestión de riesgos, son instrumentos que se deben utilizar en la empresa para mantener un esquema de seguridad de los activos, acompañado de las Normas ISO 27001, 27002 y 27005 que son normas en las cuales se basa la gestión de riesgos.
3. Se recomienda aplicar las actividades propuestas en la organización para lograr tener más seguridad en sus instalaciones y activos, mantener un estudio constante en cuando a la

Gestión de Riesgos y las normas de seguridad con sus actualizaciones, mantener al personal capacitado y preparado en caso de presentarse una situación que comprometa la seguridad de la información.

4. Se recomienda replicar este Sistema de Gestión de Seguridad de la Información y Gestión de Riesgos en las demás sucursales de la empresa alrededor del país, ampliando la seguridad de sus integrantes y clientes, delegar responsabilidades en cada área con el área encargada de la Seguridad de la Información.

5. Se recomienda conformar el Comité de Seguridad de la Información con prontitud en la empresa para lograr una mejor organización en cuanto a tareas, roles y responsables en diferentes áreas que maneja la empresa tanto en matriz como en las sucursales.

REFERENCIAS Y BIBLIOGRAFÍA

Aleksandrova, S. V., Vasiliev, V. A., & Aleksandrov, M. N. (2020). Problems of implementing information security management systems. *Proceedings of the 2020 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2020*, 78–81. https://doi.org/10.1109/ITQMIS51053.2020.9322896

Alvarado Claudia. (2021). *Sistema de gestión de seguridad de la información: qué es y sus etapas*. https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas

Auditool. (2023). *Los planes de respuesta efectivos a incidentes cibernéticos*. https://www.auditool.org/blog/auditoria-de-ti/los-planes-de-respuesta-efectivos-a-incidentes-ciberneticos

Aula Mentor. (2016). *Normas ISO sobre gestión de seguridad de la información | Seguridad Informática*. http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html

CIBERSEGURIDAD. (2020). *Política de seguridad de la información: definición, elementos y mejores prácticas*. https://ciberseguridad.com/herramientas/politica-seguridad-informacion/

CISCO. (2023a). *¿Qué es el monitoreo de red? - Cisco*. https://www.cisco.com/c/es_mx/solutions/automation/what-is-network-monitoring.html#~recursos

CISCO. (2023b). *¿Qué es una VPN? - Red privada virtual - Cisco*. https://www.cisco.com/c/es_mx/products/security/vpn-endpoint-security-clients/what-is-vpn.html

David Castañeda Echeverri, J., & Adolfo Villegas Villegas, G. (2020). *Recomendaciones y Estrategias para la Protección de Datos en la Recommendations and Strategies for Data Protection in the Cloud*.

DIRECTRICES DE SEGURIDAD DE LA INFORMACIÓN. (2018). *DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS CAMINOS Y PUENTES FEDERALES DE*

INGRESOS Y SERVICIOS CONEXOS DIRECTRICES DE SEGURIDAD DE LA INFORMACIÓN SUBDIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN.

En, D., De, G., & Bogotá, C. (2014). *Contador Público UNIVERSIDAD MILITAR NUEVA GRANADA FACULTAD DE ESTUDIOS A DISTANCIA (FAEDIS) PROGRAMA DE CONTADURIA PÚBLICA*.

Force, J. T. (2020). *Security and Privacy Controls for Information Systems and Organizations*. https://doi.org/10.6028/NIST.SP.800-53R5

Guerrero, Y. (2014). *Information security risk management models for cloud hosted systems*. 49.

IBM. (2023). *¿Qué es la respuesta a incidentes? | IBM*. https://www.ibm.com/es-es/topics/incident-response

ICS. (2019). *Principales cambios ISO/IEC 27002:2022 - ICS-Perú*. https://www.ics-peru.com/principales-cambios-iso-27002/

Innova Busines School. (2022). *Tipos de malware: Cómo eliminarlos y prevenir amenazas | Proofpoint ES*. https://www.proofpoint.com/es/corporate-blog/post/how-get-rid-malware-and-keep-it-out

Irsheid, A., Murad, A., Alnajdawi, M., & Qusef, A. (2022). Information security risk management models for cloud hosted systems: A comparative study. *Procedia Computer Science*, *204*, 205–217. https://doi.org/10.1016/J.PROCS.2022.08.025

ISO 27001. (2021). *Implementar ISO 27001 Paso a Paso- 5 ¿Que Documentar y por qué?* https://normaiso27001.es/fase-5-documentacion-del-sgsi/

ISO/IEC. (2022). *ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls*. https://www.iso.org/standard/75652.html

Lopez, T. (2023). *SGSI: Qué es y Cómo Implementarlo*. https://blog.innevo.com/que-es-sgsi

Manejo de información. (2022). *Manejo de la información: Seguridad y almacenamiento*. https://ori.hhs.gov/education/products/sdsu/espanol/sec_sto.htm

NIST. (2023). *Cybersecurity | NIST*. https://www.nist.gov/cybersecurity

Normas ISO. (2005). *ISO 27001 - Seguridad de la información: norma ISO IEC 27001/27002*. https://www.normas-iso.com/iso-27001/

OYARZÚN G. (2023). *SGSI: por qué debes implementarlo en tu empresa y cómo hacerlo*. https://ciberseguridadtips.com/sgsi-por-que-implementarlo-en-empresas/

Perez Ramiro. (2023). *LA EMPRESA: CONCEPTO, ELEMENTOS, FUNCIONES Y CLASES*.

Poomas Das. (2022). *Key Performance Indicators (KPIs) for Employee Performance: 10 Tools to Identify and Track the Right Metrics*. https://blog.empuls.io/es/employee-award-titles/

Revista IMG. (2023). *¿Qué importancia tiene la Gestión de Activos para las empresas industriales?* https://www.revistaimg.com/que-importancia-tiene-la-gestion-de-activos-para-las-empresas-industriales/

Rocha Alex. (2021). *Diferencia entre Autenticación y Autorización*. https://es.linkedin.com/pulse/diferencia-entre-autenticaci%C3%B3n-y-autorizaci%C3%B3n-alex-rocha

Rodriguez Johanna. (2022). *Manual de procedimientos: qué es y cómo hacer uno (con ejemplos)*. https://blog.hubspot.es/sales/manual-de-procedimientos-empresa

S Blog. (2022). *Respaldo y recuperación de base de datos*. https://serman.com/blog-recuperacion-datos/respaldo-y-recuperacion-de-base-de-datos/

Schwaker Eric. (2019). *Tipos de malware: Cómo eliminarlos y prevenir amenazas | Proofpoint ES*. https://www.proofpoint.com/es/corporate-blog/post/how-get-rid-malware-and-keep-it-out

Seguridad de personas y bienes. (2017). *Seguridad de personas y bienes Manual de Políticas Procesos y Procedimientos Código del Proceso*.

Software Engineering Institute. (2023). *The CERT Division | Software Engineering Institute*. https://www.sei.cmu.edu/about/divisions/cert/index.cfm

Suárez Mirella Bernal. (2023). *La importancia del Principio de Información y Capacitación ante el COVID-19 – Laboral y SST En Línea*. https://mirellabernal.com/2020/04/28/la-importancia-del-principio-de-informacion-y-capacitacion-ante-el-covid-19/

Team Asana. (2022). *Matriz de riesgos: cómo evaluar los riesgos para lograr el éxito del proyecto [2022] • Asana*. https://asana.com/es/resources/risk-matrix-template

Anexos

Anexo 1 Codificación según el tipo de activos

Tipo de Activo	Activo	Código	D	I	C	Peso ponderado	Valor
Datos/ Información	Base de Datos	D0001	10	10	10	10	Extremo
	Datos de Acceso	D0002	10	10	10	10	Extremo
	Detectores de Humo	D0003	10	9	1	7	Alto
	Kit de seguridad	D0004	9	8	2	6	Alto
Servicios	Electricidad	S0001	7	7	7	7	Alto
	Internet	S0002	8	8	8	8	Alto
	Mantenimiento	S0003	7	7	7	7	Alto
	Correo	S0004	8	8	8	8	Alto
Software	Sistema Contable	SW0001	9	10	9	9	Muy alto
	Antivirus	SW0002	10	10	9	9	Muy alto
Hardware	Fusionadoras	HW0001	9	5	2	5	Medio
	Cargadores	HW0002	8	5	2	7	Alto
	Power Meter	HW0003	9	5	2	5	Medio
	Sacabocados	HW0004	5	4	1	3	Medio
	Taladros	HW0005	5	4	1	3	Medio
	Etiquetadoras	HW0006	8	8	2	6	Alto
	Cámaras Web	HW0007	9	8	6	8	Alto
	Portátiles	HW0008	9	8	8	8	Alto
	Cooler AMD	HW0009	8	9	1	6	Alto
	CPU	HW00010	10	10	1	7	Alto
	Video Card	HW0011	9	9	2	7	Alto
	Impresoras	HW0012	5	5	0	3	Medio
	IPad Apple	HW0013	9	9	7	8	Alto
	MacBook Air	HW0014	8	9	8	8	Alto
	Monitores	HW0015	8	9	8	8	Alto
	Mouse	HW0016	8	9	1	8	Alto
	Servidor Dell	HW0017	10	10	9	9	Muy alto

	Tablet Lenovo	HW0018	9	10	7	9	Muy alto
	Teclados	HW0019	8	9	1	6	Alto
	TV	HW0020	7	8	5	7	Alto
	Amplificadores	HW0021	8	9	3	7	Alto
	Aspiradoras	HW0022	9	2	1	4	Medio
	Lectores de huellas	HW0023	8	9	7	8	Alto
	Biométricos	HW0024	8	9	7	8	Alto
	Celulares	HW0025	8	9	5	7	Alto
	Micrófonos	HW0026	9	8	5	7	Alto
	Televisores	HW0027	7	8	5	6	Alto
	Alcancel	HW0028	8	9	1	6	Alto
	Estanterías	HW0029	9	8	8	8	Alto
	Rótulos	HW0030	9	8	2	6	Alto
	Rack	HW0031	9	9	7	8	Alto
	Implementos instalación internet	HW0032	9	8	5	7	Alto
	OLT Gpon	HW0033	8	9	7	8	Alto
	Unidades de almacenamiento	HW0034	9	9	8	9	Muy alto
	Ofimática	HW0035	10	9	8	6	Alto
Comunicaciones	Teléfonos IP 2 cuentas	COM00001	8	8	2	5	Alto
	Escaleras	AUX0001	8	7	1	8	Alto
	Generadores	AUX0002	9	9	7	6	Alto
	Sillas	AUX0003	8	8	1	6	Alto
	Balanza	AUX0004	8	9	2	7	Alto
	Camilla	AUX0005	8	9	3	7	Alto
	Linternas	AUX0006	9	8	1	6	Alto
Auxiliares	Grapadoras	AUX0007	5	4	1	3	Medio
	Perforadoras	AUX0008	5	4	1	3	Medio
	Recogedores	AUX0009	9	2	1	4	Medio
	Regletas	AUX0010	5	2	1	3	Medio
	Pizarrones	AUX0011	5	5	1	4	Medio
	Sellos de oficina	AUX0012	9	8	3	7	Alto

	Microondas	AUX0013	8	0	0	3	Medio
	Minicomponentes	AUX0014	7	5	1	4	Medio
	Lector de barras	AUX0015	9	9	4	7	Alto
	Dispensador de agua	AUX0016	5	4	1	3	Medio
	Mostradores de vidrio	AUX0017	8	9	3	7	Alto
	Parlantes	AUX0018	9	8	2	6	Alto
	Copiadoras	AUX0019	9	8	6	8	Alto
	Extintores	AUX0020	10	10	1	7	Alto
	Casilleros metálicos	AUX0021	8	9	7	8	Alto
	Data Fast	AUX0022	7	8	6	7	Alto
	Arnés reforzado	AUX0023	9	9	1	6	Alto
	Cascos	AUX0024	8	7	3	6	Alto
	Cinturones	AUX0025	8	7	3	6	Alto
	Eslinga de posicionamiento	AUX0026	8	7	2	6	Alto
	Gafas	AUX0027	8	7	1	5	Medio
	Guantes	AUX0028	8	7	1	3	Medio
	Mosquetón	AUX0029	5	5	1	3	Medio
	Chalecos	AUX0030	7	7	1	5	Medio
	Conos de seguridad	AUX0031	5	5	1	7	Alto
	Letreros de advertencia	AUX0032	9	9	2	7	Alto
	Herramientas	AUX0033	10	9	1	7	Alto
	Case para discos duros	AUX0034	9	9	4	7	Alto
	Apple pencil	AUX0035	8	9	3	7	Alto
	Alexa	AUX0036	8	9	3	7	Alto
	Casa Plus 1	L0001	10	10	1	7	Alto
Instalaciones	Casa Plus 2	L0002	10	10	1	7	Alto
	Atención al Cliente	L0003	10	10	1	7	Alto
	Gerencia	P0001	5	5	5	5	Medio
Personal	Operacional						
	Gerencia Operativa	P0002	10	10	10	10	Extremo

	Gerencia Administrativa	P0003	5	5	5	4	Medio
	Gerencia Atención al Cliente	P0004	4	4	4	4	Medio
	Gerencia Comercial	P0005	5	5	5	5	Medio

Anexo 2 Activos y sus amenazas

Activo	Amenaza
	Datos/Información
Base de Datos	[1.5.11 Avería de origen lógico
Base de Datos	[E.8] Difusión de software dañino
Base de Datos	[E.15] Alteración de la información
Base de Datos	[E,20] Vulnerabilidades de los programas (software)
Base de Datos	[E.21] Errores de mantenimiento / actualización (software)
Base de Datos	[A.8] Difusión de software dañino
Base de Datos	[A.22] Manipulación de programas
Base de Datos	[1.5.11 Avería de origen lógico
Base de Datos	[E.8] Difusión de software dañino
Base de Datos	[E.20] Vulnerabilidades de los programas (software)
Base de Datos	[E.21] Errores de mantenimiento / actualización (software)
Base de Datos	[A.8] Difusión de software dañino
Base de Datos	[A.221] Manipulación de programas
	Servicios
Electricidad	[E.2] Errores del administrador del sistema / de la seguridad
Electricidad	[E.15] Alteración de la información
Electricidad	[E.19] Fugas de información
Electricidad	[A.5] Suplantación de la identidad
Electricidad	[A.6] Abuso de privilegios de acceso
Electricidad	[A.7] Uso no previsto
Electricidad	[A.11] Acceso no autorizado
Electricidad	[A.15] Modificación de la información
Internet	[E.1] Errores de los usuarios
Internet	[E.2] Errores del administrador del sistema / de la seguridad
Internet	[E.15] Alteración de la información
Internet	[E.19] Fugas de información
Internet	[A.5] Suplantación de la identidad
Internet	[A.6] Abuso de privilegios de acceso

Internet	[A.7] Uso no previsto
Internet	[A.11] Acceso no autorizado
Internet	[A.15] Modificación de la información
Mantenimiento	[E.1] Errores de los usuarios
Mantenimiento	[E.2] Errores del administrador del sistema / de la seguridad
Mantenimiento	[E.15] Alteración de la información
Mantenimiento	[E.19] Fugas de información
Mantenimiento	[A.5] Suplantación de la identidad
Mantenimiento	[A.6] Abuso de privilegios de acceso
Mantenimiento	[A.7] Uso no previsto
Mantenimiento	[A.11] Acceso no autorizado
Mantenimiento	[A.15] Modificación de la información
Correo	[E.1] Errores de los usuarios
Correo	[E.2] Errores del administrador del sistema / de la seguridad
Correo	[E.15] Alteración de la información
Correo	[E.19] Fugas de información
Correo	[A.5] Suplantación de la identidad
Correo	[A.6] Abuso de privilegios de acceso
Correo	[A.7] Uso no previsto
Correo	[A.11] Acceso no autorizado
Correo	[A.15] Modificación de la información
Datos de ingreso	[1.5.1] Avería de origen lógico
Datos de ingreso	[E.8] Difusión de software dañino
Datos de ingreso	[E.20] Vulnerabilidades de los programas (software)
Datos de ingreso	[E.21] Errores de mantenimiento / actualización (software)
Datos de ingreso	[A.8] Difusión de software dañino
Datos de ingreso	[A.221] Manipulación de programas
Detectores de humo	[1.3] Contaminación medioambiental
Kits de seguridad	[N] Desastres naturales
Kits de seguridad	[N.1] Fuego
Kits de seguridad	[A.26] Ataque destructivo
Sistema contable	[1.5.1] Avería de origen lógico
Sistema contable	[E.8] Difusión de software dañino
Sistema contable	[E.20] Vulnerabilidades de los programas (software)
Sistema contable	[E.21] Errores de mantenimiento / actualización (software)
Sistema contable	[A.8] Difusión de software dañino

Sistema contable	[A.221] Manipulación de programas
Antivirus	[1.5.1] Avería de origen lógico
Antivirus	[E.8] Difusión de software dañino
Antivirus	[E.20] Vulnerabilidades de los programas (software)
Antivirus	[E.21] Errores de mantenimiento / actualización (software)
Antivirus	[A.8] Difusión de software dañino
Antivirus	[A.221] Manipulación de programas
Fusionadoras	[N.1] Fuego
Fusionadoras	[N.2] Daños por agua
Fusionadoras	[N] Desastres naturales
Fusionadoras	[I.*] Desastres industriales
Fusionadoras	[1.3] Contaminación medioambiental
Fusionadoras	[I.4] Contaminación electromagnética
Fusionadoras	[1.5.2] Avería de origen físico
Fusionadoras	[I.6] Corte del suministro eléctrico
Fusionadoras	[I.7] Condiciones inadecuadas de temperatura o humedad
Fusionadoras	[I.11] Emanaciones electromagnéticas (TEMPEST)
Fusionadoras	[E.23] Errores de mantenimiento / actualización de equipos
Fusionadoras	[E.25] Perdida de equipos
Fusionadoras	[A.11] Acceso no autorizado
Fusionadoras	[A.23] Manipulación de hardware
Fusionadoras	[A.24] Denegación de servicio
Fusionadoras	[A.25] Robo de equipos
Fusionadoras	[A.26] Ataque destructivo
Cargadores	[N.1] Fuego
Cargadores	[N.2] Daños por agua
Cargadores	[N] Desastres naturales
Cargadores	[I.*] Desastres industriales
Cargadores	[1.3] Contaminación medioambiental
Cargadores	[I.4] Contaminación electromagnética
Cargadores	[1.5.2] Avería de origen físico
Cargadores	[I.6] Corte del suministro eléctrico
Cargadores	[I.7] Condiciones inadecuadas de temperatura o humedad
Cargadores	[I.11] Emanaciones electromagnéticas (TEMPEST)
Cargadores	[E.23] Errores de mantenimiento / actualización de equipos
Cargadores	[E.25] Perdida de equipos
Cargadores	[A.11] Acceso no autorizado
Cargadores	[A.23] Manipulación de hardware
Cargadores	[A.24] Denegación de servicio
Cargadores	[A.25] Robo de equipos
Cargadores	[A.26] Ataque destructivo
Power Meter	[N.1] Fuego
Power Meter	[N.2] Daños por agua

Power Meter	[N] Desastres naturales
Power Meter	[I.*] Desastres industriales
Power Meter	[1.3] Contaminación medioambiental
Power Meter	[I.4] Contaminación electromagnética
Power Meter	[1.5.2] Avería de origen físico
Power Meter	[I.6] Corte del suministro eléctrico
Power Meter	[I.7] Condiciones inadecuadas de temperatura o humedad
Power Meter	[I.11] Emanaciones electromagnéticas (TEMPEST)
Power Meter	[E.23] Errores de mantenimiento / actualización de equipos
Power Meter	[E.25] Perdida de equipos
Power Meter	[A.11] Acceso no autorizado
Power Meter	[A.23] Manipulación de hardware
Power Meter	[A.24] Denegación de servicio
Power Meter	[A.25] Robo de equipos
Power Meter	[A.26] Ataque destructivo
Sacabocados	[N.1] Fuego
Sacabocados	[N.2] Daños por agua
Sacabocados	[N] Desastres naturales
Sacabocados	[I.*] Desastres industriales
Sacabocados	[1.3] Contaminación medioambiental
Sacabocados	[I.4] Contaminación electromagnética
Sacabocados	[1.5.2] Avería de origen físico
Sacabocados	[I.6] Corte del suministro eléctrico
Sacabocados	[I.7] Condiciones inadecuadas de temperatura o humedad
Sacabocados	[I.11] Emanaciones electromagnéticas (TEMPEST)
Sacabocados	[E.23] Errores de mantenimiento / actualización de equipos
Sacabocados	[E.25] Perdida de equipos
Sacabocados	[A.11] Acceso no autorizado
Sacabocados	[A.23] Manipulación de hardware
Sacabocados	[A.24] Denegación de servicio
Sacabocados	[A.25] Robo de equipos
Sacabocados	[A.26] Ataque destructivo
Taladros	[N.1] Fuego
Taladros	[N.2] Daños por agua
Taladros	[N] Desastres naturales
Taladros	[I.*] Desastres industriales
Taladros	[1.3] Contaminación medioambiental
Taladros	[I.4] Contaminación electromagnética
Taladros	[1.5.2] Avería de origen físico
Taladros	[I.6] Corte del suministro eléctrico
Taladros	[I.7] Condiciones inadecuadas de temperatura o humedad
Taladros	[I.11] Emanaciones electromagnéticas (TEMPEST)
Taladros	[E.23] Errores de mantenimiento / actualización de equipos

Taladros	[E.25] Perdida de equipos
Taladros	[A.11] Acceso no autorizado
Taladros	[A.23] Manipulación de hardware
Taladros	[A.24] Denegación de servicio
Taladros	[A.25] Robo de equipos
Taladros	[A.26] Ataque destructivo
Etiquetadoras	[N.1] Fuego
Etiquetadoras	[N.2] Daños por agua
Etiquetadoras	[N] Desastres naturales
Etiquetadoras	[I.*] Desastres industriales
Etiquetadoras	[1.3] Contaminación medioambiental
Etiquetadoras	[I.4] Contaminación electromagnética
Etiquetadoras	[1.5.2] Avería de origen físico
Etiquetadoras	[I.6] Corte del suministro eléctrico
Etiquetadoras	[I.7] Condiciones inadecuadas de temperatura o humedad
Etiquetadoras	[I.11] Emanaciones electromagnéticas (TEMPEST)
Etiquetadoras	[E.23] Errores de mantenimiento / actualización de equipos
Etiquetadoras	[E.25] Perdida de equipos
Etiquetadoras	[A.11] Acceso no autorizado
Etiquetadoras	[A.23] Manipulación de hardware
Etiquetadoras	[A.24] Denegación de servicio
Etiquetadoras	[A.25] Robo de equipos
Etiquetadoras	[A.26] Ataque destructivo
Cámaras Web	[N.1] Fuego
Cámaras Web	[N.2] Daños por agua
Cámaras Web	[N] Desastres naturales
Cámaras Web	[I.*] Desastres industriales
Cámaras Web	[1.3] Contaminación medioambiental
Cámaras Web	[I.4] Contaminación electromagnética
Cámaras Web	[1.5.2] Avería de origen físico
Cámaras Web	[I.6] Corte del suministro eléctrico
Cámaras Web	[I.7] Condiciones inadecuadas de temperatura o humedad
Cámaras Web	[I.11] Emanaciones electromagnéticas (TEMPEST)
Cámaras Web	[E.23] Errores de mantenimiento / actualización de equipos
Cámaras Web	[E.25] Perdida de equipos
Cámaras Web	[A.11] Acceso no autorizado
Cámaras Web	[A.23] Manipulación de hardware
Cámaras Web	[A.24] Denegación de servicio
Cámaras Web	[A.25] Robo de equipos
Cámaras Web	[A.26] Ataque destructivo
Cooler AMD	[N.1] Fuego
Cooler AMD	[N.2] Daños por agua
Cooler AMD	[N] Desastres naturales

Cooler AMD	[I.*] Desastres industriales
Cooler AMD	[1.3] Contaminación medioambiental
Cooler AMD	[I.4] Contaminación electromagnética
Cooler AMD	[1.5.2] Avería de origen físico
Cooler AMD	[I.6] Corte del suministro eléctrico
Cooler AMD	[I.7] Condiciones inadecuadas de temperatura o humedad
Cooler AMD	[I.11] Emanaciones electromagnéticas (TEMPEST)
Cooler AMD	[E.23] Errores de mantenimiento / actualización de equipos
Cooler AMD	[E.25] Perdida de equipos
Cooler AMD	[A.11] Acceso no autorizado
Cooler AMD	[A.23] Manipulación de hardware
Cooler AMD	[A.24] Denegación de servicio
Cooler AMD	[A.25] Robo de equipos
Cooler AMD	[A.26] Ataque destructivo
CPU	[N.1] Fuego
CPU	[N.2] Daños por agua
CPU	[N] Desastres naturales
CPU	[I.*] Desastres industriales
CPU	[1.3] Contaminación medioambiental
CPU	[I.4] Contaminación electromagnética
CPU	[1.5.2] Avería de origen físico
CPU	[I.6] Corte del suministro eléctrico
CPU	[I.7] Condiciones inadecuadas de temperatura o humedad
CPU	[I.11] Emanaciones electromagnéticas (TEMPEST)
CPU	[E.23] Errores de mantenimiento / actualización de equipos
CPU	[E.25] Perdida de equipos
CPU	[A.11] Acceso no autorizado
CPU	[A.23] Manipulación de hardware
CPU	[A.24] Denegación de servicio
CPU	[A.25] Robo de equipos
CPU	[A.26] Ataque destructivo
Video Card	[N.1] Fuego
Video Card	[N.2] Daños por agua
Video Card	[N] Desastres naturales
Video Card	[I.*] Desastres industriales
Video Card	[1.3] Contaminación medioambiental
Video Card	[I.4] Contaminación electromagnética
Video Card	[1.5.2] Avería de origen físico
Video Card	[I.6] Corte del suministro eléctrico
Video Card	[I.7] Condiciones inadecuadas de temperatura o humedad
Video Card	[I.11] Emanaciones electromagnéticas (TEMPEST)
Video Card	[E.23] Errores de mantenimiento / actualización de equipos
Video Card	[E.25] Perdida de equipos

Video Card	[A.11] Acceso no autorizado
Video Card	[A.23] Manipulación de hardware
Video Card	[A.24] Denegación de servicio
Video Card	[A.25] Robo de equipos
Video Card	[A.26] Ataque destructivo
Impresoras	[N.1] Fuego
Impresoras	[N.2] Daños por agua
Impresoras	[N] Desastres naturales
Impresoras	[I.*] Desastres industriales
Impresoras	[1.3] Contaminación medioambiental
Impresoras	[I.4] Contaminación electromagnética
Impresoras	[1.5.2] Avería de origen físico
Impresoras	[I.6] Corte del suministro eléctrico
Impresoras	[I.7] Condiciones inadecuadas de temperatura o humedad
Impresoras	[I.11] Emanaciones electromagnéticas (TEMPEST)
Impresoras	[E.23] Errores de mantenimiento / actualización de equipos
Impresoras	[E.25] Perdida de equipos
Impresoras	[A.11] Acceso no autorizado
Impresoras	[A.23] Manipulación de hardware
Impresoras	[A.24] Denegación de servicio
Impresoras	[A.25] Robo de equipos
Impresoras	[A.26] Ataque destructivo
iPads Apple	[N.1] Fuego
iPads Apple	[N.2] Daños por agua
iPads Apple	[N] Desastres naturales
iPads Apple	[I.*] Desastres industriales
iPads Apple	[1.3] Contaminación medioambiental
iPads Apple	[I.4] Contaminación electromagnética
iPads Apple	[1.5.2] Avería de origen físico
iPads Apple	[I.6] Corte del suministro eléctrico
iPads Apple	[I.7] Condiciones inadecuadas de temperatura o humedad
iPads Apple	[I.11] Emanaciones electromagnéticas (TEMPEST)
iPads Apple	[E.23] Errores de mantenimiento / actualización de equipos
iPads Apple	[E.25] Perdida de equipos
iPads Apple	[A.11] Acceso no autorizado
iPads Apple	[A.23] Manipulación de hardware
iPads Apple	[A.24] Denegación de servicio
iPads Apple	[A.25] Robo de equipos
iPads Apple	[A.26] Ataque destructivo
MacBook Air	[N.1] Fuego
MacBook Air	[N.2] Daños por agua
MacBook Air	[N] Desastres naturales
MacBook Air	[I.*] Desastres industriales

MacBook Air	[1.3] Contaminación medioambiental
MacBook Air	[I.4] Contaminación electromagnética
MacBook Air	[1.5.2] Avería de origen físico
MacBook Air	[I.6] Corte del suministro eléctrico
MacBook Air	[I.7] Condiciones inadecuadas de temperatura o humedad
MacBook Air	[I.11] Emanaciones electromagnéticas (TEMPEST)
MacBook Air	[E.23] Errores de mantenimiento / actualización de equipos
MacBook Air	[E.25] Perdida de equipos
MacBook Air	[A.11] Acceso no autorizado
MacBook Air	[A.23] Manipulación de hardware
MacBook Air	[A.24] Denegación de servicio
MacBook Air	[A.25] Robo de equipos
MacBook Air	[A.26] Ataque destructivo
Monitores	[N.1] Fuego
Monitores	[N.2] Daños por agua
Monitores	[N] Desastres naturales
Monitores	[I.*] Desastres industriales
Monitores	[1.3] Contaminación medioambiental
Monitores	[I.4] Contaminación electromagnética
Monitores	[1.5.2] Avería de origen físico
Monitores	[I.6] Corte del suministro eléctrico
Monitores	[I.7] Condiciones inadecuadas de temperatura o humedad
Monitores	[I.11] Emanaciones electromagnéticas (TEMPEST)
Monitores	[E.23] Errores de mantenimiento / actualización de equipos
Monitores	[E.25] Perdida de equipos
Monitores	[A.11] Acceso no autorizado
Monitores	[A.23] Manipulación de hardware
Monitores	[A.24] Denegación de servicio
Monitores	[A.25] Robo de equipos
Monitores	[A.26] Ataque destructivo
Mouse	[N.1] Fuego
Mouse	[N.2] Daños por agua
Mouse	[N] Desastres naturales
Mouse	[I.*] Desastres industriales
Mouse	[1.3] Contaminación medioambiental
Mouse	[I.4] Contaminación electromagnética
Mouse	[1.5.2] Avería de origen físico
Mouse	[I.6] Corte del suministro eléctrico
Mouse	[I.7] Condiciones inadecuadas de temperatura o humedad
Mouse	[I.11] Emanaciones electromagnéticas (TEMPEST)
Mouse	[E.23] Errores de mantenimiento / actualización de equipos
Mouse	[E.25] Perdida de equipos
Mouse	[A.11] Acceso no autorizado

Mouse	[A.23] Manipulación de hardware
Mouse	[A.24] Denegación de servicio
Mouse	[A.25] Robo de equipos
Mouse	[A.26] Ataque destructivo
Server Dell	[N.1] Fuego
Server Dell	[N.2] Daños por agua
Server Dell	[N] Desastres naturales
Server Dell	[I.*] Desastres industriales
Server Dell	[1.3] Contaminación medioambiental
Server Dell	[I.4] Contaminación electromagnética
Server Dell	[1.5.2] Avería de origen físico
Server Dell	[I.6] Corte del suministro eléctrico
Server Dell	[I.7] Condiciones inadecuadas de temperatura o humedad
Server Dell	[I.11] Emanaciones electromagnéticas (TEMPEST)
Server Dell	[E.23] Errores de mantenimiento / actualización de equipos
Server Dell	[E.25] Perdida de equipos
Server Dell	[A.11] Acceso no autorizado
Server Dell	[A.23] Manipulación de hardware
Server Dell	[A.24] Denegación de servicio
Server Dell	[A.25] Robo de equipos
Server Dell	[A.26] Ataque destructivo
Tablet Lenovo	[N.1] Fuego
Tablet Lenovo	[N.2] Daños por agua
Tablet Lenovo	[N] Desastres naturales
Tablet Lenovo	[I.*] Desastres industriales
Tablet Lenovo	[1.3] Contaminación medioambiental
Tablet Lenovo	[I.4] Contaminación electromagnética
Tablet Lenovo	[1.5.2] Avería de origen físico
Tablet Lenovo	[I.6] Corte del suministro eléctrico
Tablet Lenovo	[I.7] Condiciones inadecuadas de temperatura o humedad
Tablet Lenovo	[I.11] Emanaciones electromagnéticas (TEMPEST)
Tablet Lenovo	[E.23] Errores de mantenimiento / actualización de equipos
Tablet Lenovo	[E.25] Perdida de equipos
Tablet Lenovo	[A.11] Acceso no autorizado
Tablet Lenovo	[A.23] Manipulación de hardware
Tablet Lenovo	[A.24] Denegación de servicio
Tablet Lenovo	[A.25] Robo de equipos
Tablet Lenovo	[A.26] Ataque destructivo
Teclados	[N.1] Fuego
Teclados	[N.2] Daños por agua
Teclados	[N] Desastres naturales
Teclados	[I.*] Desastres industriales
Teclados	[1.3] Contaminación medioambiental

Teclados	[I.4] Contaminación electromagnética
Teclados	[1.5.2] Avería de origen físico
Teclados	[I.6] Corte del suministro eléctrico
Teclados	[I.7] Condiciones inadecuadas de temperatura o humedad
Teclados	[I.11] Emanaciones electromagnéticas (TEMPEST)
Teclados	[E.23] Errores de mantenimiento / actualización de equipos
Teclados	[E.25] Perdida de equipos
Teclados	[A.11] Acceso no autorizado
Teclados	[A.23] Manipulación de hardware
Teclados	[A.24] Denegación de servicio
Teclados	[A.25] Robo de equipos
Teclados	[A.26] Ataque destructivo
TV	[N.1] Fuego
TV	[N.2] Daños por agua
TV	[N] Desastres naturales
TV	[I.*] Desastres industriales
TV	[1.3] Contaminación medioambiental
TV	[I.4] Contaminación electromagnética
TV	[1.5.2] Avería de origen físico
TV	[I.6] Corte del suministro eléctrico
TV	[I.7] Condiciones inadecuadas de temperatura o humedad
TV	[I.11] Emanaciones electromagnéticas (TEMPEST)
TV	[E.23] Errores de mantenimiento / actualización de equipos
TV	[E.25] Perdida de equipos
TV	[A.11] Acceso no autorizado
TV	[A.23] Manipulación de hardware
TV	[A.24] Denegación de servicio
TV	[A.25] Robo de equipos
TV	[A.26] Ataque destructivo
Amplificadores	[N.1] Fuego
Amplificadores	[N.2] Daños por agua
Amplificadores	[N] Desastres naturales
Amplificadores	[I.*] Desastres industriales
Amplificadores	[1.3] Contaminación medioambiental
Amplificadores	[I.4] Contaminación electromagnética
Amplificadores	[1.5.2] Avería de origen físico
Amplificadores	[I.6] Corte del suministro eléctrico
Amplificadores	[I.7] Condiciones inadecuadas de temperatura o humedad
Amplificadores	[I.11] Emanaciones electromagnéticas (TEMPEST)
Amplificadores	[E.23] Errores de mantenimiento / actualización de equipos
Amplificadores	[E.25] Perdida de equipos
Amplificadores	[A.11] Acceso no autorizado
Amplificadores	[A.23] Manipulación de hardware

Amplificadores	[A.24] Denegación de servicio
Amplificadores	[A.25] Robo de equipos
Amplificadores	[A.26] Ataque destructivo
Aspiradores	[N.1] Fuego
Aspiradores	[N.2] Daños por agua
Aspiradores	[N] Desastres naturales
Aspiradores	[I.*] Desastres industriales
Aspiradores	[1.3] Contaminación medioambiental
Aspiradores	[I.4] Contaminación electromagnética
Aspiradores	[1.5.2] Avería de origen físico
Aspiradores	[I.6] Corte del suministro eléctrico
Aspiradores	[I.7] Condiciones inadecuadas de temperatura o humedad
Aspiradores	[I.11] Emanaciones electromagnéticas (TEMPEST)
Aspiradores	[E.23] Errores de mantenimiento / actualización de equipos
Aspiradores	[E.25] Perdida de equipos
Aspiradores	[A.11] Acceso no autorizado
Aspiradores	[A.23] Manipulación de hardware
Aspiradores	[A.24] Denegación de servicio
Aspiradores	[A.25] Robo de equipos
Aspiradores	[A.26] Ataque destructivo
Lectores de huellas	[N.1] Fuego
Lectores de huellas	[N.2] Daños por agua
Lectores de huellas	[N] Desastres naturales
Lectores de huellas	[I.*] Desastres industriales
Lectores de huellas	[1.3] Contaminación medioambiental
Lectores de huellas	[I.4] Contaminación electromagnética
Lectores de huellas	[1.5.2] Avería de origen físico
Lectores de huellas	[I.6] Corte del suministro eléctrico
Lectores de huellas	[I.7] Condiciones inadecuadas de temperatura o humedad
Lectores de huellas	[I.11] Emanaciones electromagnéticas (TEMPEST)
Lectores de huellas	[E.23] Errores de mantenimiento / actualización de equipos
Lectores de huellas	[E.25] Perdida de equipos
Lectores de huellas	[A.11] Acceso no autorizado
Lectores de huellas	[A.23] Manipulación de hardware
Lectores de huellas	[A.24] Denegación de servicio
Lectores de huellas	[A.25] Robo de equipos
Lectores de huellas	[A.26] Ataque destructivo
Biométricos	[N.1] Fuego
Biométricos	[N.2] Daños por agua
Biométricos	[N] Desastres naturales
Biométricos	[I.*] Desastres industriales
Biométricos	[1.3] Contaminación medioambiental
Biométricos	[I.4] Contaminación electromagnética

Biométricos	[1.5.2] Avería de origen físico
Biométricos	[I.6] Corte del suministro eléctrico
Biométricos	[I.7] Condiciones inadecuadas de temperatura o humedad
Biométricos	[I.11] Emanaciones electromagnéticas (TEMPEST)
Biométricos	[E.23] Errores de mantenimiento / actualización de equipos
Biométricos	[E.25] Perdida de equipos
Biométricos	[A.11] Acceso no autorizado
Biométricos	[A.23] Manipulación de hardware
Biométricos	[A.24] Denegación de servicio
Biométricos	[A.25] Robo de equipos
Biométricos	[A.26] Ataque destructivo
Celulares	[N.1] Fuego
Celulares	[N.2] Daños por agua
Celulares	[N] Desastres naturales
Celulares	[I.*] Desastres industriales
Celulares	[1.3] Contaminación medioambiental
Celulares	[I.4] Contaminación electromagnética
Celulares	[1.5.2] Avería de origen físico
Celulares	[I.6] Corte del suministro eléctrico
Celulares	[I.7] Condiciones inadecuadas de temperatura o humedad
Celulares	[I.11] Emanaciones electromagnéticas (TEMPEST)
Celulares	[E.23] Errores de mantenimiento / actualización de equipos
Celulares	[E.25] Perdida de equipos
Celulares	[A.11] Acceso no autorizado
Celulares	[A.23] Manipulación de hardware
Celulares	[A.24] Denegación de servicio
Celulares	[A.25] Robo de equipos
Celulares	[A.26] Ataque destructivo
Micrófonos	[N.1] Fuego
Micrófonos	[N.2] Daños por agua
Micrófonos	[N] Desastres naturales
Micrófonos	[I.*] Desastres industriales
Micrófonos	[1.3] Contaminación medioambiental
Micrófonos	[I.4] Contaminación electromagnética
Micrófonos	[1.5.2] Avería de origen físico
Micrófonos	[I.6] Corte del suministro eléctrico
Micrófonos	[I.7] Condiciones inadecuadas de temperatura o humedad
Micrófonos	[I.11] Emanaciones electromagnéticas (TEMPEST)
Micrófonos	[E.23] Errores de mantenimiento / actualización de equipos
Micrófonos	[E.25] Perdida de equipos
Micrófonos	[A.11] Acceso no autorizado
Micrófonos	[A.23] Manipulación de hardware
Micrófonos	[A.24] Denegación de servicio

Micrófonos	[A.25] Robo de equipos
Micrófonos	[A.26] Ataque destructivo
Televisores	[N.1] Fuego
Televisores	[N.2] Daños por agua
Televisores	[N] Desastres naturales
Televisores	[I.*] Desastres industriales
Televisores	[1.3] Contaminación medioambiental
Televisores	[I.4] Contaminación electromagnética
Televisores	[1.5.2] Avería de origen físico
Televisores	[I.6] Corte del suministro eléctrico
Televisores	[I.7] Condiciones inadecuadas de temperatura o humedad
Televisores	[I.11] Emanaciones electromagnéticas (TEMPEST)
Televisores	[E.23] Errores de mantenimiento / actualización de equipos
Televisores	[E.25] Perdida de equipos
Televisores	[A.11] Acceso no autorizado
Televisores	[A.23] Manipulación de hardware
Televisores	[A.24] Denegación de servicio
Televisores	[A.25] Robo de equipos
Televisores	[A.26] Ataque destructivo
Alcancel	[N.1] Fuego
Alcancel	[N.2] Daños por agua
Alcancel	[N] Desastres naturales
Alcancel	[I.*] Desastres industriales
Alcancel	[1.3] Contaminación medioambiental
Alcancel	[I.4] Contaminación electromagnética
Alcancel	[1.5.2] Avería de origen físico
Alcancel	[I.6] Corte del suministro eléctrico
Alcancel	[I.7] Condiciones inadecuadas de temperatura o humedad
Alcancel	[I.11] Emanaciones electromagnéticas (TEMPEST)
Alcancel	[E.23] Errores de mantenimiento / actualización de equipos
Alcancel	[E.25] Perdida de equipos
Alcancel	[A.11] Acceso no autorizado
Alcancel	[A.23] Manipulación de hardware
Alcancel	[A.24] Denegación de servicio
Alcancel	[A.25] Robo de equipos
Alcancel	[A.26] Ataque destructivo
Estanterías	[N.1] Fuego
Estanterías	[N.2] Daños por agua
Estanterías	[N] Desastres naturales
Estanterías	[I.*] Desastres industriales
Estanterías	[1.3] Contaminación medioambiental
Estanterías	[I.4] Contaminación electromagnética
Estanterías	[1.5.2] Avería de origen físico

Estanterías	[I.6] Corte del suministro eléctrico
Estanterías	[I.7] Condiciones inadecuadas de temperatura o humedad
Estanterías	[I.11] Emanaciones electromagnéticas (TEMPEST)
Estanterías	[E.23] Errores de mantenimiento / actualización de equipos
Estanterías	[E.25] Perdida de equipos
Estanterías	[A.11] Acceso no autorizado
Estanterías	[A.23] Manipulación de hardware
Estanterías	[A.24] Denegación de servicio
Estanterías	[A.25] Robo de equipos
Estanterías	[A.26] Ataque destructivo
Rótulos	[N.1] Fuego
Rótulos	[N.2] Daños por agua
Rótulos	[N] Desastres naturales
Rótulos	[I.*] Desastres industriales
Rótulos	[1.3] Contaminación medioambiental
Rótulos	[I.4] Contaminación electromagnética
Rótulos	[1.5.2] Avería de origen físico
Rótulos	[I.6] Corte del suministro eléctrico
Rótulos	[I.7] Condiciones inadecuadas de temperatura o humedad
Rótulos	[I.11] Emanaciones electromagnéticas (TEMPEST)
Rótulos	[E.23] Errores de mantenimiento / actualización de equipos
Rótulos	[E.25] Perdida de equipos
Rótulos	[A.11] Acceso no autorizado
Rótulos	[A.23] Manipulación de hardware
Rótulos	[A.24] Denegación de servicio
Rótulos	[A.25] Robo de equipos
Rótulos	[A.26] Ataque destructivo
Rack	[N.1] Fuego
Rack	[N.2] Daños por agua
Rack	[N] Desastres naturales
Rack	[I.*] Desastres industriales
Rack	[1.3] Contaminación medioambiental
Rack	[I.4] Contaminación electromagnética
Rack	[1.5.2] Avería de origen físico
Rack	[I.6] Corte del suministro eléctrico
Rack	[I.7] Condiciones inadecuadas de temperatura o humedad
Rack	[I.11] Emanaciones electromagnéticas (TEMPEST)
Rack	[E.23] Errores de mantenimiento / actualización de equipos
Rack	[E.25] Perdida de equipos
Rack	[A.11] Acceso no autorizado
Rack	[A.23] Manipulación de hardware
Rack	[A.24] Denegación de servicio
Rack	[A.25] Robo de equipos

Rack	[A.26] Ataque destructivo
Implementos instalación internet	[N.1] Fuego
Implementos instalación internet	[N.2] Daños por agua
Implementos instalación internet	[N] Desastres naturales
Implementos instalación internet	[I.*] Desastres industriales
Implementos instalación internet	[1.3] Contaminación medioambiental
Implementos instalación internet	[I.4] Contaminación electromagnética
Implementos instalación internet	[1.5.2] Avería de origen físico
Implementos instalación internet	[I.6] Corte del suministro eléctrico
Implementos instalación internet	[I.7] Condiciones inadecuadas de temperatura o humedad
Implementos instalación internet	[I.11] Emanaciones electromagnéticas (TEMPEST)
Implementos instalación internet	[E.23] Errores de mantenimiento / actualización de equipos
Implementos instalación internet	[E.25] Perdida de equipos
Implementos instalación internet	[A.11] Acceso no autorizado
Implementos instalación internet	[A.23] Manipulación de hardware
Implementos instalación internet	[A.24] Denegación de servicio
Implementos instalación internet	[A.25] Robo de equipos
Implementos instalación internet	[A.26] Ataque destructivo
OLT	[N.1] Fuego
OLT	[N.2] Daños por agua
OLT	[N] Desastres naturales
OLT	[I.*] Desastres industriales
OLT	[1.3] Contaminación medioambiental
OLT	[I.4] Contaminación electromagnética
OLT	[1.5.2] Avería de origen físico
OLT	[I.6] Corte del suministro eléctrico
OLT	[I.7] Condiciones inadecuadas de temperatura o humedad
OLT	[I.11] Emanaciones electromagnéticas (TEMPEST)
OLT	[E.23] Errores de mantenimiento / actualización de equipos
OLT	[E.25] Perdida de equipos
OLT	[A.11] Acceso no autorizado
OLT	[A.23] Manipulación de hardware
OLT	[A.24] Denegación de servicio
OLT	[A.25] Robo de equipos
OLT	[A.26] Ataque destructivo
Unidades de almacenamiento	[N.1] Fuego
Unidades de almacenamiento	[N.2] Daños por agua
Unidades de almacenamiento	[N] Desastres naturales
Unidades de almacenamiento	[I.*] Desastres industriales
Unidades de almacenamiento	[1.3] Contaminación medioambiental
Unidades de almacenamiento	[I.4] Contaminación electromagnética
Unidades de almacenamiento	[1.5.2] Avería de origen físico
Unidades de almacenamiento	[I.6] Corte del suministro eléctrico

Unidades de almacenamiento	[I.7] Condiciones inadecuadas de temperatura o humedad
Unidades de almacenamiento	[I.11] Emanaciones electromagnéticas (TEMPEST)
Unidades de almacenamiento	[E.23] Errores de mantenimiento / actualización de equipos
Unidades de almacenamiento	[E.25] Perdida de equipos
Unidades de almacenamiento	[A.11] Acceso no autorizado
Unidades de almacenamiento	[A.23] Manipulación de hardware
Unidades de almacenamiento	[A.24] Denegación de servicio
Unidades de almacenamiento	[A.25] Robo de equipos
Unidades de almacenamiento	[A.26] Ataque destructivo
	Comunicaciones
Teléfonos	[I.8] Fallo de servicios de comunicación
Teléfonos	[E.2] Errores del administrador del sistema / de la seguridad
Teléfonos	[E.24] Caída del sistema por agotamiento de recursos
Teléfonos	[A.7] Uso no previsto
Teléfonos	[A.18] Destrucción de la información
Teléfonos	[A.24] Denegación de servicio
	Auxiliares
Escaleras	[N.1] Fuego
Escaleras	[N.2] Daños por agua
Escaleras	[N] Desastres naturales
Escaleras	[I.*] Desastres industriales
Escaleras	[1.3] Contaminación medioambiental
Escaleras	[I.4] Contaminación electromagnética
Escaleras	[1.5.2] Avería de origen físico
Escaleras	[I.6] Corte del suministro eléctrico
Escaleras	[I.7] Condiciones inadecuadas de temperatura o humedad
Escaleras	[I.11] Emanaciones electromagnéticas (TEMPEST)
Escaleras	[E.23] Errores de mantenimiento / actualización de equipos
Escaleras	[E.25] Perdida de equipos
Escaleras	[A.11] Acceso no autorizado
Escaleras	[A.23] Manipulación de hardware
Escaleras	[A.24] Denegación de servicio
Escaleras	[A.25] Robo de equipos
Escaleras	[A.26] Ataque destructivo
Generadores	[N.1] Fuego
Generadores	[N.2] Daños por agua
Generadores	[N] Desastres naturales
Generadores	[I.*] Desastres industriales
Generadores	[1.3] Contaminación medioambiental
Generadores	[I.4] Contaminación electromagnética
Generadores	[1.5.2] Avería de origen físico
Generadores	[I.6] Corte del suministro eléctrico
Generadores	[I.7] Condiciones inadecuadas de temperatura o humedad

Generadores	[I.11] Emanaciones electromagnéticas (TEMPEST)
Generadores	[E.23] Errores de mantenimiento / actualización de equipos
Generadores	[E.25] Perdida de equipos
Generadores	[A.11] Acceso no autorizado
Generadores	[A.23] Manipulación de hardware
Generadores	[A.24] Denegación de servicio
Generadores	[A.25] Robo de equipos
Generadores	[A.26] Ataque destructivo
Sillas	[N.1] Fuego
Sillas	[N.2] Daños por agua
Sillas	[N] Desastres naturales
Sillas	[I.*] Desastres industriales
Sillas	[1.3] Contaminación medioambiental
Sillas	[I.4] Contaminación electromagnética
Sillas	[1.5.2] Avería de origen físico
Sillas	[I.6] Corte del suministro eléctrico
Sillas	[I.7] Condiciones inadecuadas de temperatura o humedad
Sillas	[I.11] Emanaciones electromagnéticas (TEMPEST)
Sillas	[E.23] Errores de mantenimiento / actualización de equipos
Sillas	[E.25] Perdida de equipos
Sillas	[A.11] Acceso no autorizado
Sillas	[A.23] Manipulación de hardware
Sillas	[A.24] Denegación de servicio
Sillas	[A.25] Robo de equipos
Sillas	[A.26] Ataque destructivo
Balanzas	[N.1] Fuego
Balanzas	[N.2] Daños por agua
Balanzas	[N] Desastres naturales
Balanzas	[I.*] Desastres industriales
Balanzas	[1.3] Contaminación medioambiental
Balanzas	[I.4] Contaminación electromagnética
Balanzas	[1.5.2] Avería de origen físico
Balanzas	[I.6] Corte del suministro eléctrico
Balanzas	[I.7] Condiciones inadecuadas de temperatura o humedad
Balanzas	[I.11] Emanaciones electromagnéticas (TEMPEST)
Balanzas	[E.23] Errores de mantenimiento / actualización de equipos
Balanzas	[E.25] Perdida de equipos
Balanzas	[A.11] Acceso no autorizado
Balanzas	[A.23] Manipulación de hardware
Balanzas	[A.24] Denegación de servicio
Balanzas	[A.25] Robo de equipos
Balanzas	[A.26] Ataque destructivo
Camilla	[N.1] Fuego

Camilla	[N.2] Daños por agua
Camilla	[N] Desastres naturales
Camilla	[I.*] Desastres industriales
Camilla	[1.3] Contaminación medioambiental
Camilla	[I.4] Contaminación electromagnética
Camilla	[1.5.2] Avería de origen físico
Camilla	[I.6] Corte del suministro eléctrico
Camilla	[I.7] Condiciones inadecuadas de temperatura o humedad
Camilla	[I.11] Emanaciones electromagnéticas (TEMPEST)
Camilla	[E.23] Errores de mantenimiento / actualización de equipos
Camilla	[E.25] Perdida de equipos
Camilla	[A.11] Acceso no autorizado
Camilla	[A.23] Manipulación de hardware
Camilla	[A.24] Denegación de servicio
Camilla	[A.25] Robo de equipos
Camilla	[A.26] Ataque destructivo
Linternas	[N.1] Fuego
Linternas	[N.2] Daños por agua
Linternas	[N] Desastres naturales
Linternas	[I.*] Desastres industriales
Linternas	[1.3] Contaminación medioambiental
Linternas	[I.4] Contaminación electromagnética
Linternas	[1.5.2] Avería de origen físico
Linternas	[I.6] Corte del suministro eléctrico
Linternas	[I.7] Condiciones inadecuadas de temperatura o humedad
Linternas	[I.11] Emanaciones electromagnéticas (TEMPEST)
Linternas	[E.23] Errores de mantenimiento / actualización de equipos
Linternas	[E.25] Perdida de equipos
Linternas	[A.11] Acceso no autorizado
Linternas	[A.23] Manipulación de hardware
Linternas	[A.24] Denegación de servicio
Linternas	[A.25] Robo de equipos
Linternas	[A.26] Ataque destructivo
Perforadoras	[N.1] Fuego
Perforadoras	[N.2] Daños por agua
Perforadoras	[N] Desastres naturales
Perforadoras	[I.*] Desastres industriales
Perforadoras	[1.3] Contaminación medioambiental
Perforadoras	[I.4] Contaminación electromagnética
Perforadoras	[1.5.2] Avería de origen físico
Perforadoras	[I.6] Corte del suministro eléctrico
Perforadoras	[I.7] Condiciones inadecuadas de temperatura o humedad
Perforadoras	[I.11] Emanaciones electromagnéticas (TEMPEST)

Perforadoras	[E.23] Errores de mantenimiento / actualización de equipos
Perforadoras	[E.25] Perdida de equipos
Perforadoras	[A.11] Acceso no autorizado
Perforadoras	[A.23] Manipulación de hardware
Perforadoras	[A.24] Denegación de servicio
Perforadoras	[A.25] Robo de equipos
Perforadoras	[A.26] Ataque destructivo
Recogedores	[N.1] Fuego
Recogedores	[N.2] Daños por agua
Recogedores	[N] Desastres naturales
Recogedores	[I.*] Desastres industriales
Recogedores	[1.3] Contaminación medioambiental
Recogedores	[I.4] Contaminación electromagnética
Recogedores	[1.5.2] Avería de origen físico
Recogedores	[I.6] Corte del suministro eléctrico
Recogedores	[I.7] Condiciones inadecuadas de temperatura o humedad
Recogedores	[I.11] Emanaciones electromagnéticas (TEMPEST)
Recogedores	[E.23] Errores de mantenimiento / actualización de equipos
Recogedores	[E.25] Perdida de equipos
Recogedores	[A.11] Acceso no autorizado
Recogedores	[A.23] Manipulación de hardware
Recogedores	[A.24] Denegación de servicio
Recogedores	[A.25] Robo de equipos
Recogedores	[A.26] Ataque destructivo
Regletas	[N.1] Fuego
Regletas	[N.2] Daños por agua
Regletas	[N] Desastres naturales
Regletas	[I.*] Desastres industriales
Regletas	[1.3] Contaminación medioambiental
Regletas	[I.4] Contaminación electromagnética
Regletas	[1.5.2] Avería de origen físico
Regletas	[I.6] Corte del suministro eléctrico
Regletas	[I.7] Condiciones inadecuadas de temperatura o humedad
Regletas	[I.11] Emanaciones electromagnéticas (TEMPEST)
Regletas	[E.23] Errores de mantenimiento / actualización de equipos
Regletas	[E.25] Perdida de equipos
Regletas	[A.11] Acceso no autorizado
Regletas	[A.23] Manipulación de hardware
Regletas	[A.24] Denegación de servicio
Regletas	[A.25] Robo de equipos
Regletas	[A.26] Ataque destructivo
Pizarrones	[N.1] Fuego
Pizarrones	[N.2] Daños por agua

Pizarrones	[N] Desastres naturales
Pizarrones	[I.*] Desastres industriales
Pizarrones	[1.3] Contaminación medioambiental
Pizarrones	[I.4] Contaminación electromagnética
Pizarrones	[1.5.2] Avería de origen físico
Pizarrones	[I.6] Corte del suministro eléctrico
Pizarrones	[I.7] Condiciones inadecuadas de temperatura o humedad
Pizarrones	[I.11] Emanaciones electromagnéticas (TEMPEST)
Pizarrones	[E.23] Errores de mantenimiento / actualización de equipos
Pizarrones	[E.25] Perdida de equipos
Pizarrones	[A.11] Acceso no autorizado
Pizarrones	[A.23] Manipulación de hardware
Pizarrones	[A.24] Denegación de servicio
Pizarrones	[A.25] Robo de equipos
Pizarrones	[A.26] Ataque destructivo
Sellos de oficina	[N.1] Fuego
Sellos de oficina	[N.2] Daños por agua
Sellos de oficina	[N] Desastres naturales
Sellos de oficina	[I.*] Desastres industriales
Sellos de oficina	[1.3] Contaminación medioambiental
Sellos de oficina	[I.4] Contaminación electromagnética
Sellos de oficina	[1.5.2] Avería de origen físico
Sellos de oficina	[I.6] Corte del suministro eléctrico
Sellos de oficina	[I.7] Condiciones inadecuadas de temperatura o humedad
Sellos de oficina	[I.11] Emanaciones electromagnéticas (TEMPEST)
Sellos de oficina	[E.23] Errores de mantenimiento / actualización de equipos
Sellos de oficina	[E.25] Perdida de equipos
Sellos de oficina	[A.11] Acceso no autorizado
Sellos de oficina	[A.23] Manipulación de hardware
Sellos de oficina	[A.24] Denegación de servicio
Sellos de oficina	[A.25] Robo de equipos
Sellos de oficina	[A.26] Ataque destructivo
Microondas	[N.1] Fuego
Microondas	[N.2] Daños por agua
Microondas	[N] Desastres naturales
Microondas	[I.*] Desastres industriales
Microondas	[1.3] Contaminación medioambiental
Microondas	[I.4] Contaminación electromagnética
Microondas	[1.5.2] Avería de origen físico
Microondas	[I.6] Corte del suministro eléctrico
Microondas	[I.7] Condiciones inadecuadas de temperatura o humedad
Microondas	[I.11] Emanaciones electromagnéticas (TEMPEST)
Microondas	[E.23] Errores de mantenimiento / actualización de equipos

Microondas	[E.25] Perdida de equipos
Microondas	[A.11] Acceso no autorizado
Microondas	[A.23] Manipulación de hardware
Microondas	[A.24] Denegación de servicio
Microondas	[A.25] Robo de equipos
Microondas	[A.26] Ataque destructivo
Microcomponentes	[N.1] Fuego
Microcomponentes	[N.2] Daños por agua
Microcomponentes	[N] Desastres naturales
Microcomponentes	[I.*] Desastres industriales
Microcomponentes	[1.3] Contaminación medioambiental
Microcomponentes	[I.4] Contaminación electromagnética
Microcomponentes	[1.5.2] Avería de origen físico
Microcomponentes	[I.6] Corte del suministro eléctrico
Microcomponentes	[I.7] Condiciones inadecuadas de temperatura o humedad
Microcomponentes	[I.11] Emanaciones electromagnéticas (TEMPEST)
Microcomponentes	[E.23] Errores de mantenimiento / actualización de equipos
Microcomponentes	[E.25] Perdida de equipos
Microcomponentes	[A.11] Acceso no autorizado
Microcomponentes	[A.23] Manipulación de hardware
Microcomponentes	[A.24] Denegación de servicio
Microcomponentes	[A.25] Robo de equipos
Microcomponentes	[A.26] Ataque destructivo
Lectores de barras	[N.1] Fuego
Lectores de barras	[N.2] Daños por agua
Lectores de barras	[N] Desastres naturales
Lectores de barras	[I.*] Desastres industriales
Lectores de barras	[1.3] Contaminación medioambiental
Lectores de barras	[I.4] Contaminación electromagnética
Lectores de barras	[1.5.2] Avería de origen físico
Lectores de barras	[I.6] Corte del suministro eléctrico
Lectores de barras	[I.7] Condiciones inadecuadas de temperatura o humedad
Lectores de barras	[I.11] Emanaciones electromagnéticas (TEMPEST)
Lectores de barras	[E.23] Errores de mantenimiento / actualización de equipos
Lectores de barras	[E.25] Perdida de equipos
Lectores de barras	[A.11] Acceso no autorizado
Lectores de barras	[A.23] Manipulación de hardware
Lectores de barras	[A.24] Denegación de servicio
Lectores de barras	[A.25] Robo de equipos
Lectores de barras	[A.26] Ataque destructivo
Dispensador de agua	[N.1] Fuego
Dispensador de agua	[N.2] Daños por agua
Dispensador de agua	[N] Desastres naturales

Dispensador de agua	[I.*] Desastres industriales
Dispensador de agua	[1.3] Contaminación medioambiental
Dispensador de agua	[I.4] Contaminación electromagnética
Dispensador de agua	[1.5.2] Avería de origen físico
Dispensador de agua	[I.6] Corte del suministro eléctrico
Dispensador de agua	[I.7] Condiciones inadecuadas de temperatura o humedad
Dispensador de agua	[I.11] Emanaciones electromagnéticas (TEMPEST)
Dispensador de agua	[E.23] Errores de mantenimiento / actualización de equipos
Dispensador de agua	[E.25] Perdida de equipos
Dispensador de agua	[A.11] Acceso no autorizado
Dispensador de agua	[A.23] Manipulación de hardware
Dispensador de agua	[A.24] Denegación de servicio
Dispensador de agua	[A.25] Robo de equipos
Dispensador de agua	[A.26] Ataque destructivo
Mostradores de vidrio	[N.1] Fuego
Mostradores de vidrio	[N.2] Daños por agua
Mostradores de vidrio	[N] Desastres naturales
Mostradores de vidrio	[I.*] Desastres industriales
Mostradores de vidrio	[1.3] Contaminación medioambiental
Mostradores de vidrio	[I.4] Contaminación electromagnética
Mostradores de vidrio	[1.5.2] Avería de origen físico
Mostradores de vidrio	[I.6] Corte del suministro eléctrico
Mostradores de vidrio	[I.7] Condiciones inadecuadas de temperatura o humedad
Mostradores de vidrio	[I.11] Emanaciones electromagnéticas (TEMPEST)
Mostradores de vidrio	[E.23] Errores de mantenimiento / actualización de equipos
Mostradores de vidrio	[E.25] Perdida de equipos
Mostradores de vidrio	[A.11] Acceso no autorizado
Mostradores de vidrio	[A.23] Manipulación de hardware
Mostradores de vidrio	[A.24] Denegación de servicio
Mostradores de vidrio	[A.25] Robo de equipos
Mostradores de vidrio	[A.26] Ataque destructivo
Parlantes	[N.1] Fuego
Parlantes	[N.2] Daños por agua
Parlantes	[N] Desastres naturales
Parlantes	[I.*] Desastres industriales
Parlantes	[1.3] Contaminación medioambiental
Parlantes	[I.4] Contaminación electromagnética
Parlantes	[1.5.2] Avería de origen físico
Parlantes	[I.6] Corte del suministro eléctrico
Parlantes	[I.7] Condiciones inadecuadas de temperatura o humedad
Parlantes	[I.11] Emanaciones electromagnéticas (TEMPEST)
Parlantes	[E.23] Errores de mantenimiento / actualización de equipos
Parlantes	[E.25] Perdida de equipos

Parlantes	[A.11] Acceso no autorizado
Parlantes	[A.23] Manipulación de hardware
Parlantes	[A.24] Denegación de servicio
Parlantes	[A.25] Robo de equipos
Parlantes	[A.26] Ataque destructivo
Copiadoras	[N.1] Fuego
Copiadoras	[N.2] Daños por agua
Copiadoras	[N] Desastres naturales
Copiadoras	[I.*] Desastres industriales
Copiadoras	[1.3] Contaminación medioambiental
Copiadoras	[I.4] Contaminación electromagnética
Copiadoras	[1.5.2] Avería de origen físico
Copiadoras	[I.6] Corte del suministro eléctrico
Copiadoras	[I.7] Condiciones inadecuadas de temperatura o humedad
Copiadoras	[I.11] Emanaciones electromagnéticas (TEMPEST)
Copiadoras	[E.23] Errores de mantenimiento / actualización de equipos
Copiadoras	[E.25] Perdida de equipos
Copiadoras	[A.11] Acceso no autorizado
Copiadoras	[A.23] Manipulación de hardware
Copiadoras	[A.24] Denegación de servicio
Copiadoras	[A.25] Robo de equipos
Copiadoras	[A.26] Ataque destructivo
Extintores	[N.1] Fuego
Extintores	[N.2] Daños por agua
Extintores	[N] Desastres naturales
Extintores	[I.*] Desastres industriales
Extintores	[1.3] Contaminación medioambiental
Extintores	[I.4] Contaminación electromagnética
Extintores	[1.5.2] Avería de origen físico
Extintores	[I.6] Corte del suministro eléctrico
Extintores	[I.7] Condiciones inadecuadas de temperatura o humedad
Extintores	[I.11] Emanaciones electromagnéticas (TEMPEST)
Extintores	[E.23] Errores de mantenimiento / actualización de equipos
Extintores	[E.25] Perdida de equipos
Extintores	[A.11] Acceso no autorizado
Extintores	[A.23] Manipulación de hardware
Extintores	[A.24] Denegación de servicio
Extintores	[A.25] Robo de equipos
Extintores	[A.26] Ataque destructivo
Casilleros metálicos	[N.1] Fuego
Casilleros metálicos	[N.2] Daños por agua
Casilleros metálicos	[N] Desastres naturales
Casilleros metálicos	[I.*] Desastres industriales

Casilleros metálicos	[1.3] Contaminación medioambiental
Casilleros metálicos	[I.4] Contaminación electromagnética
Casilleros metálicos	[1.5.2] Avería de origen físico
Casilleros metálicos	[I.6] Corte del suministro eléctrico
Casilleros metálicos	[I.7] Condiciones inadecuadas de temperatura o humedad
Casilleros metálicos	[I.11] Emanaciones electromagnéticas (TEMPEST)
Casilleros metálicos	[E.23] Errores de mantenimiento / actualización de equipos
Casilleros metálicos	[E.25] Perdida de equipos
Casilleros metálicos	[A.11] Acceso no autorizado
Casilleros metálicos	[A.23] Manipulación de hardware
Casilleros metálicos	[A.24] Denegación de servicio
Casilleros metálicos	[A.25] Robo de equipos
Casilleros metálicos	[A.26] Ataque destructivo
Data Fast	[N.1] Fuego
Data Fast	[N.2] Daños por agua
Data Fast	[N] Desastres naturales
Data Fast	[I.*] Desastres industriales
Data Fast	[1.3] Contaminación medioambiental
Data Fast	[I.4] Contaminación electromagnética
Data Fast	[1.5.2] Avería de origen físico
Data Fast	[I.6] Corte del suministro eléctrico
Data Fast	[I.7] Condiciones inadecuadas de temperatura o humedad
Data Fast	[I.11] Emanaciones electromagnéticas (TEMPEST)
Data Fast	[E.23] Errores de mantenimiento / actualización de equipos
Data Fast	[E.25] Perdida de equipos
Data Fast	[A.11] Acceso no autorizado
Data Fast	[A.23] Manipulación de hardware
Data Fast	[A.24] Denegación de servicio
Data Fast	[A.25] Robo de equipos
Data Fast	[A.26] Ataque destructivo
Arnés reforzado	[N.1] Fuego
Arnés reforzado	[N.2] Daños por agua
Arnés reforzado	[N] Desastres naturales
Arnés reforzado	[I.*] Desastres industriales
Arnés reforzado	[1.3] Contaminación medioambiental
Arnés reforzado	[I.4] Contaminación electromagnética
Arnés reforzado	[1.5.2] Avería de origen físico
Arnés reforzado	[I.6] Corte del suministro eléctrico
Arnés reforzado	[I.7] Condiciones inadecuadas de temperatura o humedad
Arnés reforzado	[I.11] Emanaciones electromagnéticas (TEMPEST)
Arnés reforzado	[E.23] Errores de mantenimiento / actualización de equipos
Arnés reforzado	[E.25] Perdida de equipos
Arnés reforzado	[A.11] Acceso no autorizado

Arnés reforzado	[A.23] Manipulación de hardware
Arnés reforzado	[A.24] Denegación de servicio
Arnés reforzado	[A.25] Robo de equipos
Arnés reforzado	[A.26] Ataque destructivo
Cascos	[N.1] Fuego
Cascos	[N.2] Daños por agua
Cascos	[N] Desastres naturales
Cascos	[I.*] Desastres industriales
Cascos	[1.3] Contaminación medioambiental
Cascos	[I.4] Contaminación electromagnética
Cascos	[1.5.2] Avería de origen físico
Cascos	[I.6] Corte del suministro eléctrico
Cascos	[I.7] Condiciones inadecuadas de temperatura o humedad
Cascos	[I.11] Emanaciones electromagnéticas (TEMPEST)
Cascos	[E.23] Errores de mantenimiento / actualización de equipos
Cascos	[E.25] Perdida de equipos
Cascos	[A.11] Acceso no autorizado
Cascos	[A.23] Manipulación de hardware
Cascos	[A.24] Denegación de servicio
Cascos	[A.25] Robo de equipos
Cascos	[A.26] Ataque destructivo
Cinturones	[N.1] Fuego
Cinturones	[N.2] Daños por agua
Cinturones	[N] Desastres naturales
Cinturones	[I.*] Desastres industriales
Cinturones	[1.3] Contaminación medioambiental
Cinturones	[I.4] Contaminación electromagnética
Cinturones	[1.5.2] Avería de origen físico
Cinturones	[I.6] Corte del suministro eléctrico
Cinturones	[I.7] Condiciones inadecuadas de temperatura o humedad
Cinturones	[I.11] Emanaciones electromagnéticas (TEMPEST)
Cinturones	[E.23] Errores de mantenimiento / actualización de equipos
Cinturones	[E.25] Perdida de equipos
Cinturones	[A.11] Acceso no autorizado
Cinturones	[A.23] Manipulación de hardware
Cinturones	[A.24] Denegación de servicio
Cinturones	[A.25] Robo de equipos
Cinturones	[A.26] Ataque destructivo
Eslinga	[N.1] Fuego
Eslinga	[N.2] Daños por agua
Eslinga	[N] Desastres naturales
Eslinga	[I.*] Desastres industriales
Eslinga	[1.3] Contaminación medioambiental

Eslinga	[I.4] Contaminación electromagnética
Eslinga	[1.5.2] Avería de origen físico
Eslinga	[I.6] Corte del suministro eléctrico
Eslinga	[I.7] Condiciones inadecuadas de temperatura o humedad
Eslinga	[I.11] Emanaciones electromagnéticas (TEMPEST)
Eslinga	[E.23] Errores de mantenimiento / actualización de equipos
Eslinga	[E.25] Perdida de equipos
Eslinga	[A.11] Acceso no autorizado
Eslinga	[A.23] Manipulación de hardware
Eslinga	[A.24] Denegación de servicio
Eslinga	[A.25] Robo de equipos
Eslinga	[A.26] Ataque destructivo
Gafas	[N.1] Fuego
Gafas	[N.2] Daños por agua
Gafas	[N] Desastres naturales
Gafas	[I.*] Desastres industriales
Gafas	[1.3] Contaminación medioambiental
Gafas	[I.4] Contaminación electromagnética
Gafas	[1.5.2] Avería de origen físico
Gafas	[I.6] Corte del suministro eléctrico
Gafas	[I.7] Condiciones inadecuadas de temperatura o humedad
Gafas	[I.11] Emanaciones electromagnéticas (TEMPEST)
Gafas	[E.23] Errores de mantenimiento / actualización de equipos
Gafas	[E.25] Perdida de equipos
Gafas	[A.11] Acceso no autorizado
Gafas	[A.23] Manipulación de hardware
Gafas	[A.24] Denegación de servicio
Gafas	[A.25] Robo de equipos
Gafas	[A.26] Ataque destructivo
Guantes	[N.1] Fuego
Guantes	[N.2] Daños por agua
Guantes	[N] Desastres naturales
Guantes	[I.*] Desastres industriales
Guantes	[1.3] Contaminación medioambiental
Guantes	[I.4] Contaminación electromagnética
Guantes	[1.5.2] Avería de origen físico
Guantes	[I.6] Corte del suministro eléctrico
Guantes	[I.7] Condiciones inadecuadas de temperatura o humedad
Guantes	[I.11] Emanaciones electromagnéticas (TEMPEST)
Guantes	[E.23] Errores de mantenimiento / actualización de equipos
Guantes	[E.25] Perdida de equipos
Guantes	[A.11] Acceso no autorizado
Guantes	[A.23] Manipulación de hardware

Guantes	[A.24] Denegación de servicio
Guantes	[A.25] Robo de equipos
Guantes	[A.26] Ataque destructivo
Mosquetón	[N.1] Fuego
Mosquetón	[N.2] Daños por agua
Mosquetón	[N] Desastres naturales
Mosquetón	[I.*] Desastres industriales
Mosquetón	[1.3] Contaminación medioambiental
Mosquetón	[I.4] Contaminación electromagnética
Mosquetón	[1.5.2] Avería de origen físico
Mosquetón	[I.6] Corte del suministro eléctrico
Mosquetón	[I.7] Condiciones inadecuadas de temperatura o humedad
Mosquetón	[I.11] Emanaciones electromagnéticas (TEMPEST)
Mosquetón	[E.23] Errores de mantenimiento / actualización de equipos
Mosquetón	[E.25] Perdida de equipos
Mosquetón	[A.11] Acceso no autorizado
Mosquetón	[A.23] Manipulación de hardware
Mosquetón	[A.24] Denegación de servicio
Mosquetón	[A.25] Robo de equipos
Mosquetón	[A.26] Ataque destructivo
Chalecos de seguridad	[N.1] Fuego
Chalecos de seguridad	[N.2] Daños por agua
Chalecos de seguridad	[N] Desastres naturales
Chalecos de seguridad	[I.*] Desastres industriales
Chalecos de seguridad	[1.3] Contaminación medioambiental
Chalecos de seguridad	[I.4] Contaminación electromagnética
Chalecos de seguridad	[1.5.2] Avería de origen físico
Chalecos de seguridad	[I.6] Corte del suministro eléctrico
Chalecos de seguridad	[I.7] Condiciones inadecuadas de temperatura o humedad
Chalecos de seguridad	[I.11] Emanaciones electromagnéticas (TEMPEST)
Chalecos de seguridad	[E.23] Errores de mantenimiento / actualización de equipos
Chalecos de seguridad	[E.25] Perdida de equipos
Chalecos de seguridad	[A.11] Acceso no autorizado
Chalecos de seguridad	[A.23] Manipulación de hardware
Chalecos de seguridad	[A.24] Denegación de servicio
Chalecos de seguridad	[A.25] Robo de equipos
Chalecos de seguridad	[A.26] Ataque destructivo
Conos de seguridad	[N.1] Fuego
Conos de seguridad	[N.2] Daños por agua
Conos de seguridad	[N] Desastres naturales
Conos de seguridad	[I.*] Desastres industriales
Conos de seguridad	[1.3] Contaminación medioambiental
Conos de seguridad	[I.4] Contaminación electromagnética

Conos de seguridad	[1.5.2] Avería de origen físico
Conos de seguridad	[I.6] Corte del suministro eléctrico
Conos de seguridad	[I.7] Condiciones inadecuadas de temperatura o humedad
Conos de seguridad	[I.11] Emanaciones electromagnéticas (TEMPEST)
Conos de seguridad	[E.23] Errores de mantenimiento / actualización de equipos
Conos de seguridad	[E.25] Perdida de equipos
Conos de seguridad	[A.11] Acceso no autorizado
Conos de seguridad	[A.23] Manipulación de hardware
Conos de seguridad	[A.24] Denegación de servicio
Conos de seguridad	[A.25] Robo de equipos
Conos de seguridad	[A.26] Ataque destructivo
Letreros de advertencia	[N.1] Fuego
Letreros de advertencia	[N.2] Daños por agua
Letreros de advertencia	[N] Desastres naturales
Letreros de advertencia	[I.*] Desastres industriales
Letreros de advertencia	[1.3] Contaminación medioambiental
Letreros de advertencia	[I.4] Contaminación electromagnética
Letreros de advertencia	[1.5.2] Avería de origen físico
Letreros de advertencia	[I.6] Corte del suministro eléctrico
Letreros de advertencia	[I.7] Condiciones inadecuadas de temperatura o humedad
Letreros de advertencia	[I.11] Emanaciones electromagnéticas (TEMPEST)
Letreros de advertencia	[E.23] Errores de mantenimiento / actualización de equipos
Letreros de advertencia	[E.25] Perdida de equipos
Letreros de advertencia	[A.11] Acceso no autorizado
Letreros de advertencia	[A.23] Manipulación de hardware
Letreros de advertencia	[A.24] Denegación de servicio
Letreros de advertencia	[A.25] Robo de equipos
Letreros de advertencia	[A.26] Ataque destructivo
Herramientas	[N.1] Fuego
Herramientas	[N.2] Daños por agua
Herramientas	[N] Desastres naturales
Herramientas	[I.*] Desastres industriales
Herramientas	[1.3] Contaminación medioambiental
Herramientas	[I.4] Contaminación electromagnética
Herramientas	[1.5.2] Avería de origen físico
Herramientas	[I.6] Corte del suministro eléctrico
Herramientas	[I.7] Condiciones inadecuadas de temperatura o humedad
Herramientas	[I.11] Emanaciones electromagnéticas (TEMPEST)
Herramientas	[E.23] Errores de mantenimiento / actualización de equipos
Herramientas	[E.25] Perdida de equipos
Herramientas	[A.11] Acceso no autorizado
Herramientas	[A.23] Manipulación de hardware
Herramientas	[A.24] Denegación de servicio

Herramientas	[A.25] Robo de equipos
Herramientas	[A.26] Ataque destructivo
Case para discos duros	[N.1] Fuego
Case para discos duros	[N.2] Daños por agua
Case para discos duros	[N] Desastres naturales
Case para discos duros	[I.*] Desastres industriales
Case para discos duros	[1.3] Contaminación medioambiental
Case para discos duros	[I.4] Contaminación electromagnética
Case para discos duros	[1.5.2] Avería de origen físico
Case para discos duros	[I.6] Corte del suministro eléctrico
Case para discos duros	[I.7] Condiciones inadecuadas de temperatura o humedad
Case para discos duros	[I.11] Emanaciones electromagnéticas (TEMPEST)
Case para discos duros	[E.23] Errores de mantenimiento / actualización de equipos
Case para discos duros	[E.25] Perdida de equipos
Case para discos duros	[A.11] Acceso no autorizado
Case para discos duros	[A.23] Manipulación de hardware
Case para discos duros	[A.24] Denegación de servicio
Case para discos duros	[A.25] Robo de equipos
Case para discos duros	[A.26] Ataque destructivo
Apple pencil	[N.1] Fuego
Apple pencil	[N.2] Daños por agua
Apple pencil	[N] Desastres naturales
Apple pencil	[I.*] Desastres industriales
Apple pencil	[1.3] Contaminación medioambiental
Apple pencil	[I.4] Contaminación electromagnética
Apple pencil	[1.5.2] Avería de origen físico
Apple pencil	[I.6] Corte del suministro eléctrico
Apple pencil	[I.7] Condiciones inadecuadas de temperatura o humedad
Apple pencil	[I.11] Emanaciones electromagnéticas (TEMPEST)
Apple pencil	[E.23] Errores de mantenimiento / actualización de equipos
Apple pencil	[E.25] Perdida de equipos
Apple pencil	[A.11] Acceso no autorizado
Apple pencil	[A.23] Manipulación de hardware
Apple pencil	[A.24] Denegación de servicio
Apple pencil	[A.25] Robo de equipos
Apple pencil	[A.26] Ataque destructivo
Alexa	[N.1] Fuego
Alexa	[N.2] Daños por agua
Alexa	[N] Desastres naturales
Alexa	[I.*] Desastres industriales
Alexa	[1.3] Contaminación medioambiental
Alexa	[I.4] Contaminación electromagnética
Alexa	[1.5.2] Avería de origen físico

Alexa	[I.6] Corte del suministro eléctrico
Alexa	[I.7] Condiciones inadecuadas de temperatura o humedad
Alexa	[I.11] Emanaciones electromagnéticas (TEMPEST)
Alexa	[E.23] Errores de mantenimiento / actualización de equipos
Alexa	[E.25] Perdida de equipos
Alexa	[A.11] Acceso no autorizado
Alexa	[A.23] Manipulación de hardware
Alexa	[A.24] Denegación de servicio
Alexa	[A.25] Robo de equipos
Alexa	[A.26] Ataque destructivo
	Servicios subcontratados/ Instalaciones
Casa Plus 1	[N.1] Fuego
Casa Plus 1	[N.2] Daños por agua
Casa Plus 1	[N] Desastres naturales
Casa Plus 1	[N.1] Fuego
Casa Plus 1	[I.*] Desastres industriales
Casa Plus 1	[1.3] Contaminación medioambiental
Casa Plus 1	[I.4] Contaminación electromagnética
Casa Plus 1	[E.25] Perdida de equipos
Casa Plus 1	[A.6] Abuso de privilegios de acceso
Casa Plus 1	[A.7] Uso no previsto
Casa Plus 1	[A.25] Robo de equipos
Casa Plus 1	[A.26] Ataque destructivo
Casa Plus 1	[A.27] Ocupación enemiga
Casa Plus 2	[N.1] Fuego
Casa Plus 2	[N.2] Daños por agua
Casa Plus 2	[N] Desastres naturales
Casa Plus 2	[N.1] Fuego
Casa Plus 2	[I.*] Desastres industriales
Casa Plus 2	[1.3] Contaminación medioambiental
Casa Plus 2	[I.4] Contaminación electromagnética
Casa Plus 2	[E.25] Perdida de equipos
Casa Plus 2	[A.6] Abuso de privilegios de acceso
Casa Plus 2	[A.7] Uso no previsto
Casa Plus 2	[A.25] Robo de equipos
Casa Plus 2	[A.26] Ataque destructivo
Casa Plus 2	[A.27] Ocupación enemiga
	Personal
Gerencia General	[E.15] Alteración de la información
Gerencia General	[E.18] Destrucción de información
Gerencia General	[E.19] Fuga de información
Gerencia General	[E.28] Indisponibilidad de personal
Gerencia General	[A.15] Modificación de la información

Gerencia General	[A.18] Destrucción de la información
Gerencia General	[A.19] Revelación de información
Gerencia General	[E.28] Indisponibilidad de personal
Gerencia General	[A.29] Extorsión
Gerencia General	[A.30] Ingeniería Social (picaresca)
Gerencia Operativa	[E.15] Alteración de la información
Gerencia Operativa	[E.18] Destrucción de información
Gerencia Operativa	[E.19] Fuga de información
Gerencia Operativa	[E.28] Indisponibilidad de personal
Gerencia Operativa	[A.15] Modificación de la información
Gerencia Operativa	[A.18] Destrucción de la información
Gerencia Operativa	[A.19] Revelación de información
Gerencia Operativa	[E.28] Indisponibilidad de personal
Gerencia Operativa	[A.29] Extorsión
Gerencia Operativa	[A.30] Ingeniería Social (picaresca)
Gerencia Administrativa	[E.15] Alteración de la información
Gerencia Administrativa	[E.18] Destrucción de información
Gerencia Administrativa	[E.19] Fuga de información
Gerencia Administrativa	[E.28] Indisponibilidad de personal
Gerencia Administrativa	[A.15] Modificación de la información
Gerencia Administrativa	[A.18] Destrucción de la información
Gerencia Administrativa	[A.19] Revelación de información
Gerencia Administrativa	[E.28] Indisponibilidad de personal
Gerencia Administrativa	[A.29] Extorsión
Gerencia Administrativa	[A.30] Ingeniería Social (picaresca)
Gerencia Atención al Cliente	[E.15] Alteración de la información
Gerencia Atención al Cliente	[E.18] Destrucción de información
Gerencia Atención al Cliente	[E.19] Fuga de información
Gerencia Atención al Cliente	[E.28] Indisponibilidad de personal
Gerencia Atención al Cliente	[A.15] Modificación de la información
Gerencia Atención al Cliente	[A.18] Destrucción de la información
Gerencia Atención al Cliente	[A.19] Revelación de información
Gerencia Atención al Cliente	[E.28] Indisponibilidad de personal
Gerencia Atención al Cliente	[A.29] Extorsión
Gerencia Atención al Cliente	[A.30] Ingeniería Social (picaresca)
Gerencia comercial	[E.15] Alteración de la información
Gerencia comercial	[E.18] Destrucción de información
Gerencia comercial	[E.19] Fuga de información
Gerencia comercial	[E.28] Indisponibilidad de personal
Gerencia comercial	[A.15] Modificación de la información
Gerencia comercial	[A.18] Destrucción de la información
Gerencia comercial	[A.19] Revelación de información
Gerencia comercial	[E.28] Indisponibilidad de personal

Gerencia comercial	[A.29] Extorsión
Gerencia comercial	[A.30] Ingeniería Social (picaresca)

Nota: Elaboración Propia

Anexo 3 Porcentaje de disponibilidad integridad y confidencialidad de los activos

Activo	Amenaza	D	I	C
	Datos/Información			
Base de Datos	[1.5.11 Avería de origen lógico	50%		
Base de Datos	[E.8] Difusión de software dañino	10%	10%	10%
Base de Datos	[E.15] Alteración de la información	1%	20%	20%
Base de Datos	[E,20] Vulnerabilidades de los programas (software)	1%	10%	50%
Base de Datos	[E.21] Errores de mantenimiento / actualización (software)	100 %	100 %	100 %
Base de Datos	[A.8] Difusión de software dañino	50%	100 %	100 %
Base de Datos	[A.22] Manipulación de programas	100 %	100 %	100 %
Base de Datos	[1.5.11 Avería de origen lógico	50%		
Base de Datos	[E.8] Difusión de software dañino	10%	10%	10%
Base de Datos	[E.20] Vulnerabilidades de los programas (software)	1%	20%	20%
Base de Datos	[E.21] Errores de mantenimiento / actualización (software)	1%	10%	50%
Base de Datos	[A.8] Difusión de software dañino	100 %	100 %	100 %
Base de Datos	[A.221] Manipulación de programas	50%	100 %	100 %
	Servicios			
Electricidad	[E.2] Errores del administrador del sistema / de la seguridad	10%	10%	20%
Electricidad	[E.15] Alteración de la información		10%	10%
Electricidad	[E.19] Fugas de información		10%	10%
Electricidad	[A.5] Suplantación de la identidad	50%	50%	50%
Electricidad	[A.6] Abuso de privilegios de acceso	10%	10%	10%
Electricidad	[A.7] Uso no previsto	10%	10%	10%
Electricidad	[A.11] Acceso no autorizado	10%	50%	10%
Electricidad	[A.15] Modificación de la información	50%		50%
Internet	[E.1] Errores de los usuarios		10%	10%
Internet	[E.2] Errores del administrador del sistema / de la seguridad	10%	20%	20%
Internet	[E.15] Alteración de la información		1%	10%
Internet	[E.19] Fugas de información	10%	10%	10%

Internet	[A.5] Suplantación de la identidad	10%	50%	50%
Internet	[A.6] Abuso de privilegios de acceso		10%	10%
Internet	[A.7] Uso no previsto	10%	10%	10%
Internet	[A.11] Acceso no autorizado	10%	50%	10%
Internet	[A.15] Modificación de la información	50%		50%
Mantenimiento	[E.1] Errores de los usuarios		10%	10%
Mantenimiento	[E.2] Errores del administrador del sistema / de la seguridad	10%	20%	20%
Mantenimiento	[E.15] Alteración de la información		1%	10%
Mantenimiento	[E.19] Fugas de información	10%	10%	10%
Mantenimiento	[A.5] Suplantación de la identidad	10%	50%	50%
Mantenimiento	[A.6] Abuso de privilegios de acceso		10%	10%
Mantenimiento	[A.7] Uso no previsto	10%	10%	10%
Mantenimiento	[A.11] Acceso no autorizado	10%	50%	10%
Mantenimiento	[A.15] Modificación de la información	50%		50%
Correo	[E.1] Errores de los usuarios		10%	10%
Correo	[E.2] Errores del administrador del sistema / de la seguridad	10%	20%	20%
Correo	[E.15] Alteración de la información		1%	10%
Correo	[E.19] Fugas de información	10%	10%	10%
Correo	[A.5] Suplantación de la identidad	10%	50%	50%
Correo	[A.6] Abuso de privilegios de acceso		10%	10%
Correo	[A.7] Uso no previsto	10%	10%	10%
Correo	[A.11] Acceso no autorizado	10%	50%	10%
Correo	[A.15] Modificación de la información	50%		50%
Datos de ingreso	[1.5.1] Avería de origen lógico	100 %	100 %	100 %
Datos de ingreso	[E.8] Difusión de software dañino	50%		
Datos de ingreso	[E.20] Vulnerabilidades de los programas (software)	10%	10%	10%
Datos de ingreso	[E.21] Errores de mantenimiento / actualización (software)	1%	20%	20%
Datos de ingreso	[A.8] Difusión de software dañino	1%	10%	50%
Datos de ingreso	[A.221] Manipulación de programas	100 %	100 %	100 %

Detectores de humo	[1.3] Contaminación medioambiental	50%	100 %	100 %
Kits de seguridad	[N] Desastres naturales		10%	10%
Kits de seguridad	[N.1] Fuego	10%	10%	10%
Kits de seguridad	[A.26] Ataque destructivo	10%	50%	10%
Sistema contable	[1.5.1] Avería de origen lógico	50%		
Sistema contable	[E.8] Difusión de software dañino	10%	10%	10%
Sistema contable	[E.20] Vulnerabilidades de los programas (software)	1%	20%	20%
Sistema contable	[E.21] Errores de mantenimiento / actualización (software)	1%	10%	50%
Sistema contable	[A.8] Difusión de software dañino	100 %	100 %	100 %
Sistema contable	[A.221] Manipulación de programas	50%	100 %	100 %
Antivirus	[1.5.1] Avería de origen lógico	50%		
Antivirus	[E.8] Difusión de software dañino	10%	10%	10%
Antivirus	[E.20] Vulnerabilidades de los programas (software)	1%	20%	20%
Antivirus	[E.21] Errores de mantenimiento / actualización (software)	1%	10%	50%
Antivirus	[A.8] Difusión de software dañino	100 %	100 %	100 %
Antivirus	[A.221] Manipulación de programas	50%	100 %	100 %
Fusionadoras	[N.1] Fuego	100 %		
Fusionadoras	[N.2] Daños por agua	50%		
Fusionadoras	[N] Desastres naturales	100 %		
Fusionadoras	[I.*] Desastres industriales	100 %		
Fusionadoras	[1.3] Contaminación medioambiental	50%		
Fusionadoras	[I.4] Contaminación electromagnética	100 %		
Fusionadoras	[1.5.2] Avería de origen físico	50%		
Fusionadoras	[I.6] Corte del suministro eléctrico	10%		
Fusionadoras	[I.7] Condiciones inadecuadas de temperatura o humedad	50%		
Fusionadoras	[I.11] Emanaciones electromagnéticas (TEMPEST)	100 %		
Fusionadoras	[E.23] Errores de mantenimiento / actualización de equipos	100 %		
Fusionadoras	[E.25] Perdida de equipos			1%
Fusionadoras	[A.11] Acceso no autorizado	10%		
Fusionadoras	[A.23] Manipulación de hardware	50%		
Fusionadoras	[A.24] Denegación de servicio	100 %		50%

Fusionadoras	[A.25] Robo de equipos	10%	10%	50%
Fusionadoras	[A.26] Ataque destructivo	50%		50%
Cargadores	[N.1] Fuego	100 %		
Cargadores	[N.2] Daños por agua	50%		
Cargadores	[N] Desastres naturales	100 %		
Cargadores	[I.*] Desastres industriales	100 %		
Cargadores	[1.3] Contaminación medioambiental	50%		
Cargadores	[I.4] Contaminación electromagnética	100 %		
Cargadores	[1.5.2] Avería de origen físico	50%		
Cargadores	[I.6] Corte del suministro eléctrico	10%		
Cargadores	[I.7] Condiciones inadecuadas de temperatura o humedad	50%		
Cargadores	[I.11] Emanaciones electromagnéticas (TEMPEST)	100 %		
Cargadores	[E.23] Errores de mantenimiento / actualización de equipos	100 %		
Cargadores	[E.25] Perdida de equipos			1%
Cargadores	[A.11] Acceso no autorizado	10%		
Cargadores	[A.23] Manipulación de hardware	50%		
Cargadores	[A.24] Denegación de servicio	5%		10%
Cargadores	[A.25] Robo de equipos	10%	1%	10%
Cargadores	[A.26] Ataque destructivo	10%	10%	50%
Power Meter	[N.1] Fuego	100 %		
Power Meter	[N.2] Daños por agua	50%		
Power Meter	[N] Desastres naturales	100 %		
Power Meter	[I.*] Desastres industriales	100 %		
Power Meter	[1.3] Contaminación medioambiental	50%		
Power Meter	[I.4] Contaminación electromagnética	100 %		
Power Meter	[1.5.2] Avería de origen físico	50%		
Power Meter	[I.6] Corte del suministro eléctrico	10%		
Power Meter	[I.7] Condiciones inadecuadas de temperatura o humedad	50%		
Power Meter	[I.11] Emanaciones electromagnéticas (TEMPEST)	100 %		
Power Meter	[E.23] Errores de mantenimiento / actualización de equipos	100 %		
Power Meter	[E.25] Perdida de equipos			1%
Power Meter	[A.11] Acceso no autorizado	10%		
Power Meter	[A.23] Manipulación de hardware	50%		

Power Meter	[A.24] Denegación de servicio	100 %		50%
Power Meter	[A.25] Robo de equipos	10%		10%
Power Meter	[A.26] Ataque destructivo	10%	10%	50%
Sacabocados	[N.1] Fuego	100 %		
Sacabocados	[N.2] Daños por agua	50%		
Sacabocados	[N] Desastres naturales	100 %		
Sacabocados	[I.*] Desastres industriales	100 %		
Sacabocados	[1.3] Contaminación medioambiental	50%		
Sacabocados	[I.4] Contaminación electromagnética	100 %		
Sacabocados	[1.5.2] Avería de origen físico	50%		
Sacabocados	[I.6] Corte del suministro eléctrico	10%		
Sacabocados	[I.7] Condiciones inadecuadas de temperatura o humedad	50%		
Sacabocados	[I.11] Emanaciones electromagnéticas (TEMPEST)	100 %		
Sacabocados	[E.23] Errores de mantenimiento / actualización de equipos	100 %		
Sacabocados	[E.25] Perdida de equipos			1%
Sacabocados	[A.11] Acceso no autorizado	10%		
Sacabocados	[A.23] Manipulación de hardware	50%		
Sacabocados	[A.24] Denegación de servicio	100 %		50%
Sacabocados	[A.25] Robo de equipos	10%	10%	50%
Sacabocados	[A.26] Ataque destructivo	50%		50%
Taladros	[N.1] Fuego	100 %		
Taladros	[N.2] Daños por agua	50%		
Taladros	[N] Desastres naturales	100 %		
Taladros	[I.*] Desastres industriales	100 %		
Taladros	[1.3] Contaminación medioambiental	50%		
Taladros	[I.4] Contaminación electromagnética	100 %		
Taladros	[1.5.2] Avería de origen físico	50%		
Taladros	[I.6] Corte del suministro eléctrico	10%		
Taladros	[I.7] Condiciones inadecuadas de temperatura o humedad	50%		
Taladros	[I.11] Emanaciones electromagnéticas (TEMPEST)	100 %		
Taladros	[E.23] Errores de mantenimiento / actualización de equipos	100 %		
Taladros	[E.25] Perdida de equipos			1%

Taladros	[A.11] Acceso no autorizado	10%		
Taladros	[A.23] Manipulación de hardware	50%		
Taladros	[A.24] Denegación de servicio	100 %		50%
Taladros	[A.25] Robo de equipos	10%	10%	50%
Taladros	[A.26] Ataque destructivo	50%		50%
Etiquetadoras	[N.1] Fuego	100 %		
Etiquetadoras	[N.2] Daños por agua	50%		
Etiquetadoras	[N] Desastres naturales	100 %		
Etiquetadoras	[I.*] Desastres industriales	100 %		
Etiquetadoras	[1.3] Contaminación medioambiental	50%		
Etiquetadoras	[I.4] Contaminación electromagnética	100 %		
Etiquetadoras	[1.5.2] Avería de origen físico	50%		
Etiquetadoras	[I.6] Corte del suministro eléctrico	10%		
Etiquetadoras	[I.7] Condiciones inadecuadas de temperatura o humedad	50%		
Etiquetadoras	[I.11] Emanaciones electromagnéticas (TEMPEST)	100 %		
Etiquetadoras	[E.23] Errores de mantenimiento / actualización de equipos	100 %		
Etiquetadoras	[E.25] Perdida de equipos			1%
Etiquetadoras	[A.11] Acceso no autorizado	10%		
Etiquetadoras	[A.23] Manipulación de hardware	100 %		50%
Etiquetadoras	[A.24] Denegación de servicio	100 %		
Etiquetadoras	[A.25] Robo de equipos	100 %		50%
Etiquetadoras	[A.26] Ataque destructivo	100 %		
Cámaras Web	[N.1] Fuego	100 %		
Cámaras Web	[N.2] Daños por agua	50%		
Cámaras Web	[N] Desastres naturales	100 %		
Cámaras Web	[I.*] Desastres industriales	100 %		
Cámaras Web	[1.3] Contaminación medioambiental	50%		
Cámaras Web	[I.4] Contaminación electromagnética	100 %		
Cámaras Web	[1.5.2] Avería de origen físico	50%		
Cámaras Web	[I.6] Corte del suministro eléctrico	10%		
Cámaras Web	[I.7] Condiciones inadecuadas de temperatura o humedad	50%		

Cámaras Web	[I.11] Emanaciones electromagnéticas (TEMPEST)	100 %		
Cámaras Web	[E.23] Errores de mantenimiento / actualización de equipos	100 %		
Cámaras Web	[E.25] Perdida de equipos	100 %		100 %
Cámaras Web	[A.11] Acceso no autorizado	10%	100 %	100 %
Cámaras Web	[A.23] Manipulación de hardware	50%		50%
Cámaras Web	[A.24] Denegación de servicio	100 %		
Cámaras Web	[A.25] Robo de equipos	100 %		100 %
Cámaras Web	[A.26] Ataque destructivo	100 %		
Cooler AMD	[N.1] Fuego	50%		
Cooler AMD	[N.2] Daños por agua	10%		
Cooler AMD	[N] Desastres naturales	50%		
Cooler AMD	[I.*] Desastres industriales	10%	10%	50%
Cooler AMD	[1.3] Contaminación medioambiental	100 %		
Cooler AMD	[I.4] Contaminación electromagnética	50%		
Cooler AMD	[1.5.2] Avería de origen físico	10%		
Cooler AMD	[I.6] Corte del suministro eléctrico	50%		
Cooler AMD	[I.7] Condiciones inadecuadas de temperatura o humedad	10%	10%	50%
Cooler AMD	[I.11] Emanaciones electromagnéticas (TEMPEST)	100 %		
Cooler AMD	[E.23] Errores de mantenimiento / actualización de equipos	50%		
Cooler AMD	[E.25] Perdida de equipos	10%		
Cooler AMD	[A.11] Acceso no autorizado	50%		
Cooler AMD	[A.23] Manipulación de hardware	10%	10%	50%
Cooler AMD	[A.24] Denegación de servicio	100 %		
Cooler AMD	[A.25] Robo de equipos	10%	10%	50%
Cooler AMD	[A.26] Ataque destructivo	100 %		
CPU	[N.1] Fuego	100 %		
CPU	[N.2] Daños por agua	50%		
CPU	[N] Desastres naturales	100 %		
CPU	[I.*] Desastres industriales	100 %		
CPU	[1.3] Contaminación medioambiental	50%		
CPU	[I.4] Contaminación electromagnética	100 %		

CPU	[1.5.2] Avería de origen físico	50%		
CPU	[I.6] Corte del suministro eléctrico	10%		
CPU	[I.7] Condiciones inadecuadas de temperatura o humedad	50%		
CPU	[I.11] Emanaciones electromagnéticas (TEMPEST)	100 %		
CPU	[E.23] Errores de mantenimiento / actualización de equipos	100 %		100 %
CPU	[E.25] Perdida de equipos	10%	100 %	100 %
CPU	[A.11] Acceso no autorizado	10%	10%	100 %
CPU	[A.23] Manipulación de hardware	10%	100 %	100 %
CPU	[A.24] Denegación de servicio	100 %		
CPU	[A.25] Robo de equipos	100 %		100 %
CPU	[A.26] Ataque destructivo	100 %		
Video Card	[N.1] Fuego	100 %		
Video Card	[N.2] Daños por agua	50%		
Video Card	[N] Desastres naturales	100 %		
Video Card	[I.*] Desastres industriales	100 %		
Video Card	[1.3] Contaminación medioambiental	50%		
Video Card	[I.4] Contaminación electromagnética	100 %		
Video Card	[1.5.2] Avería de origen físico	50%		
Video Card	[I.6] Corte del suministro eléctrico	10%		
Video Card	[I.7] Condiciones inadecuadas de temperatura o humedad	50%		
Video Card	[I.11] Emanaciones electromagnéticas (TEMPEST)	100 %		
Video Card	[E.23] Errores de mantenimiento / actualización de equipos	100 %		
Video Card	[E.25] Perdida de equipos	100 %		50%
Video Card	[A.11] Acceso no autorizado	10%	10%	50%
Video Card	[A.23] Manipulación de hardware	50%		50%
Video Card	[A.24] Denegación de servicio	100 %		
Video Card	[A.25] Robo de equipos	100 %		50%
Video Card	[A.26] Ataque destructivo	100 %		

Impresoras	[N.1] Fuego	100%		
Impresoras	[N.2] Daños por agua	50%		
Impresoras	[N] Desastres naturales	100%		
Impresoras	[I.*] Desastres industriales	100%		
Impresoras	[1.3] Contaminación medioambiental	50%		
Impresoras	[I.4] Contaminación electromagnética	100%		
Impresoras	[1.5.2] Avería de origen físico	50%		
Impresoras	[I.6] Corte del suministro eléctrico	10%		
Impresoras	[I.7] Condiciones inadecuadas de temperatura o humedad	50%		
Impresoras	[I.11] Emanaciones electromagnéticas (TEMPEST)	100%		
Impresoras	[E.23] Errores de mantenimiento / actualización de equipos	100%		100%
Impresoras	[E.25] Perdida de equipos	1%	1%	10%
Impresoras	[A.11] Acceso no autorizado	10%	10%	50%
Impresoras	[A.23] Manipulación de hardware	50%		50%
Impresoras	[A.24] Denegación de servicio	100%		
Impresoras	[A.25] Robo de equipos	100%		100%
Impresoras	[A.26] Ataque destructivo	100%		
iPads Apple	[N.1] Fuego	100%		
iPads Apple	[N.2] Daños por agua	50%		
iPads Apple	[N] Desastres naturales	100%		
iPads Apple	[I.*] Desastres industriales	100%		
iPads Apple	[1.3] Contaminación medioambiental	50%		
iPads Apple	[I.4] Contaminación electromagnética	100%		
iPads Apple	[1.5.2] Avería de origen físico	50%		
iPads Apple	[I.6] Corte del suministro eléctrico	10%		
iPads Apple	[I.7] Condiciones inadecuadas de temperatura o humedad	50%		
iPads Apple	[I.11] Emanaciones electromagnéticas (TEMPEST)	100%		
iPads Apple	[E.23] Errores de mantenimiento / actualización de equipos	10%	100%	100%
iPads Apple	[E.25] Perdida de equipos	10%	10%	100%

iPads Apple	[A.11] Acceso no autorizado	10%	100 %	100 %
iPads Apple	[A.23] Manipulación de hardware	50%		50%
iPads Apple	[A.24] Denegación de servicio	100 %		
iPads Apple	[A.25] Robo de equipos	100 %		100 %
iPads Apple	[A.26] Ataque destructivo	100 %		
MacBook Air	[N.1] Fuego	100 %		
MacBook Air	[N.2] Daños por agua	50%		
MacBook Air	[N] Desastres naturales	100 %		
MacBook Air	[I.*] Desastres industriales	100 %		
MacBook Air	[1.3] Contaminación medioambiental	50%		
MacBook Air	[I.4] Contaminación electromagnética	100 %		
MacBook Air	[1.5.2] Avería de origen físico	50%		
MacBook Air	[I.6] Corte del suministro eléctrico	10%		
MacBook Air	[I.7] Condiciones inadecuadas de temperatura o humedad	50%		
MacBook Air	[I.11] Emanaciones electromagnéticas (TEMPEST)	100 %		100 %
MacBook Air	[E.23] Errores de mantenimiento / actualización de equipos	10%	100 %	100 %
MacBook Air	[E.25] Perdida de equipos	10%	10%	100 %
MacBook Air	[A.11] Acceso no autorizado	10%	100 %	100 %
MacBook Air	[A.23] Manipulación de hardware	100 %		50%
MacBook Air	[A.24] Denegación de servicio	100 %		
MacBook Air	[A.25] Robo de equipos	100 %		100 %
MacBook Air	[A.26] Ataque destructivo	100 %		
Monitores	[N.1] Fuego	100 %		
Monitores	[N.2] Daños por agua	50%		
Monitores	[N] Desastres naturales	100 %		
Monitores	[I.*] Desastres industriales	100 %		
Monitores	[1.3] Contaminación medioambiental	50%		
Monitores	[I.4] Contaminación electromagnética	100 %		

Monitores	[1.5.2] Avería de origen físico	50%		
Monitores	[I.6] Corte del suministro eléctrico	10%		
Monitores	[I.7] Condiciones inadecuadas de temperatura o humedad	10%	10%	50%
Monitores	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		
Monitores	[E.23] Errores de mantenimiento / actualización de equipos	100 %		100 %
Monitores	[E.25] Perdida de equipos	10%	100 %	100 %
Monitores	[A.11] Acceso no autorizado	10%	10%	100 %
Monitores	[A.23] Manipulación de hardware	10%	100 %	100 %
Monitores	[A.24] Denegación de servicio	100 %		
Monitores	[A.25] Robo de equipos	100 %		100 %
Monitores	[A.26] Ataque destructivo	100 %		
Mouse	[N.1] Fuego	100 %		
Mouse	[N.2] Daños por agua	50%		
Mouse	[N] Desastres naturales	100 %		
Mouse	[I.*] Desastres industriales	100 %		
Mouse	[1.3] Contaminación medioambiental	50%		
Mouse	[I.4] Contaminación electromagnética	100 %		
Mouse	[1.5.2] Avería de origen físico	50%		
Mouse	[I.6] Corte del suministro eléctrico	10%		
Mouse	[I.7] Condiciones inadecuadas de temperatura o humedad	50%		
Mouse	[I.11] Emanaciones electromagnéticas (TEMPEST)			1%
Mouse	[E.23] Errores de mantenimiento / actualización de equipos	10%		
Mouse	[E.25] Perdida de equipos	50%		
Mouse	[A.11] Acceso no autorizado	100 %		50%
Mouse	[A.23] Manipulación de hardware	10%	10%	50%
Mouse	[A.24] Denegación de servicio	50%		50%
Mouse	[A.25] Robo de equipos	100 %		
Mouse	[A.26] Ataque destructivo	100 %		50%
Server Dell	[N.1] Fuego	100 %		

Server Dell	[N.2] Daños por agua	50%		
Server Dell	[N] Desastres naturales	100 %		
Server Dell	[I.*] Desastres industriales	100 %		
Server Dell	[1.3] Contaminación medioambiental	50%		
Server Dell	[I.4] Contaminación electromagnética	100 %		
Server Dell	[1.5.2] Avería de origen físico	50%		
Server Dell	[I.6] Corte del suministro eléctrico	10%		
Server Dell	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %		100 %
Server Dell	[I.11] Emanaciones electromagnéticas (TEMPEST)	10%	100 %	100 %
Server Dell	[E.23] Errores de mantenimiento / actualización de equipos	10%	10%	100 %
Server Dell	[E.25] Perdida de equipos	100 %	100 %	100 %
Server Dell	[A.11] Acceso no autorizado	10%	100 %	100 %
Server Dell	[A.23] Manipulación de hardware	50%	100 %	100 %
Server Dell	[A.24] Denegación de servicio	100 %		
Server Dell	[A.25] Robo de equipos	100 %		100 %
Server Dell	[A.26] Ataque destructivo	100 %		
Tablet Lenovo	[N.1] Fuego	100 %		
Tablet Lenovo	[N.2] Daños por agua	50%		
Tablet Lenovo	[N] Desastres naturales	100 %		
Tablet Lenovo	[I.*] Desastres industriales	100 %		
Tablet Lenovo	[1.3] Contaminación medioambiental	50%		
Tablet Lenovo	[I.4] Contaminación electromagnética	100 %		
Tablet Lenovo	[1.5.2] Avería de origen físico	50%		
Tablet Lenovo	[I.6] Corte del suministro eléctrico	10%		
Tablet Lenovo	[I.7] Condiciones inadecuadas de temperatura o humedad	50%		
Tablet Lenovo	[I.11] Emanaciones electromagnéticas (TEMPEST)	100 %		100 %
Tablet Lenovo	[E.23] Errores de mantenimiento / actualización de equipos	10%	100 %	100 %
Tablet Lenovo	[E.25] Perdida de equipos	10%	10%	100 %

Tablet Lenovo	[A.11] Acceso no autorizado	10%	100 %	100 %
Tablet Lenovo	[A.23] Manipulación de hardware	50%		50%
Tablet Lenovo	[A.24] Denegación de servicio	100 %		
Tablet Lenovo	[A.25] Robo de equipos	100 %		100 %
Tablet Lenovo	[A.26] Ataque destructivo	100 %		
Teclados	[N.1] Fuego	100 %		
Teclados	[N.2] Daños por agua	50%		
Teclados	[N] Desastres naturales	100 %		
Teclados	[I.*] Desastres industriales	100 %		
Teclados	[1.3] Contaminación medioambiental	50%		
Teclados	[I.4] Contaminación electromagnética	100 %		
Teclados	[1.5.2] Avería de origen físico	50%		
Teclados	[I.6] Corte del suministro eléctrico	10%		
Teclados	[I.7] Condiciones inadecuadas de temperatura o humedad			1%
Teclados	[I.11] Emanaciones electromagnéticas (TEMPEST)	10%		
Teclados	[E.23] Errores de mantenimiento / actualización de equipos	50%		
Teclados	[E.25] Perdida de equipos	100 %		50%
Teclados	[A.11] Acceso no autorizado	10%	10%	50%
Teclados	[A.23] Manipulación de hardware	50%		50%
Teclados	[A.24] Denegación de servicio	100 %		
Teclados	[A.25] Robo de equipos	100 %		50%
Teclados	[A.26] Ataque destructivo	100 %		
TV	[N.1] Fuego	100 %		
TV	[N.2] Daños por agua	50%		
TV	[N] Desastres naturales	100 %		
TV	[I.*] Desastres industriales	100 %		
TV	[1.3] Contaminación medioambiental	50%		
TV	[I.4] Contaminación electromagnética	100 %		
TV	[1.5.2] Avería de origen físico	50%		
TV	[I.6] Corte del suministro eléctrico	10%		

TV	[I.7] Condiciones inadecuadas de temperatura o humedad			1%
TV	[I.11] Emanaciones electromagnéticas (TEMPEST)	10%		
TV	[E.23] Errores de mantenimiento / actualización de equipos	50%		
TV	[E.25] Perdida de equipos	100 %		50%
TV	[A.11] Acceso no autorizado	10%	10%	50%
TV	[A.23] Manipulación de hardware	50%		50%
TV	[A.24] Denegación de servicio	100 %		
TV	[A.25] Robo de equipos	100 %		50%
TV	[A.26] Ataque destructivo	100 %		
Amplificadores	[N.1] Fuego	100 %		
Amplificadores	[N.2] Daños por agua	50%		
Amplificadores	[N] Desastres naturales	100 %		
Amplificadores	[I.*] Desastres industriales	100 %		
Amplificadores	[1.3] Contaminación medioambiental	50%		
Amplificadores	[I.4] Contaminación electromagnética	100 %		
Amplificadores	[1.5.2] Avería de origen físico	50%		
Amplificadores	[I.6] Corte del suministro eléctrico	100 %		
Amplificadores	[I.7] Condiciones inadecuadas de temperatura o humedad			1%
Amplificadores	[I.11] Emanaciones electromagnéticas (TEMPEST)	10%		
Amplificadores	[E.23] Errores de mantenimiento / actualización de equipos	50%		
Amplificadores	[E.25] Perdida de equipos	100 %		50%
Amplificadores	[A.11] Acceso no autorizado	10%	10%	50%
Amplificadores	[A.23] Manipulación de hardware	50%		50%
Amplificadores	[A.24] Denegación de servicio	100 %		
Amplificadores	[A.25] Robo de equipos	100 %		50%
Amplificadores	[A.26] Ataque destructivo	100 %		
Aspiradores	[N.1] Fuego	100 %		
Aspiradores	[N.2] Daños por agua	50%		

Aspiradores	[N] Desastres naturales	100 %		
Aspiradores	[I.*] Desastres industriales	100 %		
Aspiradores	[1.3] Contaminación medioambiental	50%		
Aspiradores	[I.4] Contaminación electromagnética	10%		
Aspiradores	[1.5.2] Avería de origen físico	50%		
Aspiradores	[I.6] Corte del suministro eléctrico	100 %		
Aspiradores	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %		
Aspiradores	[I.11] Emanaciones electromagnéticas (TEMPEST)			1%
Aspiradores	[E.23] Errores de mantenimiento / actualización de equipos	10%		
Aspiradores	[E.25] Perdida de equipos	100 %		50%
Aspiradores	[A.11] Acceso no autorizado	10%	10%	50%
Aspiradores	[A.23] Manipulación de hardware	50%		50%
Aspiradores	[A.24] Denegación de servicio	100 %		
Aspiradores	[A.25] Robo de equipos	100 %		50%
Aspiradores	[A.26] Ataque destructivo	100 %		
Lectores de huellas	[N.1] Fuego	100 %		
Lectores de huellas	[N.2] Daños por agua	50%		
Lectores de huellas	[N] Desastres naturales	100 %		
Lectores de huellas	[I.*] Desastres industriales	100 %		
Lectores de huellas	[1.3] Contaminación medioambiental	50%		
Lectores de huellas	[I.4] Contaminación electromagnética	50%		
Lectores de huellas	[1.5.2] Avería de origen físico	50%		
Lectores de huellas	[I.6] Corte del suministro eléctrico	100 %		
Lectores de huellas	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %		
Lectores de huellas	[I.11] Emanaciones electromagnéticas (TEMPEST)			1%
Lectores de huellas	[E.23] Errores de mantenimiento / actualización de equipos	10%	10%	50%
Lectores de huellas	[E.25] Perdida de equipos	100 %		100 %
Lectores de huellas	[A.11] Acceso no autorizado	10%	100 %	100 %
Lectores de huellas	[A.23] Manipulación de hardware	50%		50%

Lectores de huellas	[A.24] Denegación de servicio	100 %		
Lectores de huellas	[A.25] Robo de equipos	100 %		100 %
Lectores de huellas	[A.26] Ataque destructivo	100 %		
Biométricos	[N.1] Fuego	100 %		
Biométricos	[N.2] Daños por agua	50%		
Biométricos	[N] Desastres naturales	100 %		
Biométricos	[I.*] Desastres industriales	100 %		
Biométricos	[1.3] Contaminación medioambiental	50%		
Biométricos	[I.4] Contaminación electromagnética	10%		
Biométricos	[1.5.2] Avería de origen físico	50%		
Biométricos	[I.6] Corte del suministro eléctrico	100 %		
Biométricos	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %		
Biométricos	[I.11] Emanaciones electromagnéticas (TEMPEST)			
Biométricos	[E.23] Errores de mantenimiento / actualización de equipos	10%		
Biométricos	[E.25] Perdida de equipos	100 %		50%
Biométricos	[A.11] Acceso no autorizado	10%	10%	50%
Biométricos	[A.23] Manipulación de hardware	50%		50%
Biométricos	[A.24] Denegación de servicio	100 %		
Biométricos	[A.25] Robo de equipos	100 %		50%
Biométricos	[A.26] Ataque destructivo	100 %		
Celulares	[N.1] Fuego	100 %		
Celulares	[N.2] Daños por agua	50%		
Celulares	[N] Desastres naturales	100 %		
Celulares	[I.*] Desastres industriales	100 %		
Celulares	[1.3] Contaminación medioambiental	50%		
Celulares	[I.4] Contaminación electromagnética	10%		
Celulares	[1.5.2] Avería de origen físico	50%		
Celulares	[I.6] Corte del suministro eléctrico	100 %		
Celulares	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %		

Celulares	[I.11] Emanaciones electromagnéticas (TEMPEST)			1%
Celulares	[E.23] Errores de mantenimiento / actualización de equipos	1%	5%	10%
Celulares	[E.25] Perdida de equipos	100 %		50%
Celulares	[A.11] Acceso no autorizado	10%	10%	50%
Celulares	[A.23] Manipulación de hardware	50%		50%
Celulares	[A.24] Denegación de servicio	100 %		
Celulares	[A.25] Robo de equipos	100 %		100 %
Celulares	[A.26] Ataque destructivo	100 %		
Micrófonos	[N.1] Fuego	100 %		
Micrófonos	[N.2] Daños por agua	50%		
Micrófonos	[N] Desastres naturales	100 %		
Micrófonos	[I.*] Desastres industriales	100 %		
Micrófonos	[1.3] Contaminación medioambiental	50%		
Micrófonos	[I.4] Contaminación electromagnética	10%		
Micrófonos	[1.5.2] Avería de origen físico	50%		
Micrófonos	[I.6] Corte del suministro eléctrico	100 %		
Micrófonos	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %		
Micrófonos	[I.11] Emanaciones electromagnéticas (TEMPEST)			1%
Micrófonos	[E.23] Errores de mantenimiento / actualización de equipos	10%		
Micrófonos	[E.25] Perdida de equipos	100 %		50%
Micrófonos	[A.11] Acceso no autorizado	10%	10%	50%
Micrófonos	[A.23] Manipulación de hardware	50%		50%
Micrófonos	[A.24] Denegación de servicio	100 %		
Micrófonos	[A.25] Robo de equipos	100 %		50%
Micrófonos	[A.26] Ataque destructivo	100 %		
Televisores	[N.1] Fuego	100 %		
Televisores	[N.2] Daños por agua	50%		
Televisores	[N] Desastres naturales	100 %		
Televisores	[I.*] Desastres industriales	100 %		

Televisores	[1.3] Contaminación medioambiental	50%		
Televisores	[I.4] Contaminación electromagnética	10%		
Televisores	[1.5.2] Avería de origen físico	50%		
Televisores	[I.6] Corte del suministro eléctrico	100 %		
Televisores	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %		
Televisores	[I.11] Emanaciones electromagnéticas (TEMPEST)			1%
Televisores	[E.23] Errores de mantenimiento / actualización de equipos	10%		
Televisores	[E.25] Perdida de equipos	100 %		50%
Televisores	[A.11] Acceso no autorizado	10%	10%	50%
Televisores	[A.23] Manipulación de hardware	50%		50%
Televisores	[A.24] Denegación de servicio	100 %		
Televisores	[A.25] Robo de equipos	100 %		50%
Televisores	[A.26] Ataque destructivo	100 %		
Alcancel	[N.1] Fuego	100 %		
Alcancel	[N.2] Daños por agua	50%		
Alcancel	[N] Desastres naturales	100 %		
Alcancel	[I.*] Desastres industriales	100 %		
Alcancel	[1.3] Contaminación medioambiental	50%		
Alcancel	[I.4] Contaminación electromagnética	10%		
Alcancel	[1.5.2] Avería de origen físico	50%		
Alcancel	[I.6] Corte del suministro eléctrico	100 %		
Alcancel	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %		
Alcancel	[I.11] Emanaciones electromagnéticas (TEMPEST)			1%
Alcancel	[E.23] Errores de mantenimiento / actualización de equipos	10%		
Alcancel	[E.25] Perdida de equipos	100 %		50%
Alcancel	[A.11] Acceso no autorizado	10%	10%	50%
Alcancel	[A.23] Manipulación de hardware	50%		50%
Alcancel	[A.24] Denegación de servicio	100 %		
Alcancel	[A.25] Robo de equipos	100 %		50%
Alcancel	[A.26] Ataque destructivo	100 %		

Estanterías	[N.1] Fuego	100%		
Estanterías	[N.2] Daños por agua	50%		
Estanterías	[N] Desastres naturales	100%		
Estanterías	[I.*] Desastres industriales	100%		
Estanterías	[1.3] Contaminación medioambiental	50%		
Estanterías	[I.4] Contaminación electromagnética	10%		
Estanterías	[1.5.2] Avería de origen físico	50%		
Estanterías	[I.6] Corte del suministro eléctrico	100%		
Estanterías	[I.7] Condiciones inadecuadas de temperatura o humedad	100%		
Estanterías	[I.11] Emanaciones electromagnéticas (TEMPEST)			1%
Estanterías	[E.23] Errores de mantenimiento / actualización de equipos	10%	10%	50%
Estanterías	[E.25] Perdida de equipos	50%		
Estanterías	[A.11] Acceso no autorizado	10%	100%	100%
Estanterías	[A.23] Manipulación de hardware	50%		50%
Estanterías	[A.24] Denegación de servicio	100%		
Estanterías	[A.25] Robo de equipos	100%		100%
Estanterías	[A.26] Ataque destructivo	100%		
Rótulos	[N.1] Fuego	100%		
Rótulos	[N.2] Daños por agua	50%		
Rótulos	[N] Desastres naturales	100%		
Rótulos	[I.*] Desastres industriales	100%		
Rótulos	[1.3] Contaminación medioambiental	50%		
Rótulos	[I.4] Contaminación electromagnética	10%		
Rótulos	[1.5.2] Avería de origen físico	50%		
Rótulos	[I.6] Corte del suministro eléctrico	100%		
Rótulos	[I.7] Condiciones inadecuadas de temperatura o humedad	100%		
Rótulos	[I.11] Emanaciones electromagnéticas (TEMPEST)			1%
Rótulos	[E.23] Errores de mantenimiento / actualización de equipos	10%		
Rótulos	[E.25] Perdida de equipos	100%		50%
Rótulos	[A.11] Acceso no autorizado	10%	10%	50%

Rótulos	[A.23] Manipulación de hardware	50%		50%
Rótulos	[A.24] Denegación de servicio	100 %		
Rótulos	[A.25] Robo de equipos	100 %		50%
Rótulos	[A.26] Ataque destructivo	100 %		
Rack	[N.1] Fuego	100 %		
Rack	[N.2] Daños por agua	50%		
Rack	[N] Desastres naturales	100 %		
Rack	[I.*] Desastres industriales	100 %		
Rack	[1.3] Contaminación medioambiental	50%		
Rack	[I.4] Contaminación electromagnética	10%		
Rack	[1.5.2] Avería de origen físico	50%		
Rack	[I.6] Corte del suministro eléctrico	100 %		
Rack	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %		
Rack	[I.11] Emanaciones electromagnéticas (TEMPEST)			1%
Rack	[E.23] Errores de mantenimiento / actualización de equipos	10%		
Rack	[E.25] Perdida de equipos	20%		50%
Rack	[A.11] Acceso no autorizado	10%	10%	50%
Rack	[A.23] Manipulación de hardware	100 %		50%
Rack	[A.24] Denegación de servicio	100 %		
Rack	[A.25] Robo de equipos	20%		50%
Rack	[A.26] Ataque destructivo	100 %		
Implementos instalación internet	[N.1] Fuego	100 %		
Implementos instalación internet	[N.2] Daños por agua	50%		
Implementos instalación internet	[N] Desastres naturales	100 %		
Implementos instalación internet	[I.*] Desastres industriales	100 %		
Implementos instalación internet	[1.3] Contaminación medioambiental	50%		
Implementos instalación internet	[I.4] Contaminación electromagnética	10%		
Implementos instalación internet	[1.5.2] Avería de origen físico	50%		

Implementos instalación internet	[I.6] Corte del suministro eléctrico	100 %		
Implementos instalación internet	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %		
Implementos instalación internet	[I.11] Emanaciones electromagnéticas (TEMPEST)			1%
Implementos instalación internet	[E.23] Errores de mantenimiento / actualización de equipos	10%		
Implementos instalación internet	[E.25] Perdida de equipos	100 %		50%
Implementos instalación internet	[A.11] Acceso no autorizado	10%	10%	50%
Implementos instalación internet	[A.23] Manipulación de hardware	100 %		50%
Implementos instalación internet	[A.24] Denegación de servicio	100 %		
Implementos instalación internet	[A.25] Robo de equipos	100 %		50%
Implementos instalación internet	[A.26] Ataque destructivo	100 %		
OLT	[N.1] Fuego	100 %		
OLT	[N.2] Daños por agua	50%		
OLT	[N] Desastres naturales	100 %		
OLT	[I.*] Desastres industriales	100 %		
OLT	[1.3] Contaminación medioambiental	50%		
OLT	[I.4] Contaminación electromagnética	10%		
OLT	[1.5.2] Avería de origen físico	50%		
OLT	[I.6] Corte del suministro eléctrico	100 %		
OLT	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %		
OLT	[I.11] Emanaciones electromagnéticas (TEMPEST)			1%
OLT	[E.23] Errores de mantenimiento / actualización de equipos	10%	10%	50%
OLT	[E.25] Perdida de equipos	100 %		100 %
OLT	[A.11] Acceso no autorizado	10%	100 %	100 %
OLT	[A.23] Manipulación de hardware	50%		50%
OLT	[A.24] Denegación de servicio	100 %		
OLT	[A.25] Robo de equipos	100 %		100 %
OLT	[A.26] Ataque destructivo	100 %		

Unidades de almacenamiento	[N.1] Fuego	100 %		
Unidades de almacenamiento	[N.2] Daños por agua	50%		
Unidades de almacenamiento	[N] Desastres naturales	100 %		
Unidades de almacenamiento	[I.*] Desastres industriales	100 %		
Unidades de almacenamiento	[1.3] Contaminación medioambiental	50%		
Unidades de almacenamiento	[I.4] Contaminación electromagnética	10%		
Unidades de almacenamiento	[1.5.2] Avería de origen físico	50%		
Unidades de almacenamiento	[I.6] Corte del suministro eléctrico	100 %		
Unidades de almacenamiento	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %		
Unidades de almacenamiento	[I.11] Emanaciones electromagnéticas (TEMPEST)			1%
Unidades de almacenamiento	[E.23] Errores de mantenimiento / actualización de equipos	10%	10%	50%
Unidades de almacenamiento	[E.25] Perdida de equipos	100 %		100 %
Unidades de almacenamiento	[A.11] Acceso no autorizado	10%	100 %	100 %
Unidades de almacenamiento	[A.23] Manipulación de hardware	50%		50%
Unidades de almacenamiento	[A.24] Denegación de servicio	100 %		
Unidades de almacenamiento	[A.25] Robo de equipos	100 %		100 %
Unidades de almacenamiento	[A.26] Ataque destructivo	100 %		
	Comunicaciones			
Teléfonos	[I.8] Fallo de servicios de comunicación	50%		
Teléfonos	[E.2] Errores del administrador del sistema / de la seguridad	20%	20%	20%
Teléfonos	[E.24] Caída del sistema por agotamiento de recursos	50%		
Teléfonos	[A.7] Uso no previsto	10%	10%	10%
Teléfonos	[A.18] Destrucción de la información	50%		
Teléfonos	[A.24] Denegación de servicio	50%		
	Auxiliares			
Escaleras	[N.1] Fuego	100 %		
Escaleras	[N.2] Daños por agua	50%		
Escaleras	[N] Desastres naturales	100 %		

Escaleras	[I.*] Desastres industriales	100%		
Escaleras	[1.3] Contaminación medioambiental	50%		
Escaleras	[I.4] Contaminación electromagnética	100%		
Escaleras	[1.5.2] Avería de origen físico	50%		
Escaleras	[I.6] Corte del suministro eléctrico	10%		
Escaleras	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Escaleras	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Escaleras	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Escaleras	[E.25] Perdida de equipos	10%		
Escaleras	[A.11] Acceso no autorizado	10%		50%
Escaleras	[A.23] Manipulación de hardware	10%		
Escaleras	[A.24] Denegación de servicio	10%		50%
Escaleras	[A.25] Robo de equipos	10%		
Escaleras	[A.26] Ataque destructivo	10%		
Generadores	[N.1] Fuego	100%		
Generadores	[N.2] Daños por agua	50%		
Generadores	[N] Desastres naturales	100%		
Generadores	[I.*] Desastres industriales	100%		
Generadores	[1.3] Contaminación medioambiental	50%		
Generadores	[I.4] Contaminación electromagnética	100%		
Generadores	[1.5.2] Avería de origen físico	50%		
Generadores	[I.6] Corte del suministro eléctrico	10%		
Generadores	[I.7] Condiciones inadecuadas de temperatura o humedad	50%		
Generadores	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		
Generadores	[E.23] Errores de mantenimiento / actualización de equipos	100%		
Generadores	[E.25] Perdida de equipos	100%		
Generadores	[A.11] Acceso no autorizado			
Generadores	[A.23] Manipulación de hardware	50%		
Generadores	[A.24] Denegación de servicio	10%		
Generadores	[A.25] Robo de equipos	50%		
Generadores	[A.26] Ataque destructivo	50%		
Sillas	[N.1] Fuego	100%		
Sillas	[N.2] Daños por agua	50%		

Sillas	[N] Desastres naturales	100 %	
Sillas	[I.*] Desastres industriales	100 %	
Sillas	[1.3] Contaminación medioambiental	50%	
Sillas	[I.4] Contaminación electromagnética	100 %	
Sillas	[1.5.2] Avería de origen físico	50%	
Sillas	[I.6] Corte del suministro eléctrico	10%	
Sillas	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %	
Sillas	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%	
Sillas	[E.23] Errores de mantenimiento / actualización de equipos	100 %	
Sillas	[E.25] Perdida de equipos	50%	
Sillas	[A.11] Acceso no autorizado	10%	
Sillas	[A.23] Manipulación de hardware	50%	50%
Sillas	[A.24] Denegación de servicio		
Sillas	[A.25] Robo de equipos	10%	50%
Sillas	[A.26] Ataque destructivo	10%	
Balanzas	[N.1] Fuego	100 %	
Balanzas	[N.2] Daños por agua	50%	
Balanzas	[N] Desastres naturales	100 %	
Balanzas	[I.*] Desastres industriales	100 %	
Balanzas	[1.3] Contaminación medioambiental	50%	
Balanzas	[I.4] Contaminación electromagnética	100 %	
Balanzas	[1.5.2] Avería de origen físico	50%	
Balanzas	[I.6] Corte del suministro eléctrico	10%	
Balanzas	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %	
Balanzas	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%	
Balanzas	[E.23] Errores de mantenimiento / actualización de equipos	100 %	
Balanzas	[E.25] Perdida de equipos	50%	
Balanzas	[A.11] Acceso no autorizado	10%	
Balanzas	[A.23] Manipulación de hardware	50%	50%
Balanzas	[A.24] Denegación de servicio		
Balanzas	[A.25] Robo de equipos	10%	50%
Balanzas	[A.26] Ataque destructivo	10%	
Camilla	[N.1] Fuego	100 %	

Camilla	[N.2] Daños por agua	50%	
Camilla	[N] Desastres naturales	100 %	
Camilla	[I.*] Desastres industriales	100 %	
Camilla	[1.3] Contaminación medioambiental	50%	
Camilla	[I.4] Contaminación electromagnética	100 %	
Camilla	[1.5.2] Avería de origen físico	50%	
Camilla	[I.6] Corte del suministro eléctrico	10%	
Camilla	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %	
Camilla	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%	
Camilla	[E.23] Errores de mantenimiento / actualización de equipos	100 %	
Camilla	[E.25] Perdida de equipos	50%	
Camilla	[A.11] Acceso no autorizado	10%	
Camilla	[A.23] Manipulación de hardware	50%	50%
Camilla	[A.24] Denegación de servicio		
Camilla	[A.25] Robo de equipos	10%	50%
Camilla	[A.26] Ataque destructivo	10%	
Linternas	[N.1] Fuego	100 %	
Linternas	[N.2] Daños por agua	50%	
Linternas	[N] Desastres naturales	100 %	
Linternas	[I.*] Desastres industriales	100 %	
Linternas	[1.3] Contaminación medioambiental	50%	
Linternas	[I.4] Contaminación electromagnética	100 %	
Linternas	[1.5.2] Avería de origen físico	50%	
Linternas	[I.6] Corte del suministro eléctrico	10%	
Linternas	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %	
Linternas	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%	
Linternas	[E.23] Errores de mantenimiento / actualización de equipos	100 %	
Linternas	[E.25] Perdida de equipos	50%	
Linternas	[A.11] Acceso no autorizado	10%	
Linternas	[A.23] Manipulación de hardware	50%	50%
Linternas	[A.24] Denegación de servicio		
Linternas	[A.25] Robo de equipos	10%	50%
Linternas	[A.26] Ataque destructivo	10%	

Perforadoras	[N.1] Fuego	100 %	
Perforadoras	[N.2] Daños por agua	50%	
Perforadoras	[N] Desastres naturales	100 %	
Perforadoras	[I.*] Desastres industriales	100 %	
Perforadoras	[1.3] Contaminación medioambiental	50%	
Perforadoras	[I.4] Contaminación electromagnética	100 %	
Perforadoras	[1.5.2] Avería de origen físico	50%	
Perforadoras	[I.6] Corte del suministro eléctrico	10%	
Perforadoras	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %	
Perforadoras	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%	
Perforadoras	[E.23] Errores de mantenimiento / actualización de equipos	100 %	
Perforadoras	[E.25] Perdida de equipos	50%	
Perforadoras	[A.11] Acceso no autorizado	10%	
Perforadoras	[A.23] Manipulación de hardware	50%	50%
Perforadoras	[A.24] Denegación de servicio		
Perforadoras	[A.25] Robo de equipos	10%	50%
Perforadoras	[A.26] Ataque destructivo	10%	
Recogedores	[N.1] Fuego	100 %	
Recogedores	[N.2] Daños por agua	50%	
Recogedores	[N] Desastres naturales	100 %	
Recogedores	[I.*] Desastres industriales	100 %	
Recogedores	[1.3] Contaminación medioambiental	50%	
Recogedores	[I.4] Contaminación electromagnética	100 %	
Recogedores	[1.5.2] Avería de origen físico	50%	
Recogedores	[I.6] Corte del suministro eléctrico	10%	
Recogedores	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %	
Recogedores	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%	
Recogedores	[E.23] Errores de mantenimiento / actualización de equipos	100 %	
Recogedores	[E.25] Perdida de equipos	50%	
Recogedores	[A.11] Acceso no autorizado	10%	
Recogedores	[A.23] Manipulación de hardware	50%	50%
Recogedores	[A.24] Denegación de servicio		
Recogedores	[A.25] Robo de equipos	10%	50%

Recogedores	[A.26] Ataque destructivo	10%	
Regletas	[N.1] Fuego	100 %	
Regletas	[N.2] Daños por agua	50%	
Regletas	[N] Desastres naturales	100 %	
Regletas	[I.*] Desastres industriales	100 %	
Regletas	[1.3] Contaminación medioambiental	50%	
Regletas	[I.4] Contaminación electromagnética	100 %	
Regletas	[1.5.2] Avería de origen físico	50%	
Regletas	[I.6] Corte del suministro eléctrico	10%	
Regletas	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %	
Regletas	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%	
Regletas	[E.23] Errores de mantenimiento / actualización de equipos	100 %	
Regletas	[E.25] Perdida de equipos	50%	
Regletas	[A.11] Acceso no autorizado	10%	
Regletas	[A.23] Manipulación de hardware	50%	50%
Regletas	[A.24] Denegación de servicio		
Regletas	[A.25] Robo de equipos	10%	50%
Regletas	[A.26] Ataque destructivo	10%	
Pizarrones	[N.1] Fuego	100 %	
Pizarrones	[N.2] Daños por agua	50%	
Pizarrones	[N] Desastres naturales	100 %	
Pizarrones	[I.*] Desastres industriales	100 %	
Pizarrones	[1.3] Contaminación medioambiental	50%	
Pizarrones	[I.4] Contaminación electromagnética	100 %	
Pizarrones	[1.5.2] Avería de origen físico	50%	
Pizarrones	[I.6] Corte del suministro eléctrico	10%	
Pizarrones	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %	
Pizarrones	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%	
Pizarrones	[E.23] Errores de mantenimiento / actualización de equipos	100 %	
Pizarrones	[E.25] Perdida de equipos	50%	
Pizarrones	[A.11] Acceso no autorizado	10%	
Pizarrones	[A.23] Manipulación de hardware	50%	50%
Pizarrones	[A.24] Denegación de servicio		

Pizarrones	[A.25] Robo de equipos	10%		50%
Pizarrones	[A.26] Ataque destructivo	10%		
Sellos de oficina	[N.1] Fuego	100 %		
Sellos de oficina	[N.2] Daños por agua	50%		
Sellos de oficina	[N] Desastres naturales	100 %		
Sellos de oficina	[I.*] Desastres industriales	100 %		
Sellos de oficina	[1.3] Contaminación medioambiental	50%		
Sellos de oficina	[I.4] Contaminación electromagnética	100 %		
Sellos de oficina	[1.5.2] Avería de origen físico	50%		
Sellos de oficina	[I.6] Corte del suministro eléctrico	10%		
Sellos de oficina	[I.7] Condiciones inadecuadas de temperatura o humedad	100 %		
Sellos de oficina	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		
Sellos de oficina	[E.23] Errores de mantenimiento / actualización de equipos	100 %		
Sellos de oficina	[E.25] Perdida de equipos	50%		
Sellos de oficina	[A.11] Acceso no autorizado	10%		
Sellos de oficina	[A.23] Manipulación de hardware	50%		50%
Sellos de oficina	[A.24] Denegación de servicio			
Sellos de oficina	[A.25] Robo de equipos	10%		50%
Sellos de oficina	[A.26] Ataque destructivo	10%		
Microondas	[N.1] Fuego	100 %		
Microondas	[N.2] Daños por agua	50%		
Microondas	[N] Desastres naturales	100 %		
Microondas	[I.*] Desastres industriales	100 %		
Microondas	[1.3] Contaminación medioambiental	50%		
Microondas	[I.4] Contaminación electromagnética	100 %		
Microondas	[1.5.2] Avería de origen físico	50%		
Microondas	[I.6] Corte del suministro eléctrico	10%		
Microondas	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Microondas	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Microondas	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Microondas	[E.25] Perdida de equipos	10%		
Microondas	[A.11] Acceso no autorizado	50%		
Microondas	[A.23] Manipulación de hardware	10%		

Microondas	[A.24] Denegación de servicio	50%	1%	1%
Microondas	[A.25] Robo de equipos	50%		50%
Microondas	[A.26] Ataque destructivo	10%		50%
Microcomponentes	[N.1] Fuego	100 %		
Microcomponentes	[N.2] Daños por agua	50%		
Microcomponentes	[N] Desastres naturales	100 %		
Microcomponentes	[I.*] Desastres industriales	100 %		
Microcomponentes	[1.3] Contaminación medioambiental	50%		
Microcomponentes	[I.4] Contaminación electromagnética	100 %		
Microcomponentes	[1.5.2] Avería de origen físico	50%		
Microcomponentes	[I.6] Corte del suministro eléctrico	10%		
Microcomponentes	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Microcomponentes	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Microcomponentes	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Microcomponentes	[E.25] Perdida de equipos	10%		
Microcomponentes	[A.11] Acceso no autorizado	50%		
Microcomponentes	[A.23] Manipulación de hardware	10%		
Microcomponentes	[A.24] Denegación de servicio	50%	1%	1%
Microcomponentes	[A.25] Robo de equipos	50%		50%
Microcomponentes	[A.26] Ataque destructivo	10%		50%
Lectores de barras	[N.1] Fuego	100 %		
Lectores de barras	[N.2] Daños por agua	50%		
Lectores de barras	[N] Desastres naturales	100 %		
Lectores de barras	[I.*] Desastres industriales	100 %		
Lectores de barras	[1.3] Contaminación medioambiental	50%		
Lectores de barras	[I.4] Contaminación electromagnética	100 %		
Lectores de barras	[1.5.2] Avería de origen físico	50%		
Lectores de barras	[I.6] Corte del suministro eléctrico	10%		
Lectores de barras	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Lectores de barras	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Lectores de barras	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Lectores de barras	[E.25] Perdida de equipos	10%		
Lectores de barras	[A.11] Acceso no autorizado	50%		

Lectores de barras	[A.23] Manipulación de hardware	10%		
Lectores de barras	[A.24] Denegación de servicio	50%	1%	1%
Lectores de barras	[A.25] Robo de equipos	50%		50%
Lectores de barras	[A.26] Ataque destructivo	10%		50%
Dispensador de agua	[N.1] Fuego	100 %		
Dispensador de agua	[N.2] Daños por agua	50%		
Dispensador de agua	[N] Desastres naturales	100 %		
Dispensador de agua	[I.*] Desastres industriales	100 %		
Dispensador de agua	[1.3] Contaminación medioambiental	50%		
Dispensador de agua	[I.4] Contaminación electromagnética	100 %		
Dispensador de agua	[1.5.2] Avería de origen físico	50%		
Dispensador de agua	[I.6] Corte del suministro eléctrico	10%		
Dispensador de agua	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Dispensador de agua	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Dispensador de agua	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Dispensador de agua	[E.25] Perdida de equipos	10%		
Dispensador de agua	[A.11] Acceso no autorizado	50%		
Dispensador de agua	[A.23] Manipulación de hardware	10%		
Dispensador de agua	[A.24] Denegación de servicio	50%	1%	1%
Dispensador de agua	[A.25] Robo de equipos	50%		50%
Dispensador de agua	[A.26] Ataque destructivo	10%		50%
Mostradores de vidrio	[N.1] Fuego	100 %		
Mostradores de vidrio	[N.2] Daños por agua	50%		
Mostradores de vidrio	[N] Desastres naturales	100 %		
Mostradores de vidrio	[I.*] Desastres industriales	100 %		
Mostradores de vidrio	[1.3] Contaminación medioambiental	50%		
Mostradores de vidrio	[I.4] Contaminación electromagnética	100 %		
Mostradores de vidrio	[1.5.2] Avería de origen físico	50%		
Mostradores de vidrio	[I.6] Corte del suministro eléctrico	10%		
Mostradores de vidrio	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Mostradores de vidrio	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Mostradores de vidrio	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Mostradores de vidrio	[E.25] Perdida de equipos	10%		

Mostradores de vidrio	[A.11] Acceso no autorizado	50%		
Mostradores de vidrio	[A.23] Manipulación de hardware	10%		
Mostradores de vidrio	[A.24] Denegación de servicio	50%	1%	1%
Mostradores de vidrio	[A.25] Robo de equipos	50%		50%
Mostradores de vidrio	[A.26] Ataque destructivo	10%		50%
Parlantes	[N.1] Fuego	100 %		
Parlantes	[N.2] Daños por agua	50%		
Parlantes	[N] Desastres naturales	100 %		
Parlantes	[I.*] Desastres industriales	100 %		
Parlantes	[1.3] Contaminación medioambiental	50%		
Parlantes	[I.4] Contaminación electromagnética	100 %		
Parlantes	[1.5.2] Avería de origen físico	50%		
Parlantes	[I.6] Corte del suministro eléctrico	10%		
Parlantes	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Parlantes	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Parlantes	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Parlantes	[E.25] Perdida de equipos	10%		
Parlantes	[A.11] Acceso no autorizado	50%		
Parlantes	[A.23] Manipulación de hardware	10%		
Parlantes	[A.24] Denegación de servicio	50%	1%	1%
Parlantes	[A.25] Robo de equipos	50%		50%
Parlantes	[A.26] Ataque destructivo	10%		50%
Copiadoras	[N.1] Fuego	100 %		
Copiadoras	[N.2] Daños por agua	50%		
Copiadoras	[N] Desastres naturales	100 %		
Copiadoras	[I.*] Desastres industriales	100 %		
Copiadoras	[1.3] Contaminación medioambiental	50%		
Copiadoras	[I.4] Contaminación electromagnética	100 %		
Copiadoras	[1.5.2] Avería de origen físico	50%		
Copiadoras	[I.6] Corte del suministro eléctrico	10%		
Copiadoras	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Copiadoras	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Copiadoras	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%

Copiadoras	[E.25] Perdida de equipos	10%		
Copiadoras	[A.11] Acceso no autorizado	50%		
Copiadoras	[A.23] Manipulación de hardware	10%		
Copiadoras	[A.24] Denegación de servicio	50%	1%	1%
Copiadoras	[A.25] Robo de equipos	50%		50%
Copiadoras	[A.26] Ataque destructivo	10%		50%
Extintores	[N.1] Fuego	100 %		
Extintores	[N.2] Daños por agua	50%		
Extintores	[N] Desastres naturales	100 %		
Extintores	[I.*] Desastres industriales	100 %		
Extintores	[1.3] Contaminación medioambiental	50%		
Extintores	[I.4] Contaminación electromagnética	100 %		
Extintores	[1.5.2] Avería de origen físico	50%		
Extintores	[I.6] Corte del suministro eléctrico	10%		
Extintores	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Extintores	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Extintores	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Extintores	[E.25] Perdida de equipos	10%		
Extintores	[A.11] Acceso no autorizado	50%		
Extintores	[A.23] Manipulación de hardware	10%		
Extintores	[A.24] Denegación de servicio	50%	1%	1%
Extintores	[A.25] Robo de equipos	50%		50%
Extintores	[A.26] Ataque destructivo	10%		50%
Casilleros metálicos	[N.1] Fuego	10%		
Casilleros metálicos	[N.2] Daños por agua	10%		
Casilleros metálicos	[N] Desastres naturales	10%		
Casilleros metálicos	[I.*] Desastres industriales	10%		
Casilleros metálicos	[1.3] Contaminación medioambiental	10%		
Casilleros metálicos	[I.4] Contaminación electromagnética	10%		
Casilleros metálicos	[1.5.2] Avería de origen físico	10%		
Casilleros metálicos	[I.6] Corte del suministro eléctrico	10%		
Casilleros metálicos	[I.7] Condiciones inadecuadas de temperatura o humedad	10%		
Casilleros metálicos	[I.11] Emanaciones electromagnéticas (TEMPEST)	10%		
Casilleros metálicos	[E.23] Errores de mantenimiento / actualización de equipos	10%		
Casilleros metálicos	[E.25] Perdida de equipos	10%		
Casilleros metálicos	[A.11] Acceso no autorizado	10%		

Casilleros metálicos	[A.23] Manipulación de hardware	10%		
Casilleros metálicos	[A.24] Denegación de servicio	10%		
Casilleros metálicos	[A.25] Robo de equipos	10%		
Casilleros metálicos	[A.26] Ataque destructivo	10%		
Data Fast	[N.1] Fuego	100 %		
Data Fast	[N.2] Daños por agua	50%		
Data Fast	[N] Desastres naturales	100 %		
Data Fast	[I.*] Desastres industriales	100 %		
Data Fast	[1.3] Contaminación medioambiental	50%		
Data Fast	[I.4] Contaminación electromagnética	100 %		
Data Fast	[1.5.2] Avería de origen físico	50%		
Data Fast	[I.6] Corte del suministro eléctrico	10%		
Data Fast	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Data Fast	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Data Fast	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Data Fast	[E.25] Perdida de equipos	10%		
Data Fast	[A.11] Acceso no autorizado	50%		
Data Fast	[A.23] Manipulación de hardware	10%		
Data Fast	[A.24] Denegación de servicio	50%	1%	1%
Data Fast	[A.25] Robo de equipos	50%		50%
Data Fast	[A.26] Ataque destructivo	10%		50%
Arnés reforzado	[N.1] Fuego	100 %		
Arnés reforzado	[N.2] Daños por agua	50%		
Arnés reforzado	[N] Desastres naturales	100 %		
Arnés reforzado	[I.*] Desastres industriales	100 %		
Arnés reforzado	[1.3] Contaminación medioambiental	50%		
Arnés reforzado	[I.4] Contaminación electromagnética	100 %		
Arnés reforzado	[1.5.2] Avería de origen físico	50%		
Arnés reforzado	[I.6] Corte del suministro eléctrico	10%		
Arnés reforzado	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Arnés reforzado	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Arnés reforzado	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Arnés reforzado	[E.25] Perdida de equipos	10%		

Arnés reforzado	[A.11] Acceso no autorizado	50%		
Arnés reforzado	[A.23] Manipulación de hardware	10%		
Arnés reforzado	[A.24] Denegación de servicio	50%	1%	1%
Arnés reforzado	[A.25] Robo de equipos	50%		50%
Arnés reforzado	[A.26] Ataque destructivo	10%		50%
Cascos	[N.1] Fuego	100 %		
Cascos	[N.2] Daños por agua	50%		
Cascos	[N] Desastres naturales	100 %		
Cascos	[I.*] Desastres industriales	100 %		
Cascos	[1.3] Contaminación medioambiental	50%		
Cascos	[I.4] Contaminación electromagnética	100 %		
Cascos	[1.5.2] Avería de origen físico	50%		
Cascos	[I.6] Corte del suministro eléctrico	10%		
Cascos	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Cascos	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Cascos	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Cascos	[E.25] Perdida de equipos	10%		
Cascos	[A.11] Acceso no autorizado	50%		
Cascos	[A.23] Manipulación de hardware	10%		
Cascos	[A.24] Denegación de servicio	50%	1%	1%
Cascos	[A.25] Robo de equipos	50%		50%
Cascos	[A.26] Ataque destructivo	10%		50%
Cinturones	[N.1] Fuego	100 %		
Cinturones	[N.2] Daños por agua	50%		
Cinturones	[N] Desastres naturales	100 %		
Cinturones	[I.*] Desastres industriales	100 %		
Cinturones	[1.3] Contaminación medioambiental	50%		
Cinturones	[I.4] Contaminación electromagnética	100 %		
Cinturones	[1.5.2] Avería de origen físico	50%		
Cinturones	[I.6] Corte del suministro eléctrico	10%		
Cinturones	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Cinturones	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Cinturones	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%

Cinturones	[E.25] Perdida de equipos	10%		
Cinturones	[A.11] Acceso no autorizado	50%		
Cinturones	[A.23] Manipulación de hardware	10%		
Cinturones	[A.24] Denegación de servicio	50%	1%	1%
Cinturones	[A.25] Robo de equipos	50%		50%
Cinturones	[A.26] Ataque destructivo	10%		50%
Eslinga	[N.1] Fuego	100 %		
Eslinga	[N.2] Daños por agua	50%		
Eslinga	[N] Desastres naturales	100 %		
Eslinga	[I.*] Desastres industriales	100 %		
Eslinga	[1.3] Contaminación medioambiental	50%		
Eslinga	[I.4] Contaminación electromagnética	100 %		
Eslinga	[1.5.2] Avería de origen físico	50%		
Eslinga	[I.6] Corte del suministro eléctrico	10%		
Eslinga	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Eslinga	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Eslinga	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Eslinga	[E.25] Perdida de equipos	10%		
Eslinga	[A.11] Acceso no autorizado	50%		
Eslinga	[A.23] Manipulación de hardware	10%		
Eslinga	[A.24] Denegación de servicio	50%	1%	1%
Eslinga	[A.25] Robo de equipos	50%		50%
Eslinga	[A.26] Ataque destructivo	10%		50%
Gafas	[N.1] Fuego	100 %		
Gafas	[N.2] Daños por agua	50%		
Gafas	[N] Desastres naturales	100 %		
Gafas	[I.*] Desastres industriales	100 %		
Gafas	[1.3] Contaminación medioambiental	50%		
Gafas	[I.4] Contaminación electromagnética	100 %		
Gafas	[1.5.2] Avería de origen físico	50%		
Gafas	[I.6] Corte del suministro eléctrico	10%		
Gafas	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Gafas	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%

Gafas	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Gafas	[E.25] Perdida de equipos	10%		
Gafas	[A.11] Acceso no autorizado	50%		
Gafas	[A.23] Manipulación de hardware	10%		
Gafas	[A.24] Denegación de servicio	50%	1%	1%
Gafas	[A.25] Robo de equipos	50%		50%
Gafas	[A.26] Ataque destructivo	10%		50%
Guantes	[N.1] Fuego	100 %		
Guantes	[N.2] Daños por agua	50%		
Guantes	[N] Desastres naturales	100 %		
Guantes	[I.*] Desastres industriales	100 %		
Guantes	[1.3] Contaminación medioambiental	50%		
Guantes	[I.4] Contaminación electromagnética	100 %		
Guantes	[1.5.2] Avería de origen físico	50%		
Guantes	[I.6] Corte del suministro eléctrico	10%		
Guantes	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Guantes	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Guantes	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Guantes	[E.25] Perdida de equipos	10%		
Guantes	[A.11] Acceso no autorizado	50%		
Guantes	[A.23] Manipulación de hardware	10%		
Guantes	[A.24] Denegación de servicio	50%	1%	1%
Guantes	[A.25] Robo de equipos	50%		50%
Guantes	[A.26] Ataque destructivo	10%		50%
Mosquetón	[N.1] Fuego	100 %		
Mosquetón	[N.2] Daños por agua	50%		
Mosquetón	[N] Desastres naturales	100 %		
Mosquetón	[I.*] Desastres industriales	100 %		
Mosquetón	[1.3] Contaminación medioambiental	50%		
Mosquetón	[I.4] Contaminación electromagnética	100 %		
Mosquetón	[1.5.2] Avería de origen físico	50%		
Mosquetón	[I.6] Corte del suministro eléctrico	10%		
Mosquetón	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%

Mosquetón	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Mosquetón	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Mosquetón	[E.25] Perdida de equipos	10%		
Mosquetón	[A.11] Acceso no autorizado	50%		
Mosquetón	[A.23] Manipulación de hardware	10%		
Mosquetón	[A.24] Denegación de servicio	50%	1%	1%
Mosquetón	[A.25] Robo de equipos	50%		50%
Mosquetón	[A.26] Ataque destructivo	10%		50%
Chalecos de seguridad	[N.1] Fuego	100 %		
Chalecos de seguridad	[N.2] Daños por agua	50%		
Chalecos de seguridad	[N] Desastres naturales	100 %		
Chalecos de seguridad	[I.*] Desastres industriales	100 %		
Chalecos de seguridad	[1.3] Contaminación medioambiental	50%		
Chalecos de seguridad	[I.4] Contaminación electromagnética	100 %		
Chalecos de seguridad	[1.5.2] Avería de origen físico	50%		
Chalecos de seguridad	[I.6] Corte del suministro eléctrico	10%		
Chalecos de seguridad	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Chalecos de seguridad	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Chalecos de seguridad	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Chalecos de seguridad	[E.25] Perdida de equipos	10%		
Chalecos de seguridad	[A.11] Acceso no autorizado	50%		
Chalecos de seguridad	[A.23] Manipulación de hardware	10%		
Chalecos de seguridad	[A.24] Denegación de servicio	50%	1%	1%
Chalecos de seguridad	[A.25] Robo de equipos	50%		50%
Chalecos de seguridad	[A.26] Ataque destructivo	10%		50%
Conos de seguridad	[N.1] Fuego	100 %		
Conos de seguridad	[N.2] Daños por agua	50%		
Conos de seguridad	[N] Desastres naturales	100 %		
Conos de seguridad	[I.*] Desastres industriales	100 %		
Conos de seguridad	[1.3] Contaminación medioambiental	50%		
Conos de seguridad	[I.4] Contaminación electromagnética	100 %		
Conos de seguridad	[1.5.2] Avería de origen físico	50%		
Conos de seguridad	[I.6] Corte del suministro eléctrico	10%		

Conos de seguridad	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Conos de seguridad	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Conos de seguridad	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Conos de seguridad	[E.25] Perdida de equipos	10%		
Conos de seguridad	[A.11] Acceso no autorizado	50%		
Conos de seguridad	[A.23] Manipulación de hardware	10%		
Conos de seguridad	[A.24] Denegación de servicio	50%	1%	1%
Conos de seguridad	[A.25] Robo de equipos	50%		50%
Conos de seguridad	[A.26] Ataque destructivo	10%		50%
Letreros de advertencia	[N.1] Fuego	100 %		
Letreros de advertencia	[N.2] Daños por agua	50%		
Letreros de advertencia	[N] Desastres naturales	100 %		
Letreros de advertencia	[I.*] Desastres industriales	100 %		
Letreros de advertencia	[1.3] Contaminación medioambiental	50%		
Letreros de advertencia	[I.4] Contaminación electromagnética	100 %		
Letreros de advertencia	[1.5.2] Avería de origen físico	50%		
Letreros de advertencia	[I.6] Corte del suministro eléctrico	10%		
Letreros de advertencia	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Letreros de advertencia	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Letreros de advertencia	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Letreros de advertencia	[E.25] Perdida de equipos	10%		
Letreros de advertencia	[A.11] Acceso no autorizado	50%		
Letreros de advertencia	[A.23] Manipulación de hardware	10%		
Letreros de advertencia	[A.24] Denegación de servicio	50%	1%	1%
Letreros de advertencia	[A.25] Robo de equipos	50%		50%
Letreros de advertencia	[A.26] Ataque destructivo	10%		50%
Herramientas	[N.1] Fuego	100 %		
Herramientas	[N.2] Daños por agua	50%		
Herramientas	[N] Desastres naturales	100 %		
Herramientas	[I.*] Desastres industriales	100 %		
Herramientas	[1.3] Contaminación medioambiental	50%		
Herramientas	[I.4] Contaminación electromagnética	100 %		
Herramientas	[1.5.2] Avería de origen físico	50%		

Herramientas	[I.6] Corte del suministro eléctrico	10%		
Herramientas	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Herramientas	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Herramientas	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Herramientas	[E.25] Perdida de equipos	10%		
Herramientas	[A.11] Acceso no autorizado	50%		
Herramientas	[A.23] Manipulación de hardware	10%		
Herramientas	[A.24] Denegación de servicio	50%	1%	1%
Herramientas	[A.25] Robo de equipos	50%		50%
Herramientas	[A.26] Ataque destructivo	10%		50%
Case para discos duros	[N.1] Fuego	100 %		
Case para discos duros	[N.2] Daños por agua	50%		
Case para discos duros	[N] Desastres naturales	100 %		
Case para discos duros	[I.*] Desastres industriales	100 %		
Case para discos duros	[1.3] Contaminación medioambiental	50%		
Case para discos duros	[I.4] Contaminación electromagnética	100 %		
Case para discos duros	[1.5.2] Avería de origen físico	50%		
Case para discos duros	[I.6] Corte del suministro eléctrico	10%		
Case para discos duros	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Case para discos duros	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Case para discos duros	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Case para discos duros	[E.25] Perdida de equipos	10%		
Case para discos duros	[A.11] Acceso no autorizado	50%		
Case para discos duros	[A.23] Manipulación de hardware	10%		
Case para discos duros	[A.24] Denegación de servicio	50%	1%	1%
Case para discos duros	[A.25] Robo de equipos	50%		50%
Case para discos duros	[A.26] Ataque destructivo	10%		50%
Apple pencil	[N.1] Fuego	100 %		
Apple pencil	[N.2] Daños por agua	50%		
Apple pencil	[N] Desastres naturales	100 %		
Apple pencil	[I.*] Desastres industriales	100 %		
Apple pencil	[1.3] Contaminación medioambiental	50%		
Apple pencil	[I.4] Contaminación electromagnética	100 %		

Apple pencil	[1.5.2] Avería de origen físico	50%		
Apple pencil	[I.6] Corte del suministro eléctrico	10%		
Apple pencil	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Apple pencil	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Apple pencil	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Apple pencil	[E.25] Perdida de equipos	10%		
Apple pencil	[A.11] Acceso no autorizado	50%		
Apple pencil	[A.23] Manipulación de hardware	10%		
Apple pencil	[A.24] Denegación de servicio	50%	1%	1%
Apple pencil	[A.25] Robo de equipos	50%		50%
Apple pencil	[A.26] Ataque destructivo	10%		50%
Alexa	[N.1] Fuego	100 %		
Alexa	[N.2] Daños por agua	50%		
Alexa	[N] Desastres naturales	100 %		
Alexa	[I.*] Desastres industriales	100 %		
Alexa	[1.3] Contaminación medioambiental	50%		
Alexa	[I.4] Contaminación electromagnética	100 %		
Alexa	[1.5.2] Avería de origen físico	50%		
Alexa	[I.6] Corte del suministro eléctrico	10%		
Alexa	[I.7] Condiciones inadecuadas de temperatura o humedad	50%	1%	1%
Alexa	[I.11] Emanaciones electromagnéticas (TEMPEST)	50%		50%
Alexa	[E.23] Errores de mantenimiento / actualización de equipos	10%		50%
Alexa	[E.25] Perdida de equipos	10%		
Alexa	[A.11] Acceso no autorizado	50%		
Alexa	[A.23] Manipulación de hardware	10%		
Alexa	[A.24] Denegación de servicio	50%	1%	1%
Alexa	[A.25] Robo de equipos	50%		50%
Alexa	[A.26] Ataque destructivo	10%		50%
	Servicios subcontratados/ Instalaciones			
Casa Plus 1	[N.1] Fuego	100 %		
Casa Plus 1	[N.2] Daños por agua	100 %		
Casa Plus 1	[N] Desastres naturales	100 %		
Casa Plus 1	[N.1] Fuego	100 %		

Casa Plus 1	[I.*] Desastres industriales	100%		
Casa Plus 1	[1.3] Contaminación medioambiental	100%		
Casa Plus 1	[I.4] Contaminación electromagnética	10%		
Casa Plus 1	[E.25] Perdida de equipos	10%		
Casa Plus 1	[A.6] Abuso de privilegios de acceso			10%
Casa Plus 1	[A.7] Uso no previsto	10%		
Casa Plus 1	[A.25] Robo de equipos	10%		
Casa Plus 1	[A.26] Ataque destructivo			100%
Casa Plus 1	[A.27] Ocupación enemiga	100%		
Casa Plus 2	[N.1] Fuego	100%		
Casa Plus 2	[N.2] Daños por agua	100%		
Casa Plus 2	[N] Desastres naturales	100%		
Casa Plus 2	[N.1] Fuego	100%		
Casa Plus 2	[I.*] Desastres industriales	100%		
Casa Plus 2	[1.3] Contaminación medioambiental	100%		
Casa Plus 2	[I.4] Contaminación electromagnética	100%		
Casa Plus 2	[E.25] Perdida de equipos	10%		
Casa Plus 2	[A.6] Abuso de privilegios de acceso	10%		
Casa Plus 2	[A.7] Uso no previsto			10%
Casa Plus 2	[A.25] Robo de equipos	10%		
Casa Plus 2	[A.26] Ataque destructivo	10%		
Casa Plus 2	[A.27] Ocupación enemiga			100%
	Personal			
Gerencia General	[E.15] Alteración de la información		10%	
Gerencia General	[E.18] Destrucción de información	1%		
Gerencia General	[E.19] Fuga de información			10%
Gerencia General	[E.28] Indisponibilidad de personal	10%		
Gerencia General	[A.15] Modificación de la información		50%	
Gerencia General	[A.18] Destrucción de la información	10%		
Gerencia General	[A.19] Revelación de información			50%
Gerencia General	[E.28] Indisponibilidad de personal	50%		
Gerencia General	[A.29] Extorsión	10%	20%	50%
Gerencia General	[A.30] Ingeniería Social (picaresca)	10%	20%	50%
Gerencia Operativa	[E.15] Alteración de la información	10%		

Gerencia Operativa	[E.18] Destrucción de información		10%	
Gerencia Operativa	[E.19] Fuga de información	1%		
Gerencia Operativa	[E.28] Indisponibilidad de personal			10%
Gerencia Operativa	[A.15] Modificación de la información	20%		
Gerencia Operativa	[A.18] Destrucción de la información		50%	
Gerencia Operativa	[A.19] Revelación de información	10%		
Gerencia Operativa	[E.28] Indisponibilidad de personal			50%
Gerencia Operativa	[A.29] Extorsión	50%		
Gerencia Operativa	[A.30] Ingeniería Social (picaresca)	50%	100 %	100 %
Gerencia Administrativa	[E.15] Alteración de la información		10%	
Gerencia Administrativa	[E.18] Destrucción de información	1%		
Gerencia Administrativa	[E.19] Fuga de información			10%
Gerencia Administrativa	[E.28] Indisponibilidad de personal	30%		
Gerencia Administrativa	[A.15] Modificación de la información		50%	
Gerencia Administrativa	[A.18] Destrucción de la información	10%		
Gerencia Administrativa	[A.19] Revelación de información			50%
Gerencia Administrativa	[E.28] Indisponibilidad de personal	50%		
Gerencia Administrativa	[A.29] Extorsión	20%	20%	50%
Gerencia Administrativa	[A.30] Ingeniería Social (picaresca)	20%	20%	50%
Gerencia Atención al Cliente	[E.15] Alteración de la información		10%	
Gerencia Atención al Cliente	[E.18] Destrucción de información	1%		
Gerencia Atención al Cliente	[E.19] Fuga de información			10%
Gerencia Atención al Cliente	[E.28] Indisponibilidad de personal	10%		
Gerencia Atención al Cliente	[A.15] Modificación de la información		50%	
Gerencia Atención al Cliente	[A.18] Destrucción de la información	10%		
Gerencia Atención al Cliente	[A.19] Revelación de información			20%
Gerencia Atención al Cliente	[E.28] Indisponibilidad de personal	50%		
Gerencia Atención al Cliente	[A.29] Extorsión	10%	20%	20%
Gerencia Atención al Cliente	[A.30] Ingeniería Social (picaresca)	10%	20%	20%
Gerencia comercial	[E.15] Alteración de la información		10%	
Gerencia comercial	[E.18] Destrucción de información	1%		
Gerencia comercial	[E.19] Fuga de información			10%
Gerencia comercial	[E.28] Indisponibilidad de personal	10%		
Gerencia comercial	[A.15] Modificación de la información		50%	
Gerencia comercial	[A.18] Destrucción de la información	10%		
Gerencia comercial	[A.19] Revelación de información			20%
Gerencia comercial	[E.28] Indisponibilidad de personal	50%		
Gerencia comercial	[A.29] Extorsión	10%	20%	20%
Gerencia comercial	[A.30] Ingeniería Social (picaresca)	10%	20%	20%

Nota: Elaboración Propia

Anexo 4 Peso ponderado de amenazas

Activo	Amenaza	Peso ponderado
	Datos/Información	
Base de Datos	[1.5.11 Avería de origen lógico	9
Base de Datos	[E.8] Difusión de software dañino	6,3
Base de Datos	[E.15] Alteración de la información	4
Base de Datos	[E,20] Vulnerabilidades de los programas (software)	6
Base de Datos	[E.21] Errores de mantenimiento I actualización (software)	6
Base de Datos	[A.8] Difusión de software dañino	9,3
Base de Datos	[A.22] Manipulación de programas	9
Base de Datos	[1.5.11 Avería de origen lógico	9
Base de Datos	[E.8] Difusión de software dañino	7
Base de Datos	[E.20] Vulnerabilidades de los programas (software)	6,7
Base de Datos	[E.21] Errores de mantenimiento / actualización (software)	6,7
Base de Datos	[A.8] Difusión de software dañino	10
Base de Datos	[A.221] Manipulación de programas	9,7
	Servicios	
Electricidad	[E.2] Errores del administrador del sistema / de la seguridad	6
Electricidad	[E.15] Alteración de la información	5,7
Electricidad	[E.19] Fugas de información	7
Electricidad	[A.5] Suplantación de la identidad	7,3
Electricidad	[A.6] Abuso de privilegios de acceso	6,3

Electricidad	[A.7] Uso no previsto	6
Electricidad	[A.11] Acceso no autorizado	7
Electricidad	[A.15] Modificación de la información	7
Internet	[E.1] Errores de los usuarios	6
Internet	[E.2] Errores del administrador del sistema / de la seguridad	6
Internet	[E.15] Alteración de la información	5,7
Internet	[E.19] Fugas de información	7
Internet	[A.5] Suplantación de la identidad	7,3
Internet	[A.6] Abuso de privilegios de acceso	6,3
Internet	[A.7] Uso no previsto	6
Internet	[A.11] Acceso no autorizado	7
Internet	[A.15] Modificación de la información	7
Mantenimiento	[E.1] Errores de los usuarios	6
Mantenimiento	[E.2] Errores del administrador del sistema / de la seguridad	6
Mantenimiento	[E.15] Alteración de la información	5,7
Mantenimiento	[E.19] Fugas de información	7
Mantenimiento	[A.5] Suplantación de la identidad	7,3
Mantenimiento	[A.6] Abuso de privilegios de acceso	6,3
Mantenimiento	[A.7] Uso no previsto	6
Mantenimiento	[A.11] Acceso no autorizado	7
Mantenimiento	[A.15] Modificación de la información	7

Correo	[E.1] Errores de los usuarios	6
Correo	[E.2] Errores del administrador del sistema / de la seguridad	6
Correo	[E.15] Alteración de la información	5,7
Correo	[E.19] Fugas de información	7
Correo	[A.5] Suplantación de la identidad	7,3
Correo	[A.6] Abuso de privilegios de acceso	6,3
Correo	[A.7] Uso no previsto	6
Correo	[A.11] Acceso no autorizado	7
Correo	[A.15] Modificación de la información	7
Datos de ingreso	[1.5.1] Avería de origen lógico	9
Datos de ingreso	[E.8] Difusión de software dañino	7
Datos de ingreso	[E.20] Vulnerabilidades de los programas (software)	6,7
Datos de ingreso	[E.21] Errores de mantenimiento / actualización (software)	6,7
Datos de ingreso	[A.8] Difusión de software dañino	10
Datos de ingreso	[A.221] Manipulación de programas	9,7
Detectores de humo	[1.3] Contaminación medioambiental	9
Kits de seguridad	[N] Desastres naturales	10
Kits de seguridad	[N.1] Fuego	9,7
Kits de seguridad	[A.26] Ataque destructivo	9
Sistema contable	[1.5.1] Avería de origen lógico	9
Sistema contable	[E.8] Difusión de software dañino	6,7
Sistema contable	[E.20] Vulnerabilidades de los programas (software)	6,3
Sistema contable	[E.21] Errores de mantenimiento / actualización (software)	6,3

Sistema contable	[A.8] Difusión de software dañino	9,7
Sistema contable	[A.221] Manipulación de programas	9,3
Antivirus	[1.5.1] Avería de origen lógico	9
Antivirus	[E.8] Difusión de software dañino	6,7
Antivirus	[E.20] Vulnerabilidades de los programas (software)	6,3
Antivirus	[E.21] Errores de mantenimiento / actualización (software)	6,3
Antivirus	[A.8] Difusión de software dañino	9,7
Antivirus	[A.221] Manipulación de programas	9,3
Fusionadoras	[N.1] Fuego	10
Fusionadoras	[N.2] Daños por agua	9
Fusionadoras	[N] Desastres naturales	10
Fusionadoras	[I.*] Desastres industriales	10
Fusionadoras	[1.3] Contaminación medioambiental	9
Fusionadoras	[I.4] Contaminación electromagnética	7
Fusionadoras	[1.5.2] Avería de origen físico	9
Fusionadoras	[I.6] Corte del suministro eléctrico	10
Fusionadoras	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Fusionadoras	[I.11] Emanaciones electromagnéticas (TEMPEST)	2
Fusionadoras	[E.23] Errores de mantenimiento / actualización de equipos	7
Fusionadoras	[E.25] Perdida de equipos	8,5
Fusionadoras	[A.11] Acceso no autorizado	7
Fusionadoras	[A.23] Manipulación de hardware	8
Fusionadoras	[A.24] Denegación de servicio	10

Fusionadoras	[A.25] Robo de equipos	8,5
Fusionadoras	[A.26] Ataque destructivo	10
Cargadores	[N.1] Fuego	10
Cargadores	[N.2] Daños por agua	9
Cargadores	[N] Desastres naturales	10
Cargadores	[I.*] Desastres industriales	10
Cargadores	[1.3] Contaminación medioambiental	9
Cargadores	[I.4] Contaminación electromagnética	10
Cargadores	[1.5.2] Avería de origen físico	9
Cargadores	[I.6] Corte del suministro eléctrico	7
Cargadores	[I.7] Condiciones inadecuadas de temperatura o humedad	9
Cargadores	[I.11] Emanaciones electromagnéticas (TEMPEST)	10
Cargadores	[E.23] Errores de mantenimiento / actualización de equipos	10
Cargadores	[E.25] Perdida de equipos	2
Cargadores	[A.11] Acceso no autorizado	7
Cargadores	[A.23] Manipulación de hardware	8
Cargadores	[A.24] Denegación de servicio	10
Cargadores	[A.25] Robo de equipos	5,5
Cargadores	[A.26] Ataque destructivo	10
Power Meter	[N.1] Fuego	10
Power Meter	[N.2] Daños por agua	9
Power Meter	[N] Desastres naturales	10
Power Meter	[I.*] Desastres industriales	10
Power Meter	[1.3] Contaminación medioambiental	9

Power Meter	[I.4] Contaminación electromagnética	10
Power Meter	[1.5.2] Avería de origen físico	9
Power Meter	[I.6] Corte del suministro eléctrico	7
Power Meter	[I.7] Condiciones inadecuadas de temperatura o humedad	9
Power Meter	[I.11] Emanaciones electromagnéticas (TEMPEST)	10
Power Meter	[E.23] Errores de mantenimiento / actualización de equipos	10
Power Meter	[E.25] Perdida de equipos	8,5
Power Meter	[A.11] Acceso no autorizado	7
Power Meter	[A.23] Manipulación de hardware	8,5
Power Meter	[A.24] Denegación de servicio	10
Power Meter	[A.25] Robo de equipos	8,5
Power Meter	[A.26] Ataque destructivo	10
Sacabocados	[N.1] Fuego	10
Sacabocados	[N.2] Daños por agua	9
Sacabocados	[N] Desastres naturales	10
Sacabocados	[I.*] Desastres industriales	10
Sacabocados	[1.3] Contaminación medioambiental	9
Sacabocados	[I.4] Contaminación electromagnética	10
Sacabocados	[1.5.2] Avería de origen físico	9
Sacabocados	[I.6] Corte del suministro eléctrico	7
Sacabocados	[I.7] Condiciones inadecuadas de temperatura o humedad	9
Sacabocados	[I.11] Emanaciones electromagnéticas (TEMPEST)	10
Sacabocados	[E.23] Errores de mantenimiento / actualización de equipos	10

Sacabocados	[E.25] Perdida de equipos	8,5
Sacabocados	[A.11] Acceso no autorizado	7
Sacabocados	[A.23] Manipulación de hardware	8
Sacabocados	[A.24] Denegación de servicio	10
Sacabocados	[A.25] Robo de equipos	8,5
Sacabocados	[A.26] Ataque destructivo	10
Taladros	[N.1] Fuego	10
Taladros	[N.2] Daños por agua	9
Taladros	[N] Desastres naturales	10
Taladros	[I.*] Desastres industriales	10
Taladros	[1.3] Contaminación medioambiental	9
Taladros	[I.4] Contaminación electromagnética	10
Taladros	[1.5.2] Avería de origen físico	9
Taladros	[I.6] Corte del suministro eléctrico	7
Taladros	[I.7] Condiciones inadecuadas de temperatura o humedad	9
Taladros	[I.11] Emanaciones electromagnéticas (TEMPEST)	10
Taladros	[E.23] Errores de mantenimiento / actualización de equipos	7
Taladros	[E.25] Perdida de equipos	8,5
Taladros	[A.11] Acceso no autorizado	7
Taladros	[A.23] Manipulación de hardware	8
Taladros	[A.24] Denegación de servicio	10
Taladros	[A.25] Robo de equipos	8,5
Taladros	[A.26] Ataque destructivo	10
Etiquetadoras	[N.1] Fuego	10

Etiquetadoras	[N.2] Daños por agua	9
Etiquetadoras	[N] Desastres naturales	10
Etiquetadoras	[I.*] Desastres industriales	10
Etiquetadoras	[1.3] Contaminación medioambiental	9
Etiquetadoras	[I.4] Contaminación electromagnética	7
Etiquetadoras	[1.5.2] Avería de origen físico	9
Etiquetadoras	[I.6] Corte del suministro eléctrico	10
Etiquetadoras	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Etiquetadoras	[I.11] Emanaciones electromagnéticas (TEMPEST)	2
Etiquetadoras	[E.23] Errores de mantenimiento / actualización de equipos	7
Etiquetadoras	[E.25] Perdida de equipos	8,5
Etiquetadoras	[A.11] Acceso no autorizado	7
Etiquetadoras	[A.23] Manipulación de hardware	8,5
Etiquetadoras	[A.24] Denegación de servicio	10
Etiquetadoras	[A.25] Robo de equipos	8,5
Etiquetadoras	[A.26] Ataque destructivo	10
Cámaras Web	[N.1] Fuego	10
Cámaras Web	[N.2] Daños por agua	9
Cámaras Web	[N] Desastres naturales	10
Cámaras Web	[I.*] Desastres industriales	10
Cámaras Web	[1.3] Contaminación medioambiental	9
Cámaras Web	[I.4] Contaminación electromagnética	7
Cámaras Web	[1.5.2] Avería de origen físico	9
Cámaras Web	[I.6] Corte del suministro eléctrico	10

Cámaras Web	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Cámaras Web	[I.11] Emanaciones electromagnéticas (TEMPEST)	2
Cámaras Web	[E.23] Errores de mantenimiento / actualización de equipos	7
Cámaras Web	[E.25] Perdida de equipos	9
Cámaras Web	[A.11] Acceso no autorizado	8,3
Cámaras Web	[A.23] Manipulación de hardware	8
Cámaras Web	[A.24] Denegación de servicio	10
Cámaras Web	[A.25] Robo de equipos	9
Cámaras Web	[A.26] Ataque destructivo	10
Cooler AMD	[N.1] Fuego	10
Cooler AMD	[N.2] Daños por agua	9
Cooler AMD	[N] Desastres naturales	10
Cooler AMD	[I.*] Desastres industriales	10
Cooler AMD	[1.3] Contaminación medioambiental	9
Cooler AMD	[I.4] Contaminación electromagnética	7
Cooler AMD	[1.5.2] Avería de origen físico	9
Cooler AMD	[I.6] Corte del suministro eléctrico	10
Cooler AMD	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Cooler AMD	[I.11] Emanaciones electromagnéticas (TEMPEST)	2
Cooler AMD	[E.23] Errores de mantenimiento / actualización de equipos	7
Cooler AMD	[E.25] Perdida de equipos	9
Cooler AMD	[A.11] Acceso no autorizado	8,3
Cooler AMD	[A.23] Manipulación de hardware	8

Cooler AMD	[A.24] Denegación de servicio	10
Cooler AMD	[A.25] Robo de equipos	9
Cooler AMD	[A.26] Ataque destructivo	10
CPU	[N.1] Fuego	10
CPU	[N.2] Daños por agua	9
CPU	[N] Desastres naturales	10
CPU	[I.*] Desastres industriales	10
CPU	[1.3] Contaminación medioambiental	9
CPU	[I.4] Contaminación electromagnética	7
CPU	[1.5.2] Avería de origen físico	9
CPU	[I.6] Corte del suministro eléctrico	10
CPU	[I.7] Condiciones inadecuadas de temperatura o humedad	10
CPU	[I.11] Emanaciones electromagnéticas (TEMPEST)	3
CPU	[E.23] Errores de mantenimiento / actualización de equipos	7,3
CPU	[E.25] Perdida de equipos	9,5
CPU	[A.11] Acceso no autorizado	8,7
CPU	[A.23] Manipulación de hardware	7,3
CPU	[A.24] Denegación de servicio	10
CPU	[A.25] Robo de equipos	9,5
CPU	[A.26] Ataque destructivo	10
Video Card	[N.1] Fuego	10
Video Card	[N.2] Daños por agua	9
Video Card	[N] Desastres naturales	10
Video Card	[I.*] Desastres industriales	10

Video Card	[1.3] Contaminación medioambiental	9
Video Card	[I.4] Contaminación electromagnética	7
Video Card	[1.5.2] Avería de origen físico	9
Video Card	[I.6] Corte del suministro eléctrico	10
Video Card	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Video Card	[I.11] Emanaciones electromagnéticas (TEMPEST)	2
Video Card	[E.23] Errores de mantenimiento / actualización de equipos	7
Video Card	[E.25] Perdida de equipos	8,5
Video Card	[A.11] Acceso no autorizado	7
Video Card	[A.23] Manipulación de hardware	8
Video Card	[A.24] Denegación de servicio	10
Video Card	[A.25] Robo de equipos	8,5
Video Card	[A.26] Ataque destructivo	10
Impresoras	[N.1] Fuego	10
Impresoras	[N.2] Daños por agua	9
Impresoras	[N] Desastres naturales	10
Impresoras	[I.*] Desastres industriales	10
Impresoras	[1.3] Contaminación medioambiental	9
Impresoras	[I.4] Contaminación electromagnética	7
Impresoras	[1.5.2] Avería de origen físico	9
Impresoras	[I.6] Corte del suministro eléctrico	10
Impresoras	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Impresoras	[I.11] Emanaciones electromagnéticas (TEMPEST)	2

Impresoras	[E.23] Errores de mantenimiento / actualización de equipos	7
Impresoras	[E.25] Perdida de equipos	9
Impresoras	[A.11] Acceso no autorizado	7
Impresoras	[A.23] Manipulación de hardware	8
Impresoras	[A.24] Denegación de servicio	10
Impresoras	[A.25] Robo de equipos	9
Impresoras	[A.26] Ataque destructivo	10
iPads Apple	[N.1] Fuego	10
iPads Apple	[N.2] Daños por agua	9
iPads Apple	[N] Desastres naturales	10
iPads Apple	[I.*] Desastres industriales	10
iPads Apple	[1.3] Contaminación medioambiental	9
iPads Apple	[I.4] Contaminación electromagnética	7
iPads Apple	[1.5.2] Avería de origen físico	9
iPads Apple	[I.6] Corte del suministro eléctrico	10
iPads Apple	[I.7] Condiciones inadecuadas de temperatura o humedad	10
iPads Apple	[I.11] Emanaciones electromagnéticas (TEMPEST)	2
iPads Apple	[E.23] Errores de mantenimiento / actualización de equipos	7
iPads Apple	[E.25] Perdida de equipos	9
iPads Apple	[A.11] Acceso no autorizado	8,3
iPads Apple	[A.23] Manipulación de hardware	8
iPads Apple	[A.24] Denegación de servicio	10
iPads Apple	[A.25] Robo de equipos	9

iPads Apple	[A.26] Ataque destructivo	10
MacBook Air	[N.1] Fuego	10
MacBook Air	[N.2] Daños por agua	9
MacBook Air	[N] Desastres naturales	10
MacBook Air	[I.*] Desastres industriales	10
MacBook Air	[1.3] Contaminación medioambiental	9
MacBook Air	[I.4] Contaminación electromagnética	7
MacBook Air	[1.5.2] Avería de origen físico	9
MacBook Air	[I.6] Corte del suministro eléctrico	10
MacBook Air	[I.7] Condiciones inadecuadas de temperatura o humedad	10
MacBook Air	[I.11] Emanaciones electromagnéticas (TEMPEST)	2
MacBook Air	[E.23] Errores de mantenimiento / actualización de equipos	7
MacBook Air	[E.25] Perdida de equipos	9
MacBook Air	[A.11] Acceso no autorizado	8,3
MacBook Air	[A.23] Manipulación de hardware	8,5
MacBook Air	[A.24] Denegación de servicio	10
MacBook Air	[A.25] Robo de equipos	9
MacBook Air	[A.26] Ataque destructivo	10
Monitores	[N.1] Fuego	10
Monitores	[N.2] Daños por agua	9
Monitores	[N] Desastres naturales	10
Monitores	[I.*] Desastres industriales	10
Monitores	[1.3] Contaminación medioambiental	9
Monitores	[I.4] Contaminación electromagnética	7

Monitores	[1.5.2] Avería de origen físico	9
Monitores	[I.6] Corte del suministro eléctrico	10
Monitores	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Monitores	[I.11] Emanaciones electromagnéticas (TEMPEST)	2
Monitores	[E.23] Errores de mantenimiento / actualización de equipos	7
Monitores	[E.25] Perdida de equipos	9
Monitores	[A.11] Acceso no autorizado	8,3
Monitores	[A.23] Manipulación de hardware	7
Monitores	[A.24] Denegación de servicio	10
Monitores	[A.25] Robo de equipos	9
Monitores	[A.26] Ataque destructivo	10
Mouse	[N.1] Fuego	10
Mouse	[N.2] Daños por agua	9
Mouse	[N] Desastres naturales	10
Mouse	[I.*] Desastres industriales	10
Mouse	[1.3] Contaminación medioambiental	9
Mouse	[I.4] Contaminación electromagnética	7
Mouse	[1.5.2] Avería de origen físico	9
Mouse	[I.6] Corte del suministro eléctrico	10
Mouse	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Mouse	[I.11] Emanaciones electromagnéticas (TEMPEST)	2
Mouse	[E.23] Errores de mantenimiento / actualización de equipos	7
Mouse	[E.25] Perdida de equipos	8,5

Mouse	[A.11] Acceso no autorizado	7
Mouse	[A.23] Manipulación de hardware	8
Mouse	[A.24] Denegación de servicio	10
Mouse	[A.25] Robo de equipos	8,5
Mouse	[A.26] Ataque destructivo	10
Server Dell	[N.1] Fuego	10
Server Dell	[N.2] Daños por agua	9
Server Dell	[N] Desastres naturales	10
Server Dell	[I.*] Desastres industriales	10
Server Dell	[1.3] Contaminación medioambiental	9
Server Dell	[I.4] Contaminación electromagnética	7
Server Dell	[1.5.2] Avería de origen físico	9
Server Dell	[I.6] Corte del suministro eléctrico	9
Server Dell	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Server Dell	[I.11] Emanaciones electromagnéticas (TEMPEST)	10
Server Dell	[E.23] Errores de mantenimiento / actualización de equipos	7
Server Dell	[E.25] Perdida de equipos	9
Server Dell	[A.11] Acceso no autorizado	8,3
Server Dell	[A.23] Manipulación de hardware	9
Server Dell	[A.24] Denegación de servicio	10
Server Dell	[A.25] Robo de equipos	9
Server Dell	[A.26] Ataque destructivo	10
Tablet Lenovo	[N.1] Fuego	10
Tablet Lenovo	[N.2] Daños por agua	9

Tablet Lenovo	[N] Desastres naturales	10
Tablet Lenovo	[I.*] Desastres industriales	10
Tablet Lenovo	[1.3] Contaminación medioambiental	9
Tablet Lenovo	[I.4] Contaminación electromagnética	7
Tablet Lenovo	[1.5.2] Avería de origen físico	9
Tablet Lenovo	[I.6] Corte del suministro eléctrico	10
Tablet Lenovo	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Tablet Lenovo	[I.11] Emanaciones electromagnéticas (TEMPEST)	2
Tablet Lenovo	[E.23] Errores de mantenimiento / actualización de equipos	7
Tablet Lenovo	[E.25] Perdida de equipos	9
Tablet Lenovo	[A.11] Acceso no autorizado	8,3
Tablet Lenovo	[A.23] Manipulación de hardware	8
Tablet Lenovo	[A.24] Denegación de servicio	10
Tablet Lenovo	[A.25] Robo de equipos	9
Tablet Lenovo	[A.26] Ataque destructivo	10
Teclados	[N.1] Fuego	10
Teclados	[N.2] Daños por agua	9
Teclados	[N] Desastres naturales	10
Teclados	[I.*] Desastres industriales	10
Teclados	[1.3] Contaminación medioambiental	9
Teclados	[I.4] Contaminación electromagnética	7
Teclados	[1.5.2] Avería de origen físico	9
Teclados	[I.6] Corte del suministro eléctrico	10
Teclados	[I.7] Condiciones inadecuadas de temperatura o humedad	10

Teclados	[I.11] Emanaciones electromagnéticas (TEMPEST)	2
Teclados	[E.23] Errores de mantenimiento / actualización de equipos	7
Teclados	[E.25] Perdida de equipos	8,5
Teclados	[A.11] Acceso no autorizado	7
Teclados	[A.23] Manipulación de hardware	8
Teclados	[A.24] Denegación de servicio	10
Teclados	[A.25] Robo de equipos	8,5
Teclados	[A.26] Ataque destructivo	10
TV	[N.1] Fuego	10
TV	[N.2] Daños por agua	9
TV	[N] Desastres naturales	10
TV	[I.*] Desastres industriales	10
TV	[1.3] Contaminación medioambiental	9
TV	[I.4] Contaminación electromagnética	7
TV	[1.5.2] Avería de origen físico	9
TV	[I.6] Corte del suministro eléctrico	10
TV	[I.7] Condiciones inadecuadas de temperatura o humedad	10
TV	[I.11] Emanaciones electromagnéticas (TEMPEST)	2
TV	[E.23] Errores de mantenimiento / actualización de equipos	7
TV	[E.25] Perdida de equipos	8,5
TV	[A.11] Acceso no autorizado	7
TV	[A.23] Manipulación de hardware	8
TV	[A.24] Denegación de servicio	10

TV	[A.25] Robo de equipos	8,5
TV	[A.26] Ataque destructivo	10
Amplificadores	[N.1] Fuego	10
Amplificadores	[N.2] Daños por agua	9
Amplificadores	[N] Desastres naturales	10
Amplificadores	[I.*] Desastres industriales	10
Amplificadores	[1.3] Contaminación medioambiental	9
Amplificadores	[I.4] Contaminación electromagnética	7
Amplificadores	[1.5.2] Avería de origen físico	9
Amplificadores	[I.6] Corte del suministro eléctrico	10
Amplificadores	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Amplificadores	[I.11] Emanaciones electromagnéticas (TEMPEST)	2
Amplificadores	[E.23] Errores de mantenimiento / actualización de equipos	7
Amplificadores	[E.25] Perdida de equipos	8,5
Amplificadores	[A.11] Acceso no autorizado	7
Amplificadores	[A.23] Manipulación de hardware	8
Amplificadores	[A.24] Denegación de servicio	10
Amplificadores	[A.25] Robo de equipos	8,5
Amplificadores	[A.26] Ataque destructivo	10
Aspiradores	[N.1] Fuego	10
Aspiradores	[N.2] Daños por agua	9
Aspiradores	[N] Desastres naturales	10
Aspiradores	[I.*] Desastres industriales	10
Aspiradores	[1.3] Contaminación medioambiental	9

Aspiradores	[I.4] Contaminación electromagnética	7
Aspiradores	[1.5.2] Avería de origen físico	9
Aspiradores	[I.6] Corte del suministro eléctrico	10
Aspiradores	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Aspiradores	[I.11] Emanaciones electromagnéticas (TEMPEST)	2
Aspiradores	[E.23] Errores de mantenimiento / actualización de equipos	7
Aspiradores	[E.25] Perdida de equipos	8,5
Aspiradores	[A.11] Acceso no autorizado	7
Aspiradores	[A.23] Manipulación de hardware	8
Aspiradores	[A.24] Denegación de servicio	10
Aspiradores	[A.25] Robo de equipos	8,5
Aspiradores	[A.26] Ataque destructivo	10
Lectores de huellas	[N.1] Fuego	10
Lectores de huellas	[N.2] Daños por agua	9
Lectores de huellas	[N] Desastres naturales	10
Lectores de huellas	[I.*] Desastres industriales	10
Lectores de huellas	[1.3] Contaminación medioambiental	9
Lectores de huellas	[I.4] Contaminación electromagnética	7
Lectores de huellas	[1.5.2] Avería de origen físico	9
Lectores de huellas	[I.6] Corte del suministro eléctrico	10
Lectores de huellas	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Lectores de huellas	[I.11] Emanaciones electromagnéticas (TEMPEST)	2
Lectores de huellas	[E.23] Errores de mantenimiento / actualización de equipos	7

Lectores de huellas	[E.25] Perdida de equipos	9
Lectores de huellas	[A.11] Acceso no autorizado	8,3
Lectores de huellas	[A.23] Manipulación de hardware	8
Lectores de huellas	[A.24] Denegación de servicio	10
Lectores de huellas	[A.25] Robo de equipos	9
Lectores de huellas	[A.26] Ataque destructivo	10
Biométricos	[N.1] Fuego	10
Biométricos	[N.2] Daños por agua	9
Biométricos	[N] Desastres naturales	10
Biométricos	[I.*] Desastres industriales	10
Biométricos	[1.3] Contaminación medioambiental	9
Biométricos	[I.4] Contaminación electromagnética	7
Biométricos	[1.5.2] Avería de origen físico	9
Biométricos	[I.6] Corte del suministro eléctrico	10
Biométricos	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Biométricos	[I.11] Emanaciones electromagnéticas (TEMPEST)	2
Biométricos	[E.23] Errores de mantenimiento / actualización de equipos	7
Biométricos	[E.25] Perdida de equipos	8,5
Biométricos	[A.11] Acceso no autorizado	7
Biométricos	[A.23] Manipulación de hardware	8
Biométricos	[A.24] Denegación de servicio	10
Biométricos	[A.25] Robo de equipos	8,5
Biométricos	[A.26] Ataque destructivo	10
Celulares	[N.1] Fuego	10

Celulares	[N.2] Daños por agua	9
Celulares	[N] Desastres naturales	10
Celulares	[I.*] Desastres industriales	10
Celulares	[1.3] Contaminación medioambiental	9
Celulares	[I.4] Contaminación electromagnética	7
Celulares	[1.5.2] Avería de origen físico	9
Celulares	[I.6] Corte del suministro eléctrico	10
Celulares	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Celulares	[I.11] Emanaciones electromagnéticas (TEMPEST)	10
Celulares	[E.23] Errores de mantenimiento / actualización de equipos	2
Celulares	[E.25] Perdida de equipos	5
Celulares	[A.11] Acceso no autorizado	7
Celulares	[A.23] Manipulación de hardware	8
Celulares	[A.24] Denegación de servicio	10
Celulares	[A.25] Robo de equipos	9
Celulares	[A.26] Ataque destructivo	10
Micrófonos	[N.1] Fuego	10
Micrófonos	[N.2] Daños por agua	9
Micrófonos	[N] Desastres naturales	10
Micrófonos	[I.*] Desastres industriales	10
Micrófonos	[1.3] Contaminación medioambiental	9
Micrófonos	[I.4] Contaminación electromagnética	7
Micrófonos	[1.5.2] Avería de origen físico	9
Micrófonos	[I.6] Corte del suministro eléctrico	10

Micrófonos	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Micrófonos	[I.11] Emanaciones electromagnéticas (TEMPEST)	2
Micrófonos	[E.23] Errores de mantenimiento / actualización de equipos	7
Micrófonos	[E.25] Perdida de equipos	8,5
Micrófonos	[A.11] Acceso no autorizado	7
Micrófonos	[A.23] Manipulación de hardware	8
Micrófonos	[A.24] Denegación de servicio	10
Micrófonos	[A.25] Robo de equipos	8,5
Micrófonos	[A.26] Ataque destructivo	10
Televisores	[N.1] Fuego	10
Televisores	[N.2] Daños por agua	9
Televisores	[N] Desastres naturales	10
Televisores	[I.*] Desastres industriales	10
Televisores	[1.3] Contaminación medioambiental	9
Televisores	[I.4] Contaminación electromagnética	7
Televisores	[1.5.2] Avería de origen físico	9
Televisores	[I.6] Corte del suministro eléctrico	10
Televisores	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Televisores	[I.11] Emanaciones electromagnéticas (TEMPEST)	2
Televisores	[E.23] Errores de mantenimiento / actualización de equipos	7
Televisores	[E.25] Perdida de equipos	8,5
Televisores	[A.11] Acceso no autorizado	7
Televisores	[A.23] Manipulación de hardware	8

Televisores	[A.24] Denegación de servicio	10
Televisores	[A.25] Robo de equipos	8,5
Televisores	[A.26] Ataque destructivo	10
Alcancel	[N.1] Fuego	10
Alcancel	[N.2] Daños por agua	9
Alcancel	[N] Desastres naturales	10
Alcancel	[I.*] Desastres industriales	10
Alcancel	[1.3] Contaminación medioambiental	9
Alcancel	[I.4] Contaminación electromagnética	7
Alcancel	[1.5.2] Avería de origen físico	9
Alcancel	[I.6] Corte del suministro eléctrico	10
Alcancel	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Alcancel	[I.11] Emanaciones electromagnéticas (TEMPEST)	2
Alcancel	[E.23] Errores de mantenimiento / actualización de equipos	7
Alcancel	[E.25] Perdida de equipos	7,5
Alcancel	[A.11] Acceso no autorizado	7
Alcancel	[A.23] Manipulación de hardware	8,5
Alcancel	[A.24] Denegación de servicio	10
Alcancel	[A.25] Robo de equipos	7,5
Alcancel	[A.26] Ataque destructivo	10
Estanterías	[N.1] Fuego	10
Estanterías	[N.2] Daños por agua	9
Estanterías	[N] Desastres naturales	10
Estanterías	[I.*] Desastres industriales	10

Estanterías	[1.3] Contaminación medioambiental	9
Estanterías	[I.4] Contaminación electromagnética	7
Estanterías	[1.5.2] Avería de origen físico	9
Estanterías	[I.6] Corte del suministro eléctrico	10
Estanterías	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Estanterías	[I.11] Emanaciones electromagnéticas (TEMPEST)	2
Estanterías	[E.23] Errores de mantenimiento / actualización de equipos	7
Estanterías	[E.25] Perdida de equipos	9
Estanterías	[A.11] Acceso no autorizado	8,3
Estanterías	[A.23] Manipulación de hardware	8
Estanterías	[A.24] Denegación de servicio	10
Estanterías	[A.25] Robo de equipos	9
Estanterías	[A.26] Ataque destructivo	10
Rótulos	[N.1] Fuego	10
Rótulos	[N.2] Daños por agua	9
Rótulos	[N] Desastres naturales	10
Rótulos	[I.*] Desastres industriales	10
Rótulos	[1.3] Contaminación medioambiental	9
Rótulos	[I.4] Contaminación electromagnética	7
Rótulos	[1.5.2] Avería de origen físico	9
Rótulos	[I.6] Corte del suministro eléctrico	10
Rótulos	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Rótulos	[I.11] Emanaciones electromagnéticas (TEMPEST)	2

Rótulos	[E.23] Errores de mantenimiento / actualización de equipos	7
Rótulos	[E.25] Perdida de equipos	8,5
Rótulos	[A.11] Acceso no autorizado	7
Rótulos	[A.23] Manipulación de hardware	8
Rótulos	[A.24] Denegación de servicio	10
Rótulos	[A.25] Robo de equipos	8,5
Rótulos	[A.26] Ataque destructivo	10
Rack	[N.1] Fuego	9
Rack	[N.2] Daños por agua	8
Rack	[N] Desastres naturales	9
Rack	[I.*] Desastres industriales	9
Rack	[1.3] Contaminación medioambiental	8
Rack	[I.4] Contaminación electromagnética	6
Rack	[1.5.2] Avería de origen físico	8
Rack	[I.6] Corte del suministro eléctrico	9
Rack	[I.7] Condiciones inadecuadas de temperatura o humedad	9
Rack	[I.11] Emanaciones electromagnéticas (TEMPEST)	1
Rack	[E.23] Errores de mantenimiento / actualización de equipos	6
Rack	[E.25] Perdida de equipos	6,5
Rack	[A.11] Acceso no autorizado	6
Rack	[A.23] Manipulación de hardware	7,5
Rack	[A.24] Denegación de servicio	9
Rack	[A.25] Robo de equipos	6,5

Rack	[A.26] Ataque destructivo	9
Implementos instalación internet	[N.1] Fuego	10
Implementos instalación internet	[N.2] Daños por agua	9
Implementos instalación internet	[N] Desastres naturales	10
Implementos instalación internet	[I.*] Desastres industriales	10
Implementos instalación internet	[I.4] Contaminación electromagnética	7
Implementos instalación internet	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Implementos instalación internet	[E.23] Errores de mantenimiento / actualización de equipos	7
Implementos instalación internet	[E.25] Perdida de equipos	7
Implementos instalación internet	[A.11] Acceso no autorizado	5,7
Implementos instalación internet	[A.23] Manipulación de hardware	7,5
Implementos instalación internet	[A.24] Denegación de servicio	9
Implementos instalación internet	[A.25] Robo de equipos	8,5
Implementos instalación internet	[A.26] Ataque destructivo	10
OLT	[N.1] Fuego	10
OLT	[N.2] Daños por agua	9

OLT	[N] Desastres naturales	10
OLT	[I.*] Desastres industriales	10
OLT	[1.3] Contaminación medioambiental	9
OLT	[I.4] Contaminación electromagnética	7
OLT	[1.5.2] Avería de origen físico	9
OLT	[I.6] Corte del suministro eléctrico	10
OLT	[I.7] Condiciones inadecuadas de temperatura o humedad	10
OLT	[E.23] Errores de mantenimiento / actualización de equipos	6,3
OLT	[E.25] Perdida de equipos	8,5
OLT	[A.11] Acceso no autorizado	8,5
OLT	[A.23] Manipulación de hardware	7,5
OLT	[A.24] Denegación de servicio	10
OLT	[A.25] Robo de equipos	8,5
OLT	[A.26] Ataque destructivo	10
Unidades de almacenamiento	[N.1] Fuego	10
Unidades de almacenamiento	[N.2] Daños por agua	9
Unidades de almacenamiento	[N] Desastres naturales	10
Unidades de almacenamiento	[I.*] Desastres industriales	10
Unidades de almacenamiento	[1.3] Contaminación medioambiental	9
Unidades de almacenamiento	[I.4] Contaminación electromagnética	7
Unidades de almacenamiento	[1.5.2] Avería de origen físico	9
Unidades de almacenamiento	[I.6] Corte del suministro eléctrico	10
Unidades de almacenamiento	[I.7] Condiciones inadecuadas de temperatura o humedad	10
Unidades de almacenamiento	[I.11] Emanaciones electromagnéticas (TEMPEST)	2

Unidades de almacenamiento	[E.23] Errores de mantenimiento / actualización de equipos	6,7
Unidades de almacenamiento	[E.25] Perdida de equipos	9
Unidades de almacenamiento	[A.11] Acceso no autorizado	8
Unidades de almacenamiento	[A.23] Manipulación de hardware	8
Unidades de almacenamiento	[A.24] Denegación de servicio	10
Unidades de almacenamiento	[A.25] Robo de equipos	9
Unidades de almacenamiento	[A.26] Ataque destructivo	10
	Comunicaciones	
Teléfonos	[I.8] Fallo de servicios de comunicación	9
Teléfonos	[E.2] Errores del administrador del sistema / de la seguridad	7,3
Teléfonos	[E.24] Caída del sistema por agotamiento de recursos	9
Teléfonos	[A.7] Uso no previsto	6,3
Teléfonos	[A.18] Destrucción de la información	9
Teléfonos	[A.24] Denegación de servicio	9
	Auxiliares	
Escaleras	[N.1] Fuego	10
Escaleras	[N.2] Daños por agua	9
Escaleras	[N] Desastres naturales	10
Escaleras	[I.*] Desastres industriales	10
Escaleras	[1.3] Contaminación medioambiental	9
Escaleras	[I.4] Contaminación electromagnética	9
Escaleras	[A.23] Manipulación de hardware	8
Escaleras	[A.25] Robo de equipos	7

Escaleras	[A.26] Ataque destructivo	7
Generadores	[N.1] Fuego	10
Generadores	[N.2] Daños por agua	9
Generadores	[N] Desastres naturales	10
Generadores	[I.*] Desastres industriales	3,4
Generadores	[1.3] Contaminación medioambiental	9
Generadores	[I.4] Contaminación electromagnética	9
Generadores	[1.5.2] Avería de origen físico	9
Generadores	[E.23] Errores de mantenimiento / actualización de equipos	7
Generadores	[A.23] Manipulación de hardware	9
Generadores	[A.25] Robo de equipos	10
Generadores	[A.26] Ataque destructivo	10
Sillas	[N.1] Fuego	10
Sillas	[N.2] Daños por agua	9
Sillas	[N] Desastres naturales	10
Sillas	[I.*] Desastres industriales	10
Sillas	[1.3] Contaminación medioambiental	9
Sillas	[E.23] Errores de mantenimiento / actualización de equipos	7
Sillas	[A.23] Manipulación de hardware	8
Sillas	[A.25] Robo de equipos	7
Sillas	[A.26] Ataque destructivo	7
Balanzas	[N.1] Fuego	10
Balanzas	[N.2] Daños por agua	9

Balanzas	[N] Desastres naturales	10
Balanzas	[I.*] Desastres industriales	10
Balanzas	[1.3] Contaminación medioambiental	9
Balanzas	[I.4] Contaminación electromagnética	9
Balanzas	[1.5.2] Avería de origen físico	1
Balanzas	[E.23] Errores de mantenimiento / actualización de equipos	8
Balanzas	[E.25] Perdida de equipos	7
Balanzas	[A.23] Manipulación de hardware	8
Balanzas	[A.25] Robo de equipos	7
Balanzas	[A.26] Ataque destructivo	7
Camilla	[N.1] Fuego	10
Camilla	[N.2] Daños por agua	9
Camilla	[N] Desastres naturales	10
Camilla	[I.*] Desastres industriales	10
Camilla	[A.23] Manipulación de hardware	8
Camilla	[A.25] Robo de equipos	7
Camilla	[A.26] Ataque destructivo	7
Linternas	[N.1] Fuego	9
Linternas	[N.2] Daños por agua	8
Linternas	[N] Desastres naturales	9
Linternas	[I.*] Desastres industriales	9
Linternas	[1.3] Contaminación medioambiental	9
Linternas	[A.23] Manipulación de hardware	4
Linternas	[A.25] Robo de equipos	3

Linternas	[A.26] Ataque destructivo	6
Perforadoras	[N.1] Fuego	5
Perforadoras	[N.2] Daños por agua	4
Perforadoras	[N] Desastres naturales	5
Perforadoras	[I.*] Desastres industriales	5
Perforadoras	[1.3] Contaminación medioambiental	4
Perforadoras	[A.23] Manipulación de hardware	2
Perforadoras	[A.25] Robo de equipos	1
Perforadoras	[A.26] Ataque destructivo	2
Recogedores	[N.1] Fuego	5
Recogedores	[N.2] Daños por agua	4
Recogedores	[N] Desastres naturales	5
Recogedores	[I.*] Desastres industriales	5
Recogedores	[1.3] Contaminación medioambiental	4
Recogedores	[A.23] Manipulación de hardware	2
Recogedores	[A.25] Robo de equipos	1
Recogedores	[A.26] Ataque destructivo	2
Regletas	[N.1] Fuego	9
Regletas	[N.2] Daños por agua	9
Regletas	[E.23] Errores de mantenimiento / actualización de equipos	5
Regletas	[E.25] Perdida de equipos	4
Pizarrones	[N.1] Fuego	10
Pizarrones	[N.2] Daños por agua	9
Pizarrones	[N] Desastres naturales	10

Pizarrones	[I.*] Desastres industriales	10
Pizarrones	[A.26] Ataque destructivo	7
Sellos de oficina	[N.1] Fuego	9
Sellos de oficina	[N.2] Daños por agua	10
Sellos de oficina	[N] Desastres naturales	10
Sellos de oficina	[A.11] Acceso no autorizado	5,5
Sellos de oficina	[A.23] Manipulación de hardware	5,5
Sellos de oficina	[A.24] Denegación de servicio	10
Microondas	[N.1] Fuego	10
Microondas	[N.2] Daños por agua	9
Microondas	[N] Desastres naturales	10
Microondas	[A.23] Manipulación de hardware	5
Microondas	[A.25] Robo de equipos	4
Microcomponentes	[N.1] Fuego	10
Microcomponentes	[N.2] Daños por agua	10
Microcomponentes	[N] Desastres naturales	10
Microcomponentes	[1.3] Contaminación medioambiental	9
Microcomponentes	[A.23] Manipulación de hardware	5
Microcomponentes	[A.24] Denegación de servicio	4
Microcomponentes	[A.25] Robo de equipos	7
Microcomponentes	[A.26] Ataque destructivo	7
Lectores de barras	[N.1] Fuego	10
Lectores de barras	[N.2] Daños por agua	9
Lectores de barras	[N] Desastres naturales	10
Lectores de barras	[I.*] Desastres industriales	10

Lectores de barras	[1.3] Contaminación medioambiental	9
Lectores de barras	[E.23] Errores de mantenimiento / actualización de equipos	7
Lectores de barras	[A.23] Manipulación de hardware	6
Lectores de barras	[A.25] Robo de equipos	5
Lectores de barras	[A.26] Ataque destructivo	7
Dispensador de agua	[N.1] Fuego	10
Dispensador de agua	[N.2] Daños por agua	9
Dispensador de agua	[N] Desastres naturales	10
Dispensador de agua	[I.*] Desastres industriales	10
Dispensador de agua	[1.3] Contaminación medioambiental	9
Dispensador de agua	[E.23] Errores de mantenimiento / actualización de equipos	7
Dispensador de agua	[A.23] Manipulación de hardware	5
Dispensador de agua	[A.25] Robo de equipos	4
Mostradores de vidrio	[N.1] Fuego	10
Mostradores de vidrio	[N.2] Daños por agua	9
Mostradores de vidrio	[N] Desastres naturales	10
Mostradores de vidrio	[1.3] Contaminación medioambiental	10
Mostradores de vidrio	[A.23] Manipulación de hardware	5,5
Mostradores de vidrio	[A.25] Robo de equipos	4,5
Mostradores de vidrio	[A.26] Ataque destructivo	7
Parlantes	[N.1] Fuego	10
Parlantes	[N.2] Daños por agua	9
Parlantes	[E.23] Errores de mantenimiento / actualización de equipos	7

Parlantes	[A.23] Manipulación de hardware	5
Parlantes	[A.25] Robo de equipos	4
Parlantes	[A.26] Ataque destructivo	7
Copiadoras	[N.1] Fuego	10
Copiadoras	[N.2] Daños por agua	9
Copiadoras	[N] Desastres naturales	10
Copiadoras	[1.3] Contaminación medioambiental	9
Copiadoras	[E.23] Errores de mantenimiento / actualización de equipos	7
Copiadoras	[A.23] Manipulación de hardware	7
Copiadoras	[A.25] Robo de equipos	6
Copiadoras	[A.26] Ataque destructivo	7
Extintores	[N.1] Fuego	10
Extintores	[N.2] Daños por agua	9
Extintores	[N] Desastres naturales	10
Extintores	[E.23] Errores de mantenimiento / actualización de equipos	7
Extintores	[A.23] Manipulación de hardware	5
Extintores	[A.25] Robo de equipos	4
Extintores	[A.26] Ataque destructivo	7
Casilleros metálicos	[N.1] Fuego	7
Casilleros metálicos	[N.2] Daños por agua	7
Casilleros metálicos	[N] Desastres naturales	7
Casilleros metálicos	[E.23] Errores de mantenimiento / actualización de equipos	7
Casilleros metálicos	[A.23] Manipulación de hardware	7

Casilleros metálicos	[A.25] Robo de equipos	7
Casilleros metálicos	[A.26] Ataque destructivo	7
Data Fast	[N.1] Fuego	10
Data Fast	[N.2] Daños por agua	9
Data Fast	[N] Desastres naturales	10
Data Fast	[I.*] Desastres industriales	10
Data Fast	[1.3] Contaminación medioambiental	9
Data Fast	[A.23] Manipulación de hardware	7
Data Fast	[A.25] Robo de equipos	6
Data Fast	[A.26] Ataque destructivo	7
Arnés reforzado	[N.1] Fuego	10
Arnés reforzado	[N.2] Daños por agua	9
Arnés reforzado	[N] Desastres naturales	10
Arnés reforzado	[I.*] Desastres industriales	10
Arnés reforzado	[1.3] Contaminación medioambiental	9
Arnés reforzado	[A.23] Manipulación de hardware	5
Arnés reforzado	[A.25] Robo de equipos	4
Arnés reforzado	[A.26] Ataque destructivo	7
Cascos	[N.1] Fuego	10
Cascos	[N.2] Daños por agua	9
Cascos	[N] Desastres naturales	10
Cascos	[I.*] Desastres industriales	10
Cascos	[1.3] Contaminación medioambiental	9
Cascos	[A.25] Robo de equipos	4,5
Cascos	[A.26] Ataque destructivo	7

Cinturones	[N.1] Fuego	10
Cinturones	[N.2] Daños por agua	9
Cinturones	[N] Desastres naturales	10
Cinturones	[I.*] Desastres industriales	9
Cinturones	[I.4] Contaminación electromagnética	9
Cinturones	[A.25] Robo de equipos	4,5
Cinturones	[A.26] Ataque destructivo	7
Eslinga	[N.1] Fuego	10
Eslinga	[N.2] Daños por agua	9
Eslinga	[N] Desastres naturales	10
Eslinga	[I.*] Desastres industriales	10
Eslinga	[1.3] Contaminación medioambiental	9
Eslinga	[A.25] Robo de equipos	4,5
Eslinga	[A.26] Ataque destructivo	7
Gafas	[N.1] Fuego	10
Gafas	[N.2] Daños por agua	9
Gafas	[N] Desastres naturales	10
Gafas	[I.*] Desastres industriales	10
Gafas	[A.25] Robo de equipos	4
Gafas	[A.26] Ataque destructivo	7
Guates	[N.1] Fuego	10
Guates	[N.2] Daños por agua	9
Guates	[N] Desastres naturales	10
Guates	[I.*] Desastres industriales	10
Guates	[A.25] Robo de equipos	4

Guates	[A.26] Ataque destructivo	7
Mosquetón	[N.1] Fuego	10
Mosquetón	[N.2] Daños por agua	9
Mosquetón	[N] Desastres naturales	10
Mosquetón	[I.*] Desastres industriales	10
Mosquetón	[A.25] Robo de equipos	4
Mosquetón	[A.26] Ataque destructivo	7
Chalecos	[N.1] Fuego	10
Chalecos	[N.2] Daños por agua	9
Chalecos	[N] Desastres naturales	10
Chalecos	[I.*] Desastres industriales	10
Chalecos	[A.25] Robo de equipos	4
Chalecos	[A.26] Ataque destructivo	7
Conos de seguridad	[N.1] Fuego	10
Conos de seguridad	[N.2] Daños por agua	9
Conos de seguridad	[N] Desastres naturales	10
Conos de seguridad	[I.*] Desastres industriales	10
Conos de seguridad	[A.25] Robo de equipos	4
Conos de seguridad	[A.26] Ataque destructivo	7
Letreros de advertencia	[N.1] Fuego	10
Letreros de advertencia	[N.2] Daños por agua	9
Letreros de advertencia	[N] Desastres naturales	10
Letreros de advertencia	[I.*] Desastres industriales	10
Letreros de advertencia	[A.25] Robo de equipos	4
Letreros de advertencia	[A.26] Ataque destructivo	7

Herramientas	[N.1] Fuego	10
Herramientas	[N.2] Daños por agua	9
Herramientas	[N] Desastres naturales	10
Herramientas	[I.*] Desastres industriales	10
Herramientas	[A.25] Robo de equipos	4
Herramientas	[A.26] Ataque destructivo	7
Case para discos duros	[N.1] Fuego	10
Case para discos duros	[N.2] Daños por agua	10
Case para discos duros	[I.*] Desastres industriales	10
Case para discos duros	[A.11] Acceso no autorizado	4
Case para discos duros	[A.23] Manipulación de hardware	6
Apple pencil	[N.1] Fuego	10
Apple pencil	[N.2] Daños por agua	9
Apple pencil	[N] Desastres naturales	10
Apple pencil	[I.*] Desastres industriales	10
Apple pencil	[A.23] Manipulación de hardware	5,5
Apple pencil	[A.25] Robo de equipos	4,5
Apple pencil	[A.26] Ataque destructivo	7
Alexa	[N.1] Fuego	10
Alexa	[N.2] Daños por agua	9
Alexa	[N] Desastres naturales	10
Alexa	[A.11] Acceso no autorizado	4
Alexa	[A.23] Manipulación de hardware	4
Alexa	[A.25] Robo de equipos	4,5
Alexa	[A.26] Ataque destructivo	7

	Servicios subcontratados/ Instalaciones	
Casa Plus 1	[N.1] Fuego	10
Casa Plus 1	[N.2] Daños por agua	10
Casa Plus 1	[N] Desastres naturales	10
Casa Plus 1	[I.1] Fuego	10
Casa Plus 1	[I.*] Desastres industriales	10
Casa Plus 1	[1.3] Contaminación medioambiental	7
Casa Plus 1	[I.4] Contaminación electromagnética	7
Casa Plus 1	[A.6] Abuso de privilegios de acceso	7
Casa Plus 1	[A.25] Robo de equipos	10
Casa Plus 1	[A.26] Ataque destructivo	10
Casa Plus 1	[A.27] Ocupación enemiga	6
Casa Plus 2	[N.1] Fuego	10
Casa Plus 2	[N.2] Daños por agua	10
Casa Plus 2	[N] Desastres naturales	10
Casa Plus 2	[I.1] Fuego	10
Casa Plus 2	[I.*] Desastres industriales	10
Casa Plus 2	[1.3] Contaminación medioambiental	7
Casa Plus 2	[I.4] Contaminación electromagnética	7
Casa Plus 2	[A.6] Abuso de privilegios de acceso	7
Casa Plus 2	[A.25] Robo de equipos	10
Casa Plus 2	[A.26] Ataque destructivo	10
Casa Plus 2	[A.27] Ocupación enemiga	6
	Personal	
Gerencia General	[E.15] Alteración de la información	6

Gerencia General	[E.18] Destrucción de información	4
Gerencia General	[E.19] Fuga de información	2
Gerencia General	[E.28] Indisponibilidad de personal	7
Gerencia General	[A.15] Modificación de la información	8
Gerencia General	[A.18] Destrucción de la información	7
Gerencia General	[A.19] Revelación de información	4
Gerencia General	[E.28] Indisponibilidad de personal	9
Gerencia General	[A.29] Extorsión	9
Gerencia General	[A.30] Ingeniería Social (picaresca)	6
Gerencia Operativa	[E.15] Alteración de la información	7
Gerencia Operativa	[E.18] Destrucción de información	4
Gerencia Operativa	[E.19] Fuga de información	5,7
Gerencia Operativa	[E.28] Indisponibilidad de personal	7
Gerencia Operativa	[A.15] Modificación de la información	9
Gerencia Operativa	[A.18] Destrucción de la información	7
Gerencia Operativa	[A.19] Revelación de información	9
Gerencia Operativa	[E.28] Indisponibilidad de personal	9
Gerencia Operativa	[A.29] Extorsión	9,7
Gerencia Operativa	[A.30] Ingeniería Social (picaresca)	9,7
Gerencia Administrativa	[E.15] Alteración de la información	4
Gerencia Administrativa	[E.18] Destrucción de información	6
Gerencia Administrativa	[E.19] Fuga de información	4
Gerencia Administrativa	[E.28] Indisponibilidad de personal	2
Gerencia Administrativa	[A.15] Modificación de la información	8
Gerencia Administrativa	[A.18] Destrucción de la información	8

Gerencia Administrativa	[A.19] Revelación de información	7
Gerencia Administrativa	[E.28] Indisponibilidad de personal	4
Gerencia Administrativa	[A.29] Extorsión	9
Gerencia Administrativa	[A.30] Ingeniería Social (picaresca)	6,3
Gerencia Atención al Cliente	[E.15] Alteración de la información	6
Gerencia Atención al Cliente	[E.18] Destrucción de información	4
Gerencia Atención al Cliente	[E.19] Fuga de información	1
Gerencia Atención al Cliente	[E.28] Indisponibilidad de personal	2
Gerencia Atención al Cliente	[A.15] Modificación de la información	8
Gerencia Atención al Cliente	[A.18] Destrucción de la información	8
Gerencia Atención al Cliente	[A.19] Revelación de información	2
Gerencia Atención al Cliente	[E.28] Indisponibilidad de personal	9
Gerencia Atención al Cliente	[A.29] Extorsión	5,3
Gerencia Atención al Cliente	[A.30] Ingeniería Social (picaresca)	6,3
Gerencia comercial	[E.15] Alteración de la información	6
Gerencia comercial	[E.18] Destrucción de información	2
Gerencia comercial	[E.19] Fuga de información	5,7
Gerencia comercial	[E.28] Indisponibilidad de personal	7
Gerencia comercial	[A.15] Modificación de la información	5,7
Gerencia comercial	[A.18] Destrucción de la información	7
Gerencia comercial	[A.19] Revelación de información	3
Gerencia comercial	[E.28] Indisponibilidad de personal	9
Gerencia comercial	[A.29] Extorsión	5,7
Gerencia comercial	[A.30] Ingeniería Social (picaresca)	5,7

Nota: Elaboración Propia

Anexo 5 Peso Ponderado de los Activos

	Amenazas de Activos	D	I	C	Peso
Base de Datos	[A.11] Acceso no autorizado	8,0	7,4	6,8	7,4
Datos de acceso	[A.11] Acceso no autorizado	6,8	6,8	7,2	6,9
Detectores de Humo	[A.11] Acceso no autorizado	8,0	6,2	2,4	5,5
Kit de Seguridad	A.22] Manipulación de programas	7,4	5,7	3,0	5,4
Sistema Contable	[I.5.1] Avería de origen lógico	6,3	6,8	6,2	6,4
Fusionadoras	[A.23] Manipulación del hardware	7,2		5,1	6,2
Cargadores	[A.23] Manipulación del hardware	7,2	5,1	5,1	5,8
Power Meter	[A.23] Manipulación del hardware	7,2	5,1	5,1	5,8
Sacabocados	[A.23] Manipulación del hardware	7,2		5,1	6,2
Taladros	[A.23] Manipulación del hardware	7,2	5,1	5,1	5,8
Etiquetadoras	[A.23] Manipulación del hardware	7,1		5,1	6,1
Cámaras Web	[E.25] Pérdida de equipos	7,2	6,8	5,7	6,6
Computadoras Portátiles	[E.25] Pérdida de equipos	8,0	6,8	6,8	7,2
Cooler AMD	[E.25] Pérdida de equipos	7,2			7,2
CPU	[E.25] Pérdida de equipos	7,2	6,8	6,2	6,7
Video Card	[E.25] Pérdida de equipos	7,2	5,1	5,1	5,8
Impresoras	[A.11] Acceso no autorizado	7,2	5,1	5,7	6,0
IPad Apple	[A.11] Acceso no autorizado	7,2	6,8	5,7	6,6
MacBook Air	[A.11] Acceso no autorizado	7,2	6,8	5,7	6,6
Monitores	[E.25] Pérdida de equipos	7,2	6,8	5,7	6,6
Mouse	[E.25] Pérdida de equipos	7,2	5,1	5,1	5,8
Server Dell	[A.15] Modificación de la información	7,2	6,8	6,0	6,7
Tablet Lenovo	[E.25] Pérdida de equipos	7,2	6,8	5,7	6,6
Teclados	[E.25] Pérdida de equipos	7,2	5,1	5,1	5,8
TV	[E.25] Pérdida de equipos	7,2	5,1	5,1	5,8
Amplificadores	[E.25] Pérdida de equipos	7,1	5,1	5,1	5,8
Aspiradoras	[E.25] Pérdida de equipos	7,2	5,1	5,1	5,8
Lectores de Huellas	[A.11] Acceso no autorizado	7,4	6,8	6,3	6,8
Biométricos	[A.11] Acceso no autorizado	7,2		5,1	6,2
Celulares	[E.25] Pérdida de equipos	8,0	7,4	6,8	7,4
Micrófonos	[E.25] Pérdida de equipos	7,2		5,1	6,2
Televisores	[E.25] Pérdida de equipos	7,1		5,1	6,1
Alcancel	[E.25] Pérdida de equipos	7,1	5,1	5,1	5,8

Estanterías	[E.25] Pérdida de equipos	7,2	6,8	5,7	6,6
Rótulos	[E.25] Pérdida de equipos	7,2	5,1	5,1	5,8
Rack	[A.11] Acceso no autorizado	6,6	4,5	4,5	5,2
Instalación internet	[A.15] Modificación de la información	8,0	4,5	4,5	5,7
OLT GPON	[E.25] Pérdida de equipos	7,2	6,2	5,1	6,2
Unidades de Almacenamiento	[A.25] Robo de equipos	7,2	6,2	5,7	6,4
Ofimática	[E.25] Pérdida de equipos	7,2	4,5	5,1	5,6
Teléfonos IP 2 cuentas	[E.25] Pérdida de equipos	7,2	5,6	5,1	6,0
Escaleras	[A.11] Acceso no autorizado	6,6	3,3	5,1	5,0
Generadores	[A.11] Acceso no autorizado	6,6			6,6
Sillas	[E.25] Pérdida de equipos	6,6	3,3	5,1	5,0
Balanzas	[E.25] Pérdida de equipos	6,6	3,3	5,1	5,0
Camilla	[E.25] Pérdida de equipos	6,6	3,3	2,1	4,0
Linternas	[E.25] Pérdida de equipos	6,0	2,1	0,9	3,0
Grapadoras	[E.25] Pérdida de equipos	3,6	0,8	1,0	1,8
Perforadoras	[E.25] Pérdida de equipos	3,6	0,8	1,0	1,8
Recogedores	[E.25] Pérdida de equipos	6,6	2,7	1,6	3,6
Regletas	[E.25] Pérdida de equipos	6,6	2,7	1,6	3,6
Pizarrones	[E.25] Pérdida de equipos	6,6	2,7	1,6	3,6
Sellos de Oficina	[E.25] Pérdida de equipos	6,6	2,7	1,9	3,7
Microondas	[E.25] Pérdida de equipos	6,6	2,7	1,6	3,6
Minicomponente	[A.11] Acceso no autorizado	6,6	2,7	1,6	3,6
Lectores de Barras	[A.11] Acceso no autorizado	6,6	2,7	2,8	4,0
Dispensador de agua	[E.25] Pérdida de equipos	6,6	2,7	1,6	3,6
Mostrador de vidrio	[E.25] Pérdida de equipos	6,6	2,7	2,2	3,8
Parlantes	[E.25] Pérdida de equipos	6,6	2,7	1,6	3,6
Copiadoras	[E.25] Pérdida de equipos	6,6	2,7	3,9	4,4
Extintores	[A.11] Acceso no autorizado	6,6	3,3	1,6	3,8
Casilleros metálicos	[A.11] Acceso no autorizado	5,1			5,1
Data Fast	[A.11] Acceso no autorizado	6,6	2,7	3,9	4,4
Arnés Reforzado	[E.25] Pérdida de equipos	6,6	2,7	1,6	3,6
Cascos	[E.25] Pérdida de equipos	6,6	2,7	2,2	3,8
Cinturones	[E.25] Pérdida de equipos	6,3	2,7	2,2	3,7
Eslinga	[E.25] Pérdida de equipos	6,6	2,7	1,6	3,6
Gafas	[E.25] Pérdida de equipos	6,6	2,7	1,6	3,6
Guantes	[E.25] Pérdida de equipos	6,6	2,7	1,6	3,6
Mosquetón	[E.25] Pérdida de equipos	6,6	2,7	1,6	3,6
Chalecos	[E.25] Pérdida de equipos	6,6	2,7	1,6	3,6

Conos de Seguridad	[E.25] Pérdida de equipos	6,6	2,7	1,6	3,6
Letreros de Advertencia	[A.11] Acceso no autorizado	6,6	2,7	1,6	3,6
Herramientas	[A.11] Acceso no autorizado	6,6	2,7	1,6	3,6
Case para Discos Duros	[A.11] Acceso no autorizado	6,3		2,8	4,6
Apple Pencil	[A.25] Robo de equipos	6,6		2,2	4,4
Alexa	[A.11] Acceso no autorizado	6,6	2,7	2,2	3,8
Casa Plus 1	[A.30] Ingeniería social (picaresca	6,8		3,0	4,9
Casa Plus 2	[A.30] Ingeniería social (picaresca	6,8		3,0	4,9
Atención al cliente	[A.30] Ingeniería social (picaresca				
Gerencia Operativa	[A.30] Ingeniería social (picaresca	6,0	5,7	4,2	5,3
Gerencia General	[A.30] Ingeniería social (picaresca	6,3	6,8	7,2	6,8
Gerencia Administrativa	[A.30] Ingeniería social (picaresca	6,0	5,7	4,2	5,3
Gerencia Atención al Cliente	[A.30] Ingeniería social (picaresca	6,0	5,7	2,1	4,6
Gerencia Comercial	[A.30] Ingeniería social (picaresca	6,0	5,7	3,5	5,1

Nota: Elaboración Propia.

Anexo 6 Tratamiento de Riesgos

Activo	Amenaza	Peso ponderado	Tratamiento
	Datos/Información		
Base de Datos	[1.5.11 Avería de origen lógico	9	Evitar
Base de Datos	[E.8] Difusión de software dañino	6,3	Evitar
Base de Datos	[E.15] Alteración de la información	4	Evitar
Base de Datos	[E,20] Vulnerabilidades de los programas (software)	6	Reducir
Base de Datos	[E.21] Errores de mantenimiento I actualización (software)	6	Reducir
Base de Datos	[A.8] Difusión de software dañino	9,3	Evitar
Base de Datos	[A.22] Manipulación de programas	9	Reducir
Base de Datos	[1.5.11 Avería de origen lógico	9	Evitar
Base de Datos	[E.8] Difusión de software dañino	7	Evitar
Base de Datos	[E.20] Vulnerabilidades de los programas (software)	6,7	Reducir
Base de Datos	[E.21] Errores de mantenimiento / actualización (software)	6,7	Evitar
Base de Datos	[A.8] Difusión de software dañino	10	Evitar
Base de Datos	[A.221] Manipulación de programas	9,7	Evitar
	Servicios		
Electricidad	[E.2] Errores del administrador del sistema / de la seguridad	6	Evitar
Electricidad	[E.15] Alteración de la información	5,7	Evitar
Electricidad	[E.19] Fugas de información	7	Evitar
Electricidad	[A.5] Suplantación de la identidad	7,3	Reducir
Electricidad	[A.6] Abuso de privilegios de acceso	6,3	Reducir
Electricidad	[A.7] Uso no previsto	6	Evitar

Electricidad	[A.11] Acceso no autorizado	7	Reducir
Electricidad	[A.15] Modificación de la información	7	Evitar
Internet	[E.1] Errores de los usuarios	6	Evitar
Internet	[E.2] Errores del administrador del sistema / de la seguridad	6	Reducir
Internet	[E.15] Alteración de la información	5,7	Evitar
Internet	[E.19] Fugas de información	7	Evitar
Internet	[A.5] Suplantación de la identidad	7,3	Evitar
Internet	[A.6] Abuso de privilegios de acceso	6,3	Evitar
Internet	[A.7] Uso no previsto	6	Evitar
Internet	[A.11] Acceso no autorizado	7	Reducir
Internet	[A.15] Modificación de la información	7	Evitar
Mantenimiento	[E.1] Errores de los usuarios	6	Evitar
Mantenimiento	[E.2] Errores del administrador del sistema / de la seguridad	6	Evitar
Mantenimiento	[E.15] Alteración de la información	5,7	Evitar
Mantenimiento	[E.19] Fugas de información	7	Evitar
Mantenimiento	[A.5] Suplantación de la identidad	7,3	Evitar
Mantenimiento	[A.6] Abuso de privilegios de acceso	6,3	Evitar
Mantenimiento	[A.7] Uso no previsto	6	Evitar
Mantenimiento	[A.11] Acceso no autorizado	7	Reducir
Mantenimiento	[A.15] Modificación de la información	7	Evitar
Correo	[E.1] Errores de los usuarios	6	
Correo	[E.2] Errores del administrador del sistema / de la seguridad	6	Reducir
Correo	[E.15] Alteración de la información	5,7	Evitar
Correo	[E.19] Fugas de información	7	Evitar
Correo	[A.5] Suplantación de la identidad	7,3	Evitar
Correo	[A.6] Abuso de privilegios de acceso	6,3	Evitar
Correo	[A.7] Uso no previsto	6	Evitar
Correo	[A.11] Acceso no autorizado	7	Reducir
Correo	[A.15] Modificación de la información	7	Reducir
Datos de ingreso	[1.5.1] Avería de origen lógico	9	Evitar

Datos de ingreso	[E.8] Difusión de software dañino	7	Evitar
Datos de ingreso	[E.20] Vulnerabilidades de los programas (software)	6,7	Evitar
Datos de ingreso	[E.21] Errores de mantenimiento / actualización (software)	6,7	Evitar
Datos de ingreso	[A.8] Difusión de software dañino	10	Evitar
Datos de ingreso	[A.221] Manipulación de programas	9,7	Evitar
Detectores de humo	[1.3] Contaminación medioambiental	9	Evitar
Kits de seguridad	[N] Desastres naturales	10	Evitar
Kits de seguridad	[N.1] Fuego	9,7	Evitar
Kits de seguridad	[A.26] Ataque destructivo	9	Evitar
Sistema contable	[1.5.1] Avería de origen lógico	9	Evitar
Sistema contable	[E.8] Difusión de software dañino	6,7	Evitar
Sistema contable	[E.20] Vulnerabilidades de los programas (software)	6,3	Evitar
Sistema contable	[E.21] Errores de mantenimiento / actualización (software)	6,3	Reducir
Sistema contable	[A.8] Difusión de software dañino	9,7	Evitar
Sistema contable	[A.221] Manipulación de programas	9,3	Evitar
Antivirus	[1.5.1] Avería de origen lógico	9	Evitar
Antivirus	[E.8] Difusión de software dañino	6,7	Evitar
Antivirus	[E.20] Vulnerabilidades de los programas (software)	6,3	Evitar
Antivirus	[E.21] Errores de mantenimiento / actualización (software)	6,3	Reducir
Antivirus	[A.8] Difusión de software dañino	9,7	Evitar
Antivirus	[A.221] Manipulación de programas	9,3	Evitar
Fusionadoras	[N.1] Fuego	10	Evitar
Fusionadoras	[N.2] Daños por agua	9	Evitar
Fusionadoras	[N] Desastres naturales	10	Evitar
Fusionadoras	[I.*] Desastres industriales	10	Evitar
Fusionadoras	[1.3] Contaminación medioambiental	9	Evitar
Fusionadoras	[I.4] Contaminación electromagnética	7	Evitar
Fusionadoras	[1.5.2] Avería de origen físico	9	Evitar
Fusionadoras	[I.6] Corte del suministro eléctrico	10	Evitar
Fusionadoras	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Fusionadoras	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Evitar
Fusionadoras	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
Fusionadoras	[E.25] Perdida de equipos	8,5	Evitar
Fusionadoras	[A.11] Acceso no autorizado	7	Reducir
Fusionadoras	[A.23] Manipulación de hardware	8	Evitar
Fusionadoras	[A.24] Denegación de servicio	10	Evitar
Fusionadoras	[A.25] Robo de equipos	8,5	Evitar

Fusionadoras	[A.26] Ataque destructivo	10	Evitar
Cargadores	[N.1] Fuego	10	Evitar
Cargadores	[N.2] Daños por agua	9	Evitar
Cargadores	[N] Desastres naturales	10	Evitar
Cargadores	[I.*] Desastres industriales	10	Evitar
Cargadores	[1.3] Contaminación medioambiental	9	Evitar
Cargadores	[I.4] Contaminación electromagnética	10	Evitar
Cargadores	[1.5.2] Avería de origen físico	9	Evitar
Cargadores	[I.6] Corte del suministro eléctrico	7	Evitar
Cargadores	[I.7] Condiciones inadecuadas de temperatura o humedad	9	Evitar
Cargadores	[I.11] Emanaciones electromagnéticas (TEMPEST)	10	Evitar
Cargadores	[E.23] Errores de mantenimiento / actualización de equipos	10	Evitar
Cargadores	[E.25] Perdida de equipos	2	Reducir
Cargadores	[A.11] Acceso no autorizado	7	Evitar
Cargadores	[A.23] Manipulación de hardware	8	Evitar
Cargadores	[A.24] Denegación de servicio	10	Evitar
Cargadores	[A.25] Robo de equipos	5,5	Reducir
Cargadores	[A.26] Ataque destructivo	10	Reducir
Power Meter	[N.1] Fuego	10	Evitar
Power Meter	[N.2] Daños por agua	9	Evitar
Power Meter	[N] Desastres naturales	10	Evitar
Power Meter	[I.*] Desastres industriales	10	Evitar
Power Meter	[1.3] Contaminación medioambiental	9	Evitar
Power Meter	[I.4] Contaminación electromagnética	10	Evitar
Power Meter	[1.5.2] Avería de origen físico	9	Reducir
Power Meter	[I.6] Corte del suministro eléctrico	7	Evitar
Power Meter	[I.7] Condiciones inadecuadas de temperatura o humedad	9	Evitar
Power Meter	[I.11] Emanaciones electromagnéticas (TEMPEST)	10	Evitar
Power Meter	[E.23] Errores de mantenimiento / actualización de equipos	10	Evitar
Power Meter	[E.25] Perdida de equipos	8,5	Reducir
Power Meter	[A.11] Acceso no autorizado	7	Reducir
Power Meter	[A.23] Manipulación de hardware	8,5	Evitar
Power Meter	[A.24] Denegación de servicio	10	Evitar
Power Meter	[A.25] Robo de equipos	8,5	Evitar
Power Meter	[A.26] Ataque destructivo	10	Reducir
Sacabocados	[N.1] Fuego	10	Evitar
Sacabocados	[N.2] Daños por agua	9	Evitar
Sacabocados	[N] Desastres naturales	10	Evitar
Sacabocados	[I.*] Desastres industriales	10	Evitar

Sacabocados	[1.3] Contaminación medioambiental	9	Reducir
Sacabocados	[I.4] Contaminación electromagnética	10	Reducir
Sacabocados	[1.5.2] Avería de origen físico	9	Evitar
Sacabocados	[I.6] Corte del suministro eléctrico	7	Evitar
Sacabocados	[I.7] Condiciones inadecuadas de temperatura o humedad	9	Evitar
Sacabocados	[I.11] Emanaciones electromagnéticas (TEMPEST)	10	Evitar
Sacabocados	[E.23] Errores de mantenimiento / actualización de equipos	10	Evitar
Sacabocados	[E.25] Perdida de equipos	8,5	Reducir
Sacabocados	[A.11] Acceso no autorizado	7	Reducir
Sacabocados	[A.23] Manipulación de hardware	8	Evitar
Sacabocados	[A.24] Denegación de servicio	10	Evitar
Sacabocados	[A.25] Robo de equipos	8,5	Evitar
Sacabocados	[A.26] Ataque destructivo	10	Reducir
Taladros	[N.1] Fuego	10	Evitar
Taladros	[N.2] Daños por agua	9	Evitar
Taladros	[N] Desastres naturales	10	Evitar
Taladros	[I.*] Desastres industriales	10	Evitar
Taladros	[1.3] Contaminación medioambiental	9	Reducir
Taladros	[I.4] Contaminación electromagnética	10	Reducir
Taladros	[1.5.2] Avería de origen físico	9	Reducir
Taladros	[I.6] Corte del suministro eléctrico	7	Evitar
Taladros	[I.7] Condiciones inadecuadas de temperatura o humedad	9	Evitar
Taladros	[I.11] Emanaciones electromagnéticas (TEMPEST)	10	Evitar
Taladros	[E.23] Errores de mantenimiento / actualización de equipos	7	Evitar
Taladros	[E.25] Perdida de equipos	8,5	Evitar
Taladros	[A.11] Acceso no autorizado	7	Reducir
Taladros	[A.23] Manipulación de hardware	8	Reducir
Taladros	[A.24] Denegación de servicio	10	Evitar
Taladros	[A.25] Robo de equipos	8,5	Evitar
Taladros	[A.26] Ataque destructivo	10	Reducir
Etiquetadoras	[N.1] Fuego	10	Evitar
Etiquetadoras	[N.2] Daños por agua	9	Evitar
Etiquetadoras	[N] Desastres naturales	10	Evitar
Etiquetadoras	[I.*] Desastres industriales	10	Evitar
Etiquetadoras	[1.3] Contaminación medioambiental	9	Reducir
Etiquetadoras	[I.4] Contaminación electromagnética	7	Reducir
Etiquetadoras	[1.5.2] Avería de origen físico	9	Reducir
Etiquetadoras	[I.6] Corte del suministro eléctrico	10	Evitar

Etiquetadoras	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Etiquetadoras	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Evitar
Etiquetadoras	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
Etiquetadoras	[E.25] Perdida de equipos	8,5	Evitar
Etiquetadoras	[A.11] Acceso no autorizado	7	Evitar
Etiquetadoras	[A.23] Manipulación de hardware	8,5	Reducir
Etiquetadoras	[A.24] Denegación de servicio	10	Evitar
Etiquetadoras	[A.25] Robo de equipos	8,5	Reducir
Etiquetadoras	[A.26] Ataque destructivo	10	Evitar
Cámaras Web	[N.1] Fuego	10	Evitar
Cámaras Web	[N.2] Daños por agua	9	Evitar
Cámaras Web	[N] Desastres naturales	10	Asumir
Cámaras Web	[I.*] Desastres industriales	10	Evitar
Cámaras Web	[1.3] Contaminación medioambiental	9	Reducir
Cámaras Web	[I.4] Contaminación electromagnética	7	Reducir
Cámaras Web	[1.5.2] Avería de origen físico	9	Reducir
Cámaras Web	[I.6] Corte del suministro eléctrico	10	Evitar
Cámaras Web	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Cámaras Web	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Evitar
Cámaras Web	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
Cámaras Web	[E.25] Perdida de equipos	9	Reducir
Cámaras Web	[A.11] Acceso no autorizado	8,3	Reducir
Cámaras Web	[A.23] Manipulación de hardware	8	Reducir
Cámaras Web	[A.24] Denegación de servicio	10	Evitar
Cámaras Web	[A.25] Robo de equipos	9	Evitar
Cámaras Web	[A.26] Ataque destructivo	10	Reducir
Cooler AMD	[N.1] Fuego	10	Evitar
Cooler AMD	[N.2] Daños por agua	9	Evitar
Cooler AMD	[N] Desastres naturales	10	Asumir
Cooler AMD	[I.*] Desastres industriales	10	Reducir
Cooler AMD	[1.3] Contaminación medioambiental	9	Reducir
Cooler AMD	[I.4] Contaminación electromagnética	7	Reducir
Cooler AMD	[1.5.2] Avería de origen físico	9	Reducir
Cooler AMD	[I.6] Corte del suministro eléctrico	10	Evitar
Cooler AMD	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Cooler AMD	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Evitar
Cooler AMD	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir

Cooler AMD	[E.25] Perdida de equipos	9	Reducir
Cooler AMD	[A.11] Acceso no autorizado	8,3	Reducir
Cooler AMD	[A.23] Manipulación de hardware	8	Reducir
Cooler AMD	[A.24] Denegación de servicio	10	Evitar
Cooler AMD	[A.25] Robo de equipos	9	Evitar
Cooler AMD	[A.26] Ataque destructivo	10	Reducir
CPU	[N.1] Fuego	10	Evitar
CPU	[N.2] Daños por agua	9	Evitar
CPU	[N] Desastres naturales	10	Asumir
CPU	[I.*] Desastres industriales	10	Evitar
CPU	[1.3] Contaminación medioambiental	9	Reducir
CPU	[I.4] Contaminación electromagnética	7	Reducir
CPU	[1.5.2] Avería de origen físico	9	Reducir
CPU	[I.6] Corte del suministro eléctrico	10	Evitar
CPU	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
CPU	[I.11] Emanaciones electromagnéticas (TEMPEST)	3	Reducir
CPU	[E.23] Errores de mantenimiento / actualización de equipos	7,3	Reducir
CPU	[E.25] Perdida de equipos	9,5	Reducir
CPU	[A.11] Acceso no autorizado	8,7	Reducir
CPU	[A.23] Manipulación de hardware	7,3	Reducir
CPU	[A.24] Denegación de servicio	10	Evitar
CPU	[A.25] Robo de equipos	9,5	Evitar
CPU	[A.26] Ataque destructivo	10	Reducir
Video Card	[N.1] Fuego	10	Reducir
Video Card	[N.2] Daños por agua	9	Evitar
Video Card	[N] Desastres naturales	10	Evitar
Video Card	[I.*] Desastres industriales	10	Asumir
Video Card	[1.3] Contaminación medioambiental	9	Reducir
Video Card	[I.4] Contaminación electromagnética	7	Reducir
Video Card	[1.5.2] Avería de origen físico	9	Reducir
Video Card	[I.6] Corte del suministro eléctrico	10	Evitar
Video Card	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Video Card	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Reducir
Video Card	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
Video Card	[E.25] Perdida de equipos	8,5	Evitar
Video Card	[A.11] Acceso no autorizado	7	Reducir
Video Card	[A.23] Manipulación de hardware	8	Reducir
Video Card	[A.24] Denegación de servicio	10	Evitar
Video Card	[A.25] Robo de equipos	8,5	Evitar

Video Card	[A.26] Ataque destructivo	10	Reducir
Impresoras	[N.1] Fuego	10	Evitar
Impresoras	[N.2] Daños por agua	9	Evitar
Impresoras	[N] Desastres naturales	10	Asumir
Impresoras	[I.*] Desastres industriales	10	Reducir
Impresoras	[1.3] Contaminación medioambiental	9	Reducir
Impresoras	[I.4] Contaminación electromagnética	7	Reducir
Impresoras	[1.5.2] Avería de origen físico	9	Reducir
Impresoras	[I.6] Corte del suministro eléctrico	10	Evitar
Impresoras	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Impresoras	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Reducir
Impresoras	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
Impresoras	[E.25] Perdida de equipos	9	Reducir
Impresoras	[A.11] Acceso no autorizado	7	Reducir
Impresoras	[A.23] Manipulación de hardware	8	Evitar
Impresoras	[A.24] Denegación de servicio	10	Evitar
Impresoras	[A.25] Robo de equipos	9	Evitar
Impresoras	[A.26] Ataque destructivo	10	Reducir
iPads Apple	[N.1] Fuego	10	Evitar
iPads Apple	[N.2] Daños por agua	9	Evitar
iPads Apple	[N] Desastres naturales	10	Asumir
iPads Apple	[I.*] Desastres industriales	10	Reducir
iPads Apple	[1.3] Contaminación medioambiental	9	Reducir
iPads Apple	[I.4] Contaminación electromagnética	7	reducir
iPads Apple	[1.5.2] Avería de origen físico	9	Reducir
iPads Apple	[I.6] Corte del suministro eléctrico	10	Evitar
iPads Apple	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
iPads Apple	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Reducir
iPads Apple	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
iPads Apple	[E.25] Perdida de equipos	9	Reducir
iPads Apple	[A.11] Acceso no autorizado	8,3	Reducir
iPads Apple	[A.23] Manipulación de hardware	8	reducir
iPads Apple	[A.24] Denegación de servicio	10	Evitar
iPads Apple	[A.25] Robo de equipos	9	Evitar
iPads Apple	[A.26] Ataque destructivo	10	Reducir
MacBook Air	[N.1] Fuego	10	Evitar
MacBook Air	[N.2] Daños por agua	9	Evitar
MacBook Air	[N] Desastres naturales	10	Asumir
MacBook Air	[I.*] Desastres industriales	10	reducir

MacBook Air	[1.3] Contaminación medioambiental	9	reducir
MacBook Air	[I.4] Contaminación electromagnética	7	reducir
MacBook Air	[1.5.2] Avería de origen físico	9	Reducir
MacBook Air	[I.6] Corte del suministro eléctrico	10	Evitar
MacBook Air	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
MacBook Air	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	reducir
MacBook Air	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
MacBook Air	[E.25] Perdida de equipos	9	Reducir
MacBook Air	[A.11] Acceso no autorizado	8,3	Reducir
MacBook Air	[A.23] Manipulación de hardware	8,5	reducir
MacBook Air	[A.24] Denegación de servicio	10	Evitar
MacBook Air	[A.25] Robo de equipos	9	Evitar
MacBook Air	[A.26] Ataque destructivo	10	reducir
Monitores	[N.1] Fuego	10	Evitar
Monitores	[N.2] Daños por agua	9	Evitar
Monitores	[N] Desastres naturales	10	Asumir
Monitores	[I.*] Desastres industriales	10	Reducir
Monitores	[1.3] Contaminación medioambiental	9	Reducir
Monitores	[I.4] Contaminación electromagnética	7	reducir
Monitores	[1.5.2] Avería de origen físico	9	Reducir
Monitores	[I.6] Corte del suministro eléctrico	10	Evitar
Monitores	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Monitores	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	reducir
Monitores	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
Monitores	[E.25] Perdida de equipos	9	Reducir
Monitores	[A.11] Acceso no autorizado	8,3	Reducir
Monitores	[A.23] Manipulación de hardware	7	Reducir
Monitores	[A.24] Denegación de servicio	10	Evitar
Monitores	[A.25] Robo de equipos	9	Evitar
Monitores	[A.26] Ataque destructivo	10	Reducir
Mouse	[N.1] Fuego	10	Evitar
Mouse	[N.2] Daños por agua	9	Evitar
Mouse	[N] Desastres naturales	10	Asumir
Mouse	[I.*] Desastres industriales	10	Reducir
Mouse	[1.3] Contaminación medioambiental	9	reducir
Mouse	[I.4] Contaminación electromagnética	7	Reducir
Mouse	[1.5.2] Avería de origen físico	9	Reducir
Mouse	[I.6] Corte del suministro eléctrico	10	Evitar

Mouse	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Reducir
Mouse	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Reducir
Mouse	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
Mouse	[E.25] Perdida de equipos	8,5	Evitar
Mouse	[A.11] Acceso no autorizado	7	Reducir
Mouse	[A.23] Manipulación de hardware	8	Reducir
Mouse	[A.24] Denegación de servicio	10	Evitar
Mouse	[A.25] Robo de equipos	8,5	Evitar
Mouse	[A.26] Ataque destructivo	10	Reducir
Server Dell	[N.1] Fuego	10	Evitar
Server Dell	[N.2] Daños por agua	9	Evitar
Server Dell	[N] Desastres naturales	10	Asumir
Server Dell	[I.*] Desastres industriales	10	Reducir
Server Dell	[1.3] Contaminación medioambiental	9	Reducir
Server Dell	[I.4] Contaminación electromagnética	7	Reducir
Server Dell	[1.5.2] Avería de origen físico	9	Evitar
Server Dell	[I.6] Corte del suministro eléctrico	9	Evitar
Server Dell	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Server Dell	[I.11] Emanaciones electromagnéticas (TEMPEST)	10	Reducir
Server Dell	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
Server Dell	[E.25] Perdida de equipos	9	Evitar
Server Dell	[A.11] Acceso no autorizado	8,3	Reducir
Server Dell	[A.23] Manipulación de hardware	9	reducir
Server Dell	[A.24] Denegación de servicio	10	Evitar
Server Dell	[A.25] Robo de equipos	9	reducir
Server Dell	[A.26] Ataque destructivo	10	Reducir
Tablet Lenovo	[N.1] Fuego	10	Evitar
Tablet Lenovo	[N.2] Daños por agua	9	Evitar
Tablet Lenovo	[N] Desastres naturales	10	Asumir
Tablet Lenovo	[I.*] Desastres industriales	10	Reducir
Tablet Lenovo	[1.3] Contaminación medioambiental	9	reducir
Tablet Lenovo	[I.4] Contaminación electromagnética	7	Reducir
Tablet Lenovo	[1.5.2] Avería de origen físico	9	Reducir
Tablet Lenovo	[I.6] Corte del suministro eléctrico	10	Evitar
Tablet Lenovo	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Tablet Lenovo	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Reducir
Tablet Lenovo	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir

Tablet Lenovo	[E.25] Perdida de equipos	9	Evitar
Tablet Lenovo	[A.11] Acceso no autorizado	8,3	Reducir
Tablet Lenovo	[A.23] Manipulación de hardware	8	Reducir
Tablet Lenovo	[A.24] Denegación de servicio	10	Evitar
Tablet Lenovo	[A.25] Robo de equipos	9	Evitar
Tablet Lenovo	[A.26] Ataque destructivo	10	Reducir
Teclados	[N.1] Fuego	10	Evitar
Teclados	[N.2] Daños por agua	9	Evitar
Teclados	[N] Desastres naturales	10	Asumir
Teclados	[I.*] Desastres industriales	10	Reducir
Teclados	[1.3] Contaminación medioambiental	9	Reducir
Teclados	[I.4] Contaminación electromagnética	7	Reducir
Teclados	[1.5.2] Avería de origen físico	9	Reducir
Teclados	[I.6] Corte del suministro eléctrico	10	Evitar
Teclados	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Teclados	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Reducir
Teclados	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
Teclados	[E.25] Perdida de equipos	8,5	Evitar
Teclados	[A.11] Acceso no autorizado	7	Reducir
Teclados	[A.23] Manipulación de hardware	8	Reducir
Teclados	[A.24] Denegación de servicio	10	Evitar
Teclados	[A.25] Robo de equipos	8,5	Evitar
Teclados	[A.26] Ataque destructivo	10	Reducir
TV	[N.1] Fuego	10	Evitar
TV	[N.2] Daños por agua	9	Evitar
TV	[N] Desastres naturales	10	Asumir
TV	[I.*] Desastres industriales	10	Reducir
TV	[1.3] Contaminación medioambiental	9	Reducir
TV	[I.4] Contaminación electromagnética	7	Reducir
TV	[1.5.2] Avería de origen físico	9	Reducir
TV	[I.6] Corte del suministro eléctrico	10	Evitar
TV	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
TV	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Reducir
TV	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
TV	[E.25] Perdida de equipos	8,5	Evitar
TV	[A.11] Acceso no autorizado	7	Reducir
TV	[A.23] Manipulación de hardware	8	Reducir
TV	[A.24] Denegación de servicio	10	Evitar
TV	[A.25] Robo de equipos	8,5	Evitar

TV	[A.26] Ataque destructivo	10	Reducir
Amplificadores	[N.1] Fuego	10	Evitar
Amplificadores	[N.2] Daños por agua	9	Evitar
Amplificadores	[N] Desastres naturales	10	Asumir
Amplificadores	[I.*] Desastres industriales	10	Reducir
Amplificadores	[1.3] Contaminación medioambiental	9	Reducir
Amplificadores	[I.4] Contaminación electromagnética	7	Reducir
Amplificadores	[1.5.2] Avería de origen físico	9	Reducir
Amplificadores	[I.6] Corte del suministro eléctrico	10	Evitar
Amplificadores	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Amplificadores	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Reducir
Amplificadores	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
Amplificadores	[E.25] Perdida de equipos	8,5	Evitar
Amplificadores	[A.11] Acceso no autorizado	7	Reducir
Amplificadores	[A.23] Manipulación de hardware	8	Reducir
Amplificadores	[A.24] Denegación de servicio	10	Evitar
Amplificadores	[A.25] Robo de equipos	8,5	Evitar
Amplificadores	[A.26] Ataque destructivo	10	Reducir
Aspiradores	[N.1] Fuego	10	Evitar
Aspiradores	[N.2] Daños por agua	9	Evitar
Aspiradores	[N] Desastres naturales	10	Asumir
Aspiradores	[I.*] Desastres industriales	10	Reducir
Aspiradores	[1.3] Contaminación medioambiental	9	Reducir
Aspiradores	[I.4] Contaminación electromagnética	7	Reducir
Aspiradores	[1.5.2] Avería de origen físico	9	Reducir
Aspiradores	[I.6] Corte del suministro eléctrico	10	Reducir
Aspiradores	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Aspiradores	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Reducir
Aspiradores	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
Aspiradores	[E.25] Perdida de equipos	8,5	Evitar
Aspiradores	[A.11] Acceso no autorizado	7	Reducir
Aspiradores	[A.23] Manipulación de hardware	8	Reducir
Aspiradores	[A.24] Denegación de servicio	10	Evitar
Aspiradores	[A.25] Robo de equipos	8,5	Evitar
Aspiradores	[A.26] Ataque destructivo	10	Reducir
Lectores de huellas	[N.1] Fuego	10	Evitar
Lectores de huellas	[N.2] Daños por agua	9	Evitar
Lectores de huellas	[N] Desastres naturales	10	Asumir
Lectores de huellas	[I.*] Desastres industriales	10	Reducir

Lectores de huellas	[1.3] Contaminación medioambiental	9	Reducir
Lectores de huellas	[I.4] Contaminación electromagnética	7	Reducir
Lectores de huellas	[1.5.2] Avería de origen físico	9	Reducir
Lectores de huellas	[I.6] Corte del suministro eléctrico	10	Evitar
Lectores de huellas	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Lectores de huellas	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Reducir
Lectores de huellas	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
Lectores de huellas	[E.25] Perdida de equipos	9	Evitar
Lectores de huellas	[A.11] Acceso no autorizado	8,3	Reducir
Lectores de huellas	[A.23] Manipulación de hardware	8	Reducir
Lectores de huellas	[A.24] Denegación de servicio	10	Evitar
Lectores de huellas	[A.25] Robo de equipos	9	Evitar
Lectores de huellas	[A.26] Ataque destructivo	10	Reducir
Biométricos	[N.1] Fuego	10	Evitar
Biométricos	[N.2] Daños por agua	9	Evitar
Biométricos	[N] Desastres naturales	10	Evitar
Biométricos	[I.*] Desastres industriales	10	Evitar
Biométricos	[1.3] Contaminación medioambiental	9	Evitar
Biométricos	[I.4] Contaminación electromagnética	7	Evitar
Biométricos	[1.5.2] Avería de origen físico	9	Evitar
Biométricos	[I.6] Corte del suministro eléctrico	10	Evitar
Biométricos	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Biométricos	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Evitar
Biométricos	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
Biométricos	[E.25] Perdida de equipos	8,5	Evitar
Biométricos	[A.11] Acceso no autorizado	7	Reducir
Biométricos	[A.23] Manipulación de hardware	8	Reducir
Biométricos	[A.24] Denegación de servicio	10	Evitar
Biométricos	[A.25] Robo de equipos	8,5	Evitar
Biométricos	[A.26] Ataque destructivo	10	Reducir
Celulares	[N.1] Fuego	10	Evitar
Celulares	[N.2] Daños por agua	9	Evitar
Celulares	[N] Desastres naturales	10	Evitar
Celulares	[I.*] Desastres industriales	10	Evitar
Celulares	[1.3] Contaminación medioambiental	9	Evitar
Celulares	[I.4] Contaminación electromagnética	7	Evitar
Celulares	[1.5.2] Avería de origen físico	9	Evitar
Celulares	[I.6] Corte del suministro eléctrico	10	Evitar

Celulares	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Celulares	[I.11] Emanaciones electromagnéticas (TEMPEST)	10	Evitar
Celulares	[E.23] Errores de mantenimiento / actualización de equipos	2	Reducir
Celulares	[E.25] Perdida de equipos	5	Evitar
Celulares	[A.11] Acceso no autorizado	7	Reducir
Celulares	[A.23] Manipulación de hardware	8	Reducir
Celulares	[A.24] Denegación de servicio	10	Evitar
Celulares	[A.25] Robo de equipos	9	Evitar
Celulares	[A.26] Ataque destructivo	10	Reducir
Micrófonos	[N.1] Fuego	10	Evitar
Micrófonos	[N.2] Daños por agua	9	Evitar
Micrófonos	[N] Desastres naturales	10	Evitar
Micrófonos	[I.*] Desastres industriales	10	Evitar
Micrófonos	[1.3] Contaminación medioambiental	9	Evitar
Micrófonos	[I.4] Contaminación electromagnética	7	Evitar
Micrófonos	[1.5.2] Avería de origen físico	9	Evitar
Micrófonos	[I.6] Corte del suministro eléctrico	10	Evitar
Micrófonos	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Micrófonos	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Evitar
Micrófonos	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
Micrófonos	[E.25] Perdida de equipos	8,5	Evitar
Micrófonos	[A.11] Acceso no autorizado	7	Reducir
Micrófonos	[A.23] Manipulación de hardware	8	Reducir
Micrófonos	[A.24] Denegación de servicio	10	Evitar
Micrófonos	[A.25] Robo de equipos	8,5	Evitar
Micrófonos	[A.26] Ataque destructivo	10	Reducir
Televisores	[N.1] Fuego	10	Evitar
Televisores	[N.2] Daños por agua	9	Evitar
Televisores	[N] Desastres naturales	10	Evitar
Televisores	[I.*] Desastres industriales	10	Evitar
Televisores	[1.3] Contaminación medioambiental	9	Evitar
Televisores	[I.4] Contaminación electromagnética	7	Evitar
Televisores	[1.5.2] Avería de origen físico	9	Evitar
Televisores	[I.6] Corte del suministro eléctrico	10	Evitar
Televisores	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Televisores	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Evitar
Televisores	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir

Televisores	[E.25] Perdida de equipos	8,5	Evitar
Televisores	[A.11] Acceso no autorizado	7	Reducir
Televisores	[A.23] Manipulación de hardware	8	Reducir
Televisores	[A.24] Denegación de servicio	10	Evitar
Televisores	[A.25] Robo de equipos	8,5	Evitar
Televisores	[A.26] Ataque destructivo	10	Reducir
Alcancel	[N.1] Fuego	10	Evitar
Alcancel	[N.2] Daños por agua	9	Evitar
Alcancel	[N] Desastres naturales	10	Evitar
Alcancel	[I.*] Desastres industriales	10	Evitar
Alcancel	[1.3] Contaminación medioambiental	9	Evitar
Alcancel	[I.4] Contaminación electromagnética	7	Evitar
Alcancel	[1.5.2] Avería de origen físico	9	Evitar
Alcancel	[I.6] Corte del suministro eléctrico	10	Evitar
Alcancel	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Alcancel	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Evitar
Alcancel	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
Alcancel	[E.25] Perdida de equipos	7,5	Evitar
Alcancel	[A.11] Acceso no autorizado	7	Reducir
Alcancel	[A.23] Manipulación de hardware	8,5	Reducir
Alcancel	[A.24] Denegación de servicio	10	Evitar
Alcancel	[A.25] Robo de equipos	7,5	Evitar
Alcancel	[A.26] Ataque destructivo	10	Reducir
Estanterías	[N.1] Fuego	10	Evitar
Estanterías	[N.2] Daños por agua	9	Evitar
Estanterías	[N] Desastres naturales	10	Evitar
Estanterías	[I.*] Desastres industriales	10	Evitar
Estanterías	[1.3] Contaminación medioambiental	9	Evitar
Estanterías	[I.4] Contaminación electromagnética	7	Evitar
Estanterías	[1.5.2] Avería de origen físico	9	Evitar
Estanterías	[I.6] Corte del suministro eléctrico	10	Evitar
Estanterías	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Estanterías	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Evitar
Estanterías	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
Estanterías	[E.25] Perdida de equipos	9	Evitar
Estanterías	[A.11] Acceso no autorizado	8,3	Reducir
Estanterías	[A.23] Manipulación de hardware	8	Reducir
Estanterías	[A.24] Denegación de servicio	10	Evitar
Estanterías	[A.25] Robo de equipos	9	Evitar

Estanterías	[A.26] Ataque destructivo	10	Reducir
Rótulos	[N.1] Fuego	10	Evitar
Rótulos	[N.2] Daños por agua	9	Evitar
Rótulos	[N] Desastres naturales	10	Evitar
Rótulos	[I.*] Desastres industriales	10	Evitar
Rótulos	[1.3] Contaminación medioambiental	9	Evitar
Rótulos	[I.4] Contaminación electromagnética	7	Evitar
Rótulos	[1.5.2] Avería de origen físico	9	Evitar
Rótulos	[I.6] Corte del suministro eléctrico	10	Evitar
Rótulos	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Rótulos	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Evitar
Rótulos	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
Rótulos	[E.25] Perdida de equipos	8,5	Evitar
Rótulos	[A.11] Acceso no autorizado	7	Reducir
Rótulos	[A.23] Manipulación de hardware	8	Reducir
Rótulos	[A.24] Denegación de servicio	10	Evitar
Rótulos	[A.25] Robo de equipos	8,5	Evitar
Rótulos	[A.26] Ataque destructivo	10	Reducir
Rack	[N.1] Fuego	9	Evitar
Rack	[N.2] Daños por agua	8	Evitar
Rack	[N] Desastres naturales	9	Evitar
Rack	[I.*] Desastres industriales	9	Evitar
Rack	[1.3] Contaminación medioambiental	8	Evitar
Rack	[I.4] Contaminación electromagnética	6	Evitar
Rack	[1.5.2] Avería de origen físico	8	Evitar
Rack	[I.6] Corte del suministro eléctrico	9	Evitar
Rack	[I.7] Condiciones inadecuadas de temperatura o humedad	9	Evitar
Rack	[I.11] Emanaciones electromagnéticas (TEMPEST)	1	Evitar
Rack	[E.23] Errores de mantenimiento / actualización de equipos	6	Reducir
Rack	[E.25] Perdida de equipos	6,5	Evitar
Rack	[A.11] Acceso no autorizado	6	Reducir
Rack	[A.23] Manipulación de hardware	7,5	Reducir
Rack	[A.24] Denegación de servicio	9	Evitar
Rack	[A.25] Robo de equipos	6,5	Evitar
Rack	[A.26] Ataque destructivo	9	Reducir
Implementos instalación internet	[N.1] Fuego	10	Evitar
Implementos instalación internet	[N.2] Daños por agua	9	Evitar

Implementos instalación internet	[N] Desastres naturales	10	Evitar
Implementos instalación internet	[I.*] Desastres industriales	10	Evitar
Implementos instalación internet	[I.4] Contaminación electromagnética	7	Evitar
Implementos instalación internet	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Implementos instalación internet	[E.23] Errores de mantenimiento / actualización de equipos	7	Evitar
Implementos instalación internet	[E.25] Perdida de equipos	7	Evitar
Implementos instalación internet	[A.11] Acceso no autorizado	5,7	Reducir
Implementos instalación internet	[A.23] Manipulación de hardware	7,5	Reducir
Implementos instalación internet	[A.24] Denegación de servicio	9	Evitar
Implementos instalación internet	[A.25] Robo de equipos	8,5	Evitar
Implementos instalación internet	[A.26] Ataque destructivo	10	Reducir
OLT	[N.1] Fuego	10	Evitar
OLT	[N.2] Daños por agua	9	Evitar
OLT	[N] Desastres naturales	10	Evitar
OLT	[I.*] Desastres industriales	10	Evitar
OLT	[1.3] Contaminación medioambiental	9	Evitar
OLT	[I.4] Contaminación electromagnética	7	Evitar
OLT	[1.5.2] Avería de origen físico	9	Evitar
OLT	[I.6] Corte del suministro eléctrico	10	Evitar
OLT	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
OLT	[E.23] Errores de mantenimiento / actualización de equipos	6,3	Evitar
OLT	[E.25] Perdida de equipos	8,5	Reducir
OLT	[A.11] Acceso no autorizado	8,5	Evitar
OLT	[A.23] Manipulación de hardware	7,5	Reducir
OLT	[A.24] Denegación de servicio	10	Reducir
OLT	[A.25] Robo de equipos	8,5	Evitar
OLT	[A.26] Ataque destructivo	10	Evitar
Unidades de almacenamiento	[N.1] Fuego	10	Evitar
Unidades de almacenamiento	[N.2] Daños por agua	9	Evitar
Unidades de almacenamiento	[N] Desastres naturales	10	Evitar
Unidades de almacenamiento	[I.*] Desastres industriales	10	Evitar
Unidades de almacenamiento	[1.3] Contaminación medioambiental	9	Evitar

Unidades de almacenamiento	[I.4] Contaminación electromagnética	7	Evitar
Unidades de almacenamiento	[1.5.2] Avería de origen físico	9	Evitar
Unidades de almacenamiento	[I.6] Corte del suministro eléctrico	10	Evitar
Unidades de almacenamiento	[I.7] Condiciones inadecuadas de temperatura o humedad	10	Evitar
Unidades de almacenamiento	[I.11] Emanaciones electromagnéticas (TEMPEST)	2	Evitar
Unidades de almacenamiento	[E.23] Errores de mantenimiento / actualización de equipos	6,7	Reducir
Unidades de almacenamiento	[E.25] Perdida de equipos	9	Evitar
Unidades de almacenamiento	[A.11] Acceso no autorizado	8	Reducir
Unidades de almacenamiento	[A.23] Manipulación de hardware	8	Reducir
Unidades de almacenamiento	[A.24] Denegación de servicio	10	Evitar
Unidades de almacenamiento	[A.25] Robo de equipos	9	Evitar
Unidades de almacenamiento	[A.26] Ataque destructivo	10	Reducir
	Comunicaciones		
Teléfonos	[I.8] Fallo de servicios de comunicación	9	Evitar
Teléfonos	[E.2] Errores del administrador del sistema / de la seguridad	7,3	Reducir
Teléfonos	[E.24] Caída del sistema por agotamiento de recursos	9	Reducir
Teléfonos	[A.7] Uso no previsto	6,3	Evitar
Teléfonos	[A.18] Destrucción de la información	9	Evitar
Teléfonos	[A.24] Denegación de servicio	9	Reducir
	Auxiliares		
Escaleras	[N.1] Fuego	10	Evitar
Escaleras	[N.2] Daños por agua	9	Evitar
Escaleras	[N] Desastres naturales	10	Asumir
Escaleras	[I.*] Desastres industriales	10	Evitar
Escaleras	[1.3] Contaminación medioambiental	9	Evitar
Escaleras	[I.4] Contaminación electromagnética	9	Evitar
Escaleras	[A.23] Manipulación de hardware	8	Evitar
Escaleras	[A.25] Robo de equipos	7	Evitar
Escaleras	[A.26] Ataque destructivo	7	Reducir
Generadores	[N.1] Fuego	10	Evitar
Generadores	[N.2] Daños por agua	9	Evitar
Generadores	[N] Desastres naturales	10	Asumir
Generadores	[I.*] Desastres industriales	3,4	Evitar
Generadores	[1.3] Contaminación medioambiental	9	Evitar

Generadores	[I.4] Contaminación electromagnética	9	Evitar
Generadores	[1.5.2] Avería de origen físico	9	Evitar
Generadores	[E.23] Errores de mantenimiento / actualización de equipos	7	Evitar
Generadores	[A.23] Manipulación de hardware	9	Reducir
Generadores	[A.25] Robo de equipos	10	Evitar
Generadores	[A.26] Ataque destructivo	10	Evitar
Sillas	[N.1] Fuego	10	Evitar
Sillas	[N.2] Daños por agua	9	Evitar
Sillas	[N] Desastres naturales	10	Asumir
Sillas	[I.*] Desastres industriales	10	Evitar
Sillas	[1.3] Contaminación medioambiental	9	Evitar
Sillas	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
Sillas	[A.23] Manipulación de hardware	8	Reducir
Sillas	[A.25] Robo de equipos	7	Evitar
Sillas	[A.26] Ataque destructivo	7	Reducir
Balanzas	[N.1] Fuego	10	Evitar
Balanzas	[N.2] Daños por agua	9	Evitar
Balanzas	[N] Desastres naturales	10	Asumir
Balanzas	[I.*] Desastres industriales	10	Evitar
Balanzas	[1.3] Contaminación medioambiental	9	Evitar
Balanzas	[I.4] Contaminación electromagnética	9	Evitar
Balanzas	[1.5.2] Avería de origen físico	1	Reducir
Balanzas	[E.23] Errores de mantenimiento / actualización de equipos	8	Reducir
Balanzas	[E.25] Perdida de equipos	7	Evitar
Balanzas	[A.23] Manipulación de hardware	8	Reducir
Balanzas	[A.25] Robo de equipos	7	Evitar
Balanzas	[A.26] Ataque destructivo	7	Reducir
Camilla	[N.1] Fuego	10	Evitar
Camilla	[N.2] Daños por agua	9	Evitar
Camilla	[N] Desastres naturales	10	Asumir
Camilla	[I.*] Desastres industriales	10	Evitar
Camilla	[A.23] Manipulación de hardware	8	Reducir
Camilla	[A.25] Robo de equipos	7	Evitar
Camilla	[A.26] Ataque destructivo	7	Reducir
Linternas	[N.1] Fuego	9	Evitar
Linternas	[N.2] Daños por agua	8	Evitar
Linternas	[N] Desastres naturales	9	Asumir
Linternas	[I.*] Desastres industriales	9	Evitar
Linternas	[1.3] Contaminación medioambiental	9	Reducir
Linternas	[A.23] Manipulación de hardware	4	Evitar
Linternas	[A.25] Robo de equipos	3	Evitar

Linternas	[A.26] Ataque destructivo	6	Reducir
Perforadoras	[N.1] Fuego	5	Evitar
Perforadoras	[N.2] Daños por agua	4	Evitar
Perforadoras	[N] Desastres naturales	5	Asumir
Perforadoras	[I.*] Desastres industriales	5	Evitar
Perforadoras	[1.3] Contaminación medioambiental	4	Reducir
Perforadoras	[A.23] Manipulación de hardware	2	Evitar
Perforadoras	[A.25] Robo de equipos	1	Evitar
Perforadoras	[A.26] Ataque destructivo	2	Reducir
Recogedores	[N.1] Fuego	5	Evitar
Recogedores	[N.2] Daños por agua	4	Evitar
Recogedores	[N] Desastres naturales	5	Asumir
Recogedores	[I.*] Desastres industriales	5	Evitar
Recogedores	[1.3] Contaminación medioambiental	4	Reducir
Recogedores	[A.23] Manipulación de hardware	2	Evitar
Recogedores	[A.25] Robo de equipos	1	Evitar
Recogedores	[A.26] Ataque destructivo	2	Reducir
Regletas	[N.1] Fuego	9	Evitar
Regletas	[N.2] Daños por agua	9	Evitar
Regletas	[E.23] Errores de mantenimiento / actualización de equipos	5	Asumir
Regletas	[E.25] Perdida de equipos	4	Evitar
Pizarrones	[N.1] Fuego	10	Reducir
Pizarrones	[N.2] Daños por agua	9	Evitar
Pizarrones	[N] Desastres naturales	10	Evitar
Pizarrones	[I.*] Desastres industriales	10	Reducir
Pizarrones	[A.26] Ataque destructivo	7	Reducir
Sellos de oficina	[N.1] Fuego	9	Evitar
Sellos de oficina	[N.2] Daños por agua	10	Evitar
Sellos de oficina	[N] Desastres naturales	10	Asumir
Sellos de oficina	[A.11] Acceso no autorizado	5,5	Evitar
Sellos de oficina	[A.23] Manipulación de hardware	5,5	Reducir
Sellos de oficina	[A.24] Denegación de servicio	10	Evitar
Microondas	[N.1] Fuego	10	Evitar
Microondas	[N.2] Daños por agua	9	Reducir
Microondas	[N] Desastres naturales	10	Asumir
Microondas	[A.23] Manipulación de hardware	5	Reducir
Microondas	[A.25] Robo de equipos	4	Evitar
Microcomponentes	[N.1] Fuego	10	Evitar
Microcomponentes	[N.2] Daños por agua	10	Evitar
Microcomponentes	[N] Desastres naturales	10	Asumir
Microcomponentes	[1.3] Contaminación medioambiental	9	Evitar
Microcomponentes	[A.23] Manipulación de hardware	5	Reducir

Microcomponentes	[A.24] Denegación de servicio	4	Reducir
Microcomponentes	[A.25] Robo de equipos	7	Evitar
Microcomponentes	[A.26] Ataque destructivo	7	Reducir
Lectores de barras	[N.1] Fuego	10	Evitar
Lectores de barras	[N.2] Daños por agua	9	Evitar
Lectores de barras	[N] Desastres naturales	10	Asumir
Lectores de barras	[I.*] Desastres industriales	10	Reducir
Lectores de barras	[1.3] Contaminación medioambiental	9	Reducir
Lectores de barras	[E.23] Errores de mantenimiento / actualización de equipos	7	Evitar
Lectores de barras	[A.23] Manipulación de hardware	6	Reducir
Lectores de barras	[A.25] Robo de equipos	5	Evitar
Lectores de barras	[A.26] Ataque destructivo	7	Evitar
Dispensador de agua	[N.1] Fuego	10	Evitar
Dispensador de agua	[N.2] Daños por agua	9	Evitar
Dispensador de agua	[N] Desastres naturales	10	Asumir
Dispensador de agua	[I.*] Desastres industriales	10	Reducir
Dispensador de agua	[1.3] Contaminación medioambiental	9	Reducir
Dispensador de agua	[E.23] Errores de mantenimiento / actualización de equipos	7	Evitar
Dispensador de agua	[A.23] Manipulación de hardware	5	Reducir
Dispensador de agua	[A.25] Robo de equipos	4	Evitar
Mostradores de vidrio	[N.1] Fuego	10	Evitar
Mostradores de vidrio	[N.2] Daños por agua	9	Evitar
Mostradores de vidrio	[N] Desastres naturales	10	Asumir
Mostradores de vidrio	[1.3] Contaminación medioambiental	10	Reducir
Mostradores de vidrio	[A.23] Manipulación de hardware	5,5	Reducir
Mostradores de vidrio	[A.25] Robo de equipos	4,5	Evitar
Mostradores de vidrio	[A.26] Ataque destructivo	7	Reducir
Parlantes	[N.1] Fuego	10	Evitar
Parlantes	[N.2] Daños por agua	9	Evitar
Parlantes	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
Parlantes	[A.23] Manipulación de hardware	5	Reducir
Parlantes	[A.25] Robo de equipos	4	Evitar
Parlantes	[A.26] Ataque destructivo	7	Evitar
Copiadoras	[N.1] Fuego	10	Evitar
Copiadoras	[N.2] Daños por agua	9	Evitar
Copiadoras	[N] Desastres naturales	10	Reducir
Copiadoras	[1.3] Contaminación medioambiental	9	Reducir
Copiadoras	[E.23] Errores de mantenimiento / actualización de equipos	7	Evitar
Copiadoras	[A.23] Manipulación de hardware	7	Evitar
Copiadoras	[A.25] Robo de equipos	6	Evitar

Copiadoras	[A.26] Ataque destructivo	7	Evitar
Extintores	[N.1] Fuego	10	Evitar
Extintores	[N.2] Daños por agua	9	Evitar
Extintores	[N] Desastres naturales	10	Asumir
Extintores	[E.23] Errores de mantenimiento / actualización de equipos	7	Evitar
Extintores	[A.23] Manipulación de hardware	5	Reducir
Extintores	[A.25] Robo de equipos	4	Evitar
Extintores	[A.26] Ataque destructivo	7	Evitar
Casilleros metálicos	[N.1] Fuego	7	Evitar
Casilleros metálicos	[N.2] Daños por agua	7	Evitar
Casilleros metálicos	[N] Desastres naturales	7	Asumir
Casilleros metálicos	[E.23] Errores de mantenimiento / actualización de equipos	7	Reducir
Casilleros metálicos	[A.23] Manipulación de hardware	7	Reducir
Casilleros metálicos	[A.25] Robo de equipos	7	Reducir
Casilleros metálicos	[A.26] Ataque destructivo	7	Evitar
Data Fast	[N.1] Fuego	10	Evitar
Data Fast	[N.2] Daños por agua	9	Evitar
Data Fast	[N] Desastres naturales	10	Asumir
Data Fast	[I.*] Desastres industriales	10	Evitar
Data Fast	[1.3] Contaminación medioambiental	9	Evitar
Data Fast	[A.23] Manipulación de hardware	7	Reducir
Data Fast	[A.25] Robo de equipos	6	Evitar
Data Fast	[A.26] Ataque destructivo	7	Evitar
Arnés reforzado	[N.1] Fuego	10	Evitar
Arnés reforzado	[N.2] Daños por agua	9	Evitar
Arnés reforzado	[N] Desastres naturales	10	Asumir
Arnés reforzado	[I.*] Desastres industriales	10	Evitar
Arnés reforzado	[1.3] Contaminación medioambiental	9	Evitar
Arnés reforzado	[A.23] Manipulación de hardware	5	Reducir
Arnés reforzado	[A.25] Robo de equipos	4	Reducir
Arnés reforzado	[A.26] Ataque destructivo	7	Reducir
Cascos	[N.1] Fuego	10	Evitar
Cascos	[N.2] Daños por agua	9	Evitar
Cascos	[N] Desastres naturales	10	Asumir
Cascos	[I.*] Desastres industriales	10	Evitar
Cascos	[1.3] Contaminación medioambiental	9	Evitar
Cascos	[A.25] Robo de equipos	4,5	Reducir
Cascos	[A.26] Ataque destructivo	7	Reducir
Cinturones	[N.1] Fuego	10	Evitar
Cinturones	[N.2] Daños por agua	9	Evitar
Cinturones	[N] Desastres naturales	10	Asumir

Cinturones	[I.*] Desastres industriales	9	Reducir
Cinturones	[I.4] Contaminación electromagnética	9	Reducir
Cinturones	[A.25] Robo de equipos	4,5	Evitar
Cinturones	[A.26] Ataque destructivo	7	Reducir
Eslinga	[N.1] Fuego	10	Evitar
Eslinga	[N.2] Daños por agua	9	Evitar
Eslinga	[N] Desastres naturales	10	Asumir
Eslinga	[I.*] Desastres industriales	10	Reducir
Eslinga	[1.3] Contaminación medioambiental	9	Reducir
Eslinga	[A.25] Robo de equipos	4,5	Evitar
Eslinga	[A.26] Ataque destructivo	7	Reducir
Gafas	[N.1] Fuego	10	Evitar
Gafas	[N.2] Daños por agua	9	Evitar
Gafas	[N] Desastres naturales	10	Asumir
Gafas	[I.*] Desastres industriales	10	Reducir
Gafas	[A.25] Robo de equipos	4	Reducir
Gafas	[A.26] Ataque destructivo	7	Evitar
Guates	[N.1] Fuego	10	Reducir
Guates	[N.2] Daños por agua	9	Evitar
Guates	[N] Desastres naturales	10	Evitar
Guates	[I.*] Desastres industriales	10	Asumir
Guates	[A.25] Robo de equipos	4	Reducir
Guates	[A.26] Ataque destructivo	7	Reducir
Mosquetón	[N.1] Fuego	10	Evitar
Mosquetón	[N.2] Daños por agua	9	Evitar
Mosquetón	[N] Desastres naturales	10	Asumir
Mosquetón	[I.*] Desastres industriales	10	Reducir
Mosquetón	[A.25] Robo de equipos	4	Evitar
Mosquetón	[A.26] Ataque destructivo	7	Reducir
Chalecos	[N.1] Fuego	10	Evitar
Chalecos	[N.2] Daños por agua	9	Evitar
Chalecos	[N] Desastres naturales	10	Asumir
Chalecos	[I.*] Desastres industriales	10	Reducir
Chalecos	[A.25] Robo de equipos	4	Evitar
Chalecos	[A.26] Ataque destructivo	7	Reducir
Conos de seguridad	[N.1] Fuego	10	Evitar
Conos de seguridad	[N.2] Daños por agua	9	Evitar
Conos de seguridad	[N] Desastres naturales	10	Asumir
Conos de seguridad	[I.*] Desastres industriales	10	Reducir
Conos de seguridad	[A.25] Robo de equipos	4	Evitar
Conos de seguridad	[A.26] Ataque destructivo	7	Reducir
Letreros de advertencia	[N.1] Fuego	10	Evitar
Letreros de advertencia	[N.2] Daños por agua	9	Evitar

Letreros de advertencia	[N] Desastres naturales	10	Asumir
Letreros de advertencia	[I.*] Desastres industriales	10	Reducir
Letreros de advertencia	[A.25] Robo de equipos	4	Evitar
Letreros de advertencia	[A.26] Ataque destructivo	7	Reducir
Herramientas	[N.1] Fuego	10	Evitar
Herramientas	[N.2] Daños por agua	9	Evitar
Herramientas	[N] Desastres naturales	10	Asumir
Herramientas	[I.*] Desastres industriales	10	Reducir
Herramientas	[A.25] Robo de equipos	4	Evitar
Herramientas	[A.26] Ataque destructivo	7	Reducir
Case para discos duros	[N.1] Fuego	10	Evitar
Case para discos duros	[N.2] Daños por agua	10	Evitar
Case para discos duros	[I.*] Desastres industriales	10	Asumir
Case para discos duros	[A.11] Acceso no autorizado	4	Reducir
Case para discos duros	[A.23] Manipulación de hardware	6	Evitar
Apple pencil	[N.1] Fuego	10	Evitar
Apple pencil	[N.2] Daños por agua	9	Evitar
Apple pencil	[N] Desastres naturales	10	Asumir
Apple pencil	[I.*] Desastres industriales	10	Reducir
Apple pencil	[A.23] Manipulación de hardware	5,5	Reducir
Apple pencil	[A.25] Robo de equipos	4,5	Evitar
Apple pencil	[A.26] Ataque destructivo	7	Reducir
Alexa	[N.1] Fuego	10	Evitar
Alexa	[N.2] Daños por agua	9	Evitar
Alexa	[N] Desastres naturales	10	Asumir
Alexa	[A.11] Acceso no autorizado	4	Reducir
Alexa	[A.23] Manipulación de hardware	4	Reducir
Alexa	[A.25] Robo de equipos	4,5	Evitar
Alexa	[A.26] Ataque destructivo	7	Reducir
	Servicios subcontratados/ Instalaciones		
Casa Plus 1	[N.1] Fuego	10	Evitar
Casa Plus 1	[N.2] Daños por agua	10	Evitar
Casa Plus 1	[N] Desastres naturales	10	Asumir
Casa Plus 1	[I.1] Fuego	10	Evitar
Casa Plus 1	[I.*] Desastres industriales	10	Evitar
Casa Plus 1	[1.3] Contaminación medioambiental	7	Evitar
Casa Plus 1	[I.4] Contaminación electromagnética	7	Evitar
Casa Plus 1	[A.6] Abuso de privilegios de acceso	7	Reducir
Casa Plus 1	[A.25] Robo de equipos	10	Evitar
Casa Plus 1	[A.26] Ataque destructivo	10	Reducir
Casa Plus 1	[A.27] Ocupación enemiga	6	Evitar
Casa Plus 2	[N.1] Fuego	10	Evitar

Casa Plus 2	[N.2] Daños por agua	10	Evitar
Casa Plus 2	[N] Desastres naturales	10	Asumir
Casa Plus 2	[I.1] Fuego	10	Evitar
Casa Plus 2	[I.*] Desastres industriales	10	Evitar
Casa Plus 2	[1.3] Contaminación medioambiental	7	Evitar
Casa Plus 2	[I.4] Contaminación electromagnética	7	Evitar
Casa Plus 2	[A.6] Abuso de privilegios de acceso	7	Reducir
Casa Plus 2	[A.25] Robo de equipos	10	Evitar
Casa Plus 2	[A.26] Ataque destructivo	10	Reducir
Casa Plus 2	[A.27] Ocupación enemiga	6	Evitar
	Personal		
Gerencia General	[E.15] Alteración de la información	6	Reducir
Gerencia General	[E.18] Destrucción de información	4	Evitar
Gerencia General	[E.19] Fuga de información	2	Evitar
Gerencia General	[E.28] Indisponibilidad de personal	7	Reducir
Gerencia General	[A.15] Modificación de la información	8	Reducir
Gerencia General	[A.18] Destrucción de la información	7	Evitar
Gerencia General	[A.19] Revelación de información	4	Evitar
Gerencia General	[E.28] Indisponibilidad de personal	9	Reducir
Gerencia General	[A.29] Extorsión	9	Evitar
Gerencia General	[A.30] Ingeniería Social (picaresca)	6	Evitar
Gerencia Operativa	[E.15] Alteración de la información	7	Reducir
Gerencia Operativa	[E.18] Destrucción de información	4	Evitar
Gerencia Operativa	[E.19] Fuga de información	5,7	Evitar
Gerencia Operativa	[E.28] Indisponibilidad de personal	7	Reducir
Gerencia Operativa	[A.15] Modificación de la información	9	Reducir
Gerencia Operativa	[A.18] Destrucción de la información	7	Evitar
Gerencia Operativa	[A.19] Revelación de información	9	Evitar
Gerencia Operativa	[E.28] Indisponibilidad de personal	9	Reducir
Gerencia Operativa	[A.29] Extorsión	9,7	Evitar
Gerencia Operativa	[A.30] Ingeniería Social (picaresca)	9,7	Evitar
Gerencia Administrativa	[E.15] Alteración de la información	4	Reducir
Gerencia Administrativa	[E.18] Destrucción de información	6	Evitar
Gerencia Administrativa	[E.19] Fuga de información	4	Evitar
Gerencia Administrativa	[E.28] Indisponibilidad de personal	2	Reducir
Gerencia Administrativa	[A.15] Modificación de la información	8	Reducir
Gerencia Administrativa	[A.18] Destrucción de la información	8	Evitar
Gerencia Administrativa	[A.19] Revelación de información	7	Evitar
Gerencia Administrativa	[E.28] Indisponibilidad de personal	4	Reducir
Gerencia Administrativa	[A.29] Extorsión	9	Evitar
Gerencia Administrativa	[A.30] Ingeniería Social (picaresca)	6,3	Evitar
Gerencia Atención al Cliente	[E.15] Alteración de la información	6	Reducir

Gerencia Atención al Cliente	[E.18] Destrucción de información	4	Evitar
Gerencia Atención al Cliente	[E.19] Fuga de información	1	Evitar
Gerencia Atención al Cliente	[E.28] Indisponibilidad de personal	2	Reducir
Gerencia Atención al Cliente	[A.15] Modificación de la información	8	Reducir
Gerencia Atención al Cliente	[A.18] Destrucción de la información	8	Evitar
Gerencia Atención al Cliente	[A.19] Revelación de información	2	Evitar
Gerencia Atención al Cliente	[E.28] Indisponibilidad de personal	9	Reducir
Gerencia Atención al Cliente	[A.29] Extorsión	5,3	Evitar
Gerencia Atención al Cliente	[A.30] Ingeniería Social (picaresca)	6,3	Evitar
Gerencia comercial	[E.15] Alteración de la información	6	Reducir
Gerencia comercial	[E.18] Destrucción de información	2	Evitar
Gerencia comercial	[E.19] Fuga de información	5,7	Evitar
Gerencia comercial	[E.28] Indisponibilidad de personal	7	Reducir
Gerencia comercial	[A.15] Modificación de la información	5,7	Reducir
Gerencia comercial	[A.18] Destrucción de la información	7	Evitar
Gerencia comercial	[A.19] Revelación de información	3	Evitar
Gerencia comercial	[E.28] Indisponibilidad de personal	9	Reducir
Gerencia comercial	[A.29] Extorsión	5,7	Evitar
Gerencia comercial	[A.30] Ingeniería Social (picaresca)	5,7	Evitar

Nota: Elaboración Propia.

Anexo 7 Políticas de Seguridad de la Información

Dominio	Resumen de Objetivo y Control	Detalles de Políticas
1. Políticas de Seguridad	1.1 Directrices de la Dirección en Seguridad de la Información 1.1.1. Conjunto de políticas que estén a favor de la seguridad de la información. 1.1.2. Revisión de políticas de seguridad	Políticas generales. Definición de la documentación dentro de los requisitos legales y regulatorios en vigencia. Definir procesos para identificar, evaluar y mitigar los riesgos de seguridad de la información.

2. Aspectos Organizativos	**2.1 Organización interna** 2.1.1 Asignación de responsables 2.1.2 Asignación de tareas 2.1.3 Seguridad de la información en la gestión de proyectos **2.2 Dispositivos para trabajo remoto** 2.2.1 Dispositivos y red que permita el desempeño de labores de forma remota.	La empresa debe tener personal capacitado en seguridad de la información en la empresa de internet AIRMAXTELECOM Soluciones Tecnológicas S.A. con la finalidad de periódicamente establecer políticas de seguridad de la información, capacitar al personal y asignar roles y actividades para lograr tener un óptimo desempeño.
3. Seguridad en RRHH	**3.1 Antes de contratar** 3.1.1 Entrevista y revisión de antecedentes. 3.1.2 Términos y condiciones **3.2 Durante el contrato** 3.2.1 Responsabilidad en la gestión. 3.2.2 Conocimiento de la formación en su vida académica.	La empresa debe realizar el proceso de capacitación en cuanto a los lineamientos y políticas relevantes.
4. Gestión de activos	**4.1 Responsabilidad de activos** 4.1.1 Realizar periódicamente el levantamiento de activos. 4.1.2 Utilizar de forma adecuada los activos. 4.1.3 Realizar el análisis de riesgos y amenazas para	El personal encargado de realizar la gestión de activos debe comprender la importancia de tener un inventario de los activos de la empresa con la finalidad de ser analizados ante los posibles riesgos.

	contrarrestarlas periódicamente.	Establecer manuales para la gestión de activos, administrar las instalaciones, realizar backups de la información, monitorear los sistemas.
	4.2 Manejo de almacenamiento	
	4.2.1 Gestión de almacenamiento de los activos.	
	4.2.2 Almacenar de forma segura los activos, con cerraduras adecuadas.	
	5.1 Requerimientos de acceso.	
	5.1.1 Políticas de control de acceso.	
	5.1.2 Portar las credenciales de la empresa para conceder el acceso.	
	5.2 Gestión de acceso de usuarios.	Establecer manuales para el control de acceso.
5. Controles de acceso	5.2.1 Manejo y uso correcto de la información de acceso y autenticación.	Políticas que delimiten el acceso al personal de acuerdo con el área de trabajo.
	5.3 Control de accesos a sistemas.	Revisión de accesos de usuario.
	5.3.1 Restringir el acceso no autorizado.	
	5.3.2 Delimitar el acceso al personal solamente al área designada para desarrollar sus tareas.	

	5.3.3 Procedimientos de acceso seguro e inicios de sesión.	
6. Cifrado	**6.1 Controles criptográficos** 6.1.1 Gestión de claves 6.1.2 Cambio periódico de claves de acuerdo con pautas en las que debe estar una contraseña.	Definir estándares en los cuales debe ir una contraseña tales como: • Mayúsculas • Minúsculas • Números • Caracteres. • No usar contraseñas como fechas o nombres de la empresa.
7. Seguridad física	**7.1 Áreas seguras.** 7.1.1 Protección en los ingresos al establecimiento. 7.1.2 Delimitar el acceso a ciertas áreas solo a personal autorizado. 7.1.3 Mantener aseguradas las áreas en donde se resguarda información. 7.1.4 Mantener los gabinetes y estanterías con puertas y candados. **7.2 Seguridad de los activos** 7.2.1 Protección segura para los activos.	Establecer y delimitar normativas en las cuales se garantice el orden y cuidado de los activos. Delimitar el acceso a las áreas sensibles en el caso de personal que no pertenezca a la empresa o practicantes.

	7.2.2 Mantenimiento preventivo y correctivo de los equipos.	
	7.2.3 Auditorias constantes a los activos físicos e instalaciones**.**	
	8.1 Responsabilidad operacional	
	8.1.1 Documentación en regla de los procesos empresariales.	
	8.2 Registro de actividades.	
8. Seguridad operativa	8.2.1 Monitoreo y registro continuo de actividades del personal de la empresa ya sea de las actividades que se realizan a nivel operativo y de sistemas.	Determinar políticas de seguridad operacional para constante monitoreo de actividades en hardware y software.
	8.3 Gestión de vulnerabilidades	Revisión de licencias adecuadas en los sistemas que se utilizan en la empresa.
	8.3.1 Restricción de software o instalación de licencias no autorizadas.	
	8.3.2 Mantener las licencias de los dispositivos en condiciones óptimas, Office, Antivirus.	
	8.3.3 Auditorias a los sistemas.	
	9.1 Gestión de comunicación	Políticas de seguridad de intercambio de información.
9. Seguridad en telecomunicaciones	9.1.1 Controles de servicios en la red.	Controles y protección de datos a los cuales se tiene acceso.

	9.2 Intercambio de información.	Limitar la información que se puede informas a personas externas de la empresa.
	9.2.1 Políticas y procedimientos que controlen el intercambio de información.	Pruebas de funcionalidad y confidencialidad en la comunicación de la empresa.
	9.2.2 Clausulas de acuerdos de confidencialidad.	
	9.2.3 Cifrado de extremo a extremo.	
	9.2.4 Pautas de uso seguro de dispositivos.	
	9.2.5 Principios de protección en base a la ingeniería en sistemas.	
	9.2.6 Pruebas de correcta funcionalidad.	
	10.1 Seguridad en los sistemas de información	
10. Mantenimiento de sistemas de información	10.1.1 Establecer parámetros de seguridad.	Garantizar la protección de datos, realizando pruebas periódicamente a los sistemas, controlando que no haya perdida o alteración de información.
	10.1.2 Protección de transacciones.	
	10.1.3 Contraseñas estandarizadas y su protección.	Garantizar la confidencialidad e integridad de la información sensible para el acceso en áreas no autorizadas.
	10.1.4 Pruebas de ataques al sistema y reforzar la seguridad periódicamente.	
	10.1.5 Licencias y antivirus originales.	

	10.1.6 Seguridad en el entorno de desarrollo. 10.1.7 Mejora continua.	
11. Relaciones con suministros	**11.1 Seguridad de suministros.** 11.1.1 Políticas de seguridad tanto de las instalaciones, activos como seguridad de la información en cuanto a proveedores.	Mantener acuerdos de confidencialidad con proveedores que tengan acceso o contacto con personal de la empresa, instalaciones o equipos por parte de la empresa AIRMAXTELECOM Soluciones Tecnológicas S.A.
12. Gestión de incidentes en la seguridad de la información	**12.1 Gestión de incidentes.** 12.1.1 Procedimientos ante vulnerabilidades en la información. 12.1.2 Capacitación ante incidentes que comprometan la información. 12.1.3 Toma de decisiones. 12.1.3 Mejora continua en la gestión de seguridad.	Mantener informado al personal que conforma la empresa sobre la gestión de incidentes y la toma de decisiones ante posibles escenarios. Cumplir a cabalidad con el proceso de gestión de riesgos.
13. Seguridad de la información y continuidad de negocio	**13.1 Continuidad y seguridad de la información** 13.1.1 Planes de continuidad de negocio. 13.1.2 Continuidad del negocio en aspectos de seguridad de la información.	Garantizar la continuidad del negocio pese a cualquier suceso que pueda presentarse, manteniendo la seguridad de la información, ya sea por causa de factores externos o naturales que son imperceptibles a cuando puedan suceder.

	13.1.3 Proveer del servicio ante eventos externos a la empresa.	
14. Recuperación del servicio	**14.1 Plan de recuperación del servicio.** 14.1.1 Plan re recuperar el servicio en el menor tiempo posible y bridar el servicio a los clientes.	Tener lineamientos y procedimientos a seguir para levantar nuevamente el servicio en el menor tiempo posible.
15. Uso responsable de dispositivos	**15.1 Regulación de uso en dispositivos** 15.1.1 Regular el uso de redes sociales o actividades de ocio. 15.1.2 Evitar el uso de dispositivos que afecten la productividad.	Política de regulación en el uso de dispositivos que puedan distraer y frenar la productividad de las actividades en la empresa.
16. Cumplimiento	**16.1 Cumplimiento de las normativas empresariales y legales.** 16.1.1 Identificar las regulaciones vigentes para la empresa. 16.1.2 Derechos de propiedad intelectual.	Cumplir los lineamientos mediante estrategias establecidas por la empresa y por empresas reguladoras externas.

Nota: Elaboración Propia

Anexo 8 Material Didáctico para la Socialización

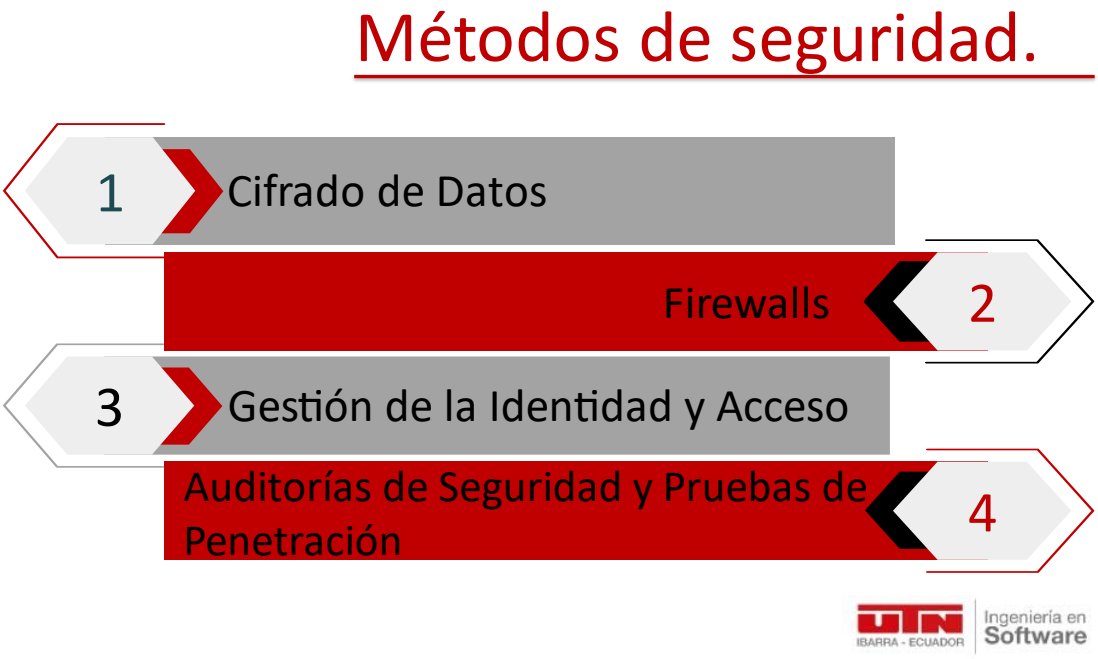
Conceptos de SGSI

2024

Nota: Elaboración Propia.

Nota: Elaboración Propia.

Nota: Elaboración Propia.



Nota: Elaboración Propia.

Anexo 9 Encuesta a los trabajadores de la empresa

Se muestra a continuación la encuesta realizada al personal de la Empresa AIRMAXELECOM SOLUCIONES TECNOLÓGICAS S.A.

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN SOFTWARE

Encuesta sobre el nivel de conocimiento en cuanto a Disponibilidad, Integridad y Confidencialidad

La siguiente encuesta tiene la finalidad de conocer el nivel de importancia y conocimiento en cuanto a Disponibilidad, Integridad y Confidencialidad en la Empresa AIRMAXELECOM SOLUCIONES TECNOLÓGICAS S.A. Se basa en los niveles de criticidad en la escala de Likert

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

Dimensión de Valoración	Preguntas
1. Preguntas acerca de la disponibilidad de la información en la empresa de internet AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.	¿Qué impacto tendría para el departamento de tecnologías de la información que la información de la empresa no estuviera disponible para desarrollar las actividades?

	¿La inaccesibilidad de la información afectaría la actividad normal de la Institución?
2. Preguntas acerca de la integridad de la información en la empresa de internet AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.	¿Qué impacto tendría para el departamento de tecnología de información que la información de la empresa fuera falsa, alterada o estuviera incompleta? ¿Si la información que se maneja por medio del sistema de la empresa es alterada sin autorización en qué grado puede perjudicar la imagen de la identidad? ¿Si la información que se maneja en la empresa es alterada sin autorización puede provocar sanciones de entes de control?
1. Preguntas acerca de la confidencialidad de la información en la empresa de internet AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.	¿Cómo afectaría al departamento de tecnología de información de la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A. que los datos que se obtiene en el sistema fueran conocido por usuarios no autorizados? ¿El acceso no autorizado a la información puede perjudicar la imagen de la organización? ¿La divulgación no autorizada podría revelar datos sensibles de la empresa, para las decisiones críticas, estratégicas y financieras?

Nota: Elaboración Propia.

Anexo 10 Cuestionario para validación con Expertos

Se muestra a continuación la encuesta realizada a los expertos con el Método Delphi en cuanto al Sistema de Gestión de Seguridad de la Información basado en las Normas ISO/IEC 27001 y 27002:2022 para la empresa AIRMAXELECOM SOLUCIONES TECNOLÓGICAS S.A.

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN SOFTWARE

Preguntas para Validación SGSI con Método Delphi con expertos

1: ¿Considera usted que es muy imprescindible el Diseño de un Sistema de Gestión de Seguridad de la Información con la ISO/27001 y 27002:2022 en el departamento de Tecnología de la Información de la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A?

2: ¿Cómo evalúa el Diseño de un Sistema de Gestión de Seguridad de la Información con la ISO/27001 y 27002:2022 para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A., es un informe comprensible?

3: ¿Está de acuerdo con la elección de la Metodología Magerit y la ISO/27001 y 27002:2022 para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.?

4: ¿Considera usted que los procedimientos realizados en el Diseño de un Sistema de Gestión de Seguridad de la Información para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A., fueron los necesarios?

5: ¿A su criterio el informe de Diseño de un Sistema de Gestión de Seguridad de la Información con la ISO/ 27001 y 27002:2022 para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A., Tiene la información necesaria?

6: ¿Considera usted que la herramienta Pilar y la hoja de cálculo de Excel son eficientes para el desarrollo de un Sistema de Gestión de Seguridad de la información para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.?

7: ¿En su opinión las tareas propuestas para el control y mitigación de riesgos en el desarrollo de un Sistema de Gestión de Seguridad de la información para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A., fueron adecuadas?

8: ¿Considera usted que las políticas de seguridad para el Sistema de Gestión de Seguridad de la Información para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A. fueron las más adecuadas?

9: ¿Considera usted que el número de políticas establecidas en el Sistema de Gestión de Seguridad de la Información para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A. son las óptimas para la empresa?

10: ¿Considera usted que las políticas de seguridad descritas para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A., cubren todos los aspectos de seguridad de la información?

11: ¿Considera usted que ha recibido suficiente información para seguir y entender las políticas de seguridad de la información para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.?

Nota: Elaboración Propia.

Anexo 11 Certificado

PLUS

Ibarra, 4 de junio de 2024

AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.
RUC:1091732455001

CERTIFICA

Que el Sr. HEINZ DYLAN DELGADO OJEDA con CI: 1050440732, en referencia al OF-AM-23-07-00130 del 21 de julio de 2023, en el cual se aprobó el desarrollo del trabajo de titulación "***DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LAS NORMAS DE SEGURIDAD ISO/IEC 27001-27002:2022 PARA LA EMPRESA AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS***", me permito informar que los documentos han sido entregados para su aplicación en nuestra empresa, como se detalla a continuación:

- Informe final del SGSI.
- Matriz de riesgos.
- Manual de políticas.
- Políticas de seguridad de la información.

Es todo cuanto puedo certificar, el interesado puede hacer uso del mismo para los trámites que estime conveniente.

Atentamente,

AIRMAX TELECOM
PLUS
RECURSOS HUMANOS
RUC. 1091732455001

Ing. Andrea Paola García T. MSc.
JEFE DE TALENTO HUMANO
AIRMAXTELECOM

Av. Teodoro Gómez de la Torre y Calixto Miranda (Esq.) (06)3 700 910 - 099 198 4757 ventas@iplus.com.ec
www.iplus.com.ec