ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DESARROLLO E IMPLEMENTACIÓN DE CONTROLES PARA EL DOMINIO DE SEGURIDAD FÍSICA Y AMBIENTAL PARA LA EMPRESA FELMOVA S.A USANDO LA NORMA ISO 27002: 2013".

TRABAJO DE TITULACIÓN

Previa a la obtención del Título de

MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por:

ING. YAN AN CORNEJO MONTOYA

GUAYAQUIL - ECUADOR

AÑO: 2017

AGRADECIMIENTO

Doy gracias a Dios por permitirme alcanzar esta meta profesional. A mis padres, mis suegros, mi esposo y mis dos hijas, que con amor y sacrificio me acompañaron en cada paso. A mis profesores Lenín Freire Msig, mi tutor Jorge Olaya PHD , Laura Ureta Msig, y mis compañeros que supieron aconsejarme y guiarme para continuar en este largo camino..

Yan An Cornejo Montoya

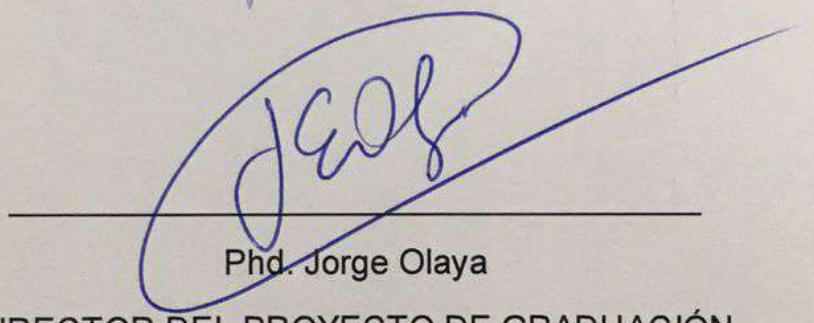
DEDICATORIA

A Dios, a mis padres, a mi esposo, a mis hijas, a mi familia, tutor, maestros, amigos y a todos aquellos que me acompañaron y alentaron a seguir adelante.

TRIBUNAL DE SUSTENTACIÓN

Mgs. Lenín Freire Cobo

DIRECTOR MSIA



Phd. Jorge Olaya

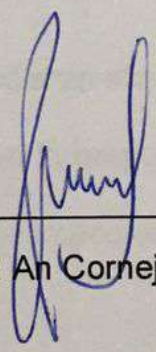
DIRECTOR DEL PROYECTO DE GRADUACIÓN

Msig. Laura Ureta Arreaga

MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

"Declaro de forma expresa que todo el contenido de esta Tesis de Grado es de mi completa autoría y responsabilidad, por lo que doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"



Yan An Cornejo Montoya

RESUMEN

Este trabajo de investigación presenta un análisis de los pasos necesarios para llevar a cabo la implantación de controles de las normas ISO 27002:2013 utilizando la metodología MAGERIT en conjunto con la herramienta PILAR, la misma que permitirá analizar, y evaluar los activos de información de la empresa FELMOVA S.A, así como la identificación de las amenazas y vulnerabilidades a las que puede ser susceptible la empresa.

Se identificaron riesgos que pudieran afectar en forma material, financiera y de imagen a la empresa, así como la propuesta de controles de mitigación para minimizar los posibles efectos e impactos en la organización.

La herramienta PILAR (licencia temporal), permitió el ingreso de valoraciones, en donde se les realizó evaluaciones de los activos, amenazas y salvaguardas, y así obtener niveles de riesgo e impacto mostrados en las gráficas, que dieron la pauta y la dirección para implementar procedimientos y normas, con el propósito de proteger los recursos e información.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La presente tesis está dirigida a la implementación de los controles de seguridad utilizando la norma ISO/IEC 27002:2013, en los activos de la empresa “Felmova S.A”.

Siendo la información el activo más valioso en cualquier organización es importante tomar las medidas necesarias para que se garantice su disponibilidad, integridad y confidencialidad.

En la actualidad debido al mundo vertiginoso de la tecnología, los activos de información están expuestos a amenazas y debilidades que deben ser controladas, ya que no existe un sistema que elimine por completo los riesgos.

Los riesgos pueden afectar o impactar de manera negativa al desenvolvimiento de la empresa inclusive llegando a paralizar sus operaciones por lo que es importante definir controles que, permitan mitigar o minimizar el impacto que una amenaza pueda llegar a tener sobre un determinado activo.

En el primer capítulo se desarrolla sobre los antecedentes, descripción del problema, solución propuesta, objetivo general, objetivos específicos, y

metodología Magerit, que recomendará las medidas apropiadas para conocer, prevenir, impedir y controlar riesgos identificados y poder reducirlos al mínimo.

En el segundo capítulo explica detalladamente sobre las normas ISO IEC 27001: 2013 y la norma ISO /IEC 27002 :2013 , en donde la primera permite obtener la certificación a cualquier organización y la segunda trata sobre las buenas prácticas recomendadas en cualquier empresa, Así mismo se incluye el Anexo A que sirve de apoyo a las normas ISO 27001, las amenazas previstas en la seguridad física, desastres, vulnerabilidades, disturbios, riesgos y peligros.

El tercer capítulo se basa en la explicación de la Metodología de Magerit versión 3.0, la misma que consta de las fases de Análisis y Gestión de riesgos, en donde, la herramienta Pilar servirá como soporte para el inventario y valoración de activos, ponderación y determinación de amenazas de los mismos. Impactos, riesgos, valoración de amenazas, tipos de riesgos, cómo manejar el riesgo. Los controles que se deben tener en cuenta en la seguridad física para obtener resultados del riesgo a niveles aceptables. Finalmente, las salvaguardas y su eficacia al aplicarlas en base a los estudios realizados

En el cuarto capítulo es un estudio sobre los estándares de seguridad física, evaluación de riesgos, determinación de controles, y plan de implementación de los controles sugeridos.

En el quinto capítulo se mencionan los factores físicos que afectan de alguna manera a las organizaciones y pueden repercutir como posibles riesgos.
El factor humano, se lo analiza como proceso de control en las empresas, se analizan las políticas y procedimientos de seguridad, los tipos de instalaciones según el riesgo sea alto, medio o bajo. Y la difusión de políticas mediante un cronograma de trabajo.

En el sexto capítulo se realiza un análisis de resultados de las pruebas realizadas en la empresa, y la entrega de informes con cuadros estadísticos, los cuales mostrarán a la gerencia general los pasos a seguir en cuanto a las guías de las Buenas Prácticas de las normas de seguridad que se recomiendan, según cronograma indicada en esta investigación.

CAPÍTULO 1

GENERALIDADES

1.1. Antecedentes

FELMOVA S.A es una empresa que opera en la ciudad de Guayaquil desde el año 2007 y desarrolla sus actividades en el campo comercial y de servicios. Su misión es ser una empresa líder en suministrar productos de calidad no perecibles al por mayor y menor, cumpliendo con estándares de eficiencia y responsabilidad, generando un entorno de confianza y seguridad a sus clientes y colaboradores, a su vez bridando un excelente servicio y contribuyendo al crecimiento económico del país.

Siendo una época de grandes cambios tecnológicos, el aplicar controles para la protección de los datos, así como la protección en la seguridad física, de una forma adecuada resulta imprescindible analizar los tipos de controles adecuados para cada empresa.

Es por esto que la empresa FELMOVA S.A. deseando mantener su competitividad comercial y buscando garantizar sus procesos de manera efectiva, confiable y organizada, brindar un servicio de mejor calidad, desea ser parte de la propuesta de Controles para El Dominio De Seguridad Física Y Ambiental usando la Norma ISO 27002:2013, la cual consiste en las políticas de seguridad y procedimientos que se sugiere a la organización.

Como parte de este esquema propuesto, se debe realizar una serie de actividades en donde actualmente existen muchas herramientas en el mercado, que de una manera fácil y con poco esfuerzo se tiene acceso de personas no autorizadas a cualquier sitio, esto debido a que no hay controles bien definidos pudiendo causar perjuicios económicos a la empresa. Por ejemplo, en enero del 2015 el malware Cryptolocker, atacó en menos de 5 días a 17 empresas privadas y públicas ubicadas en Guayaquil, Quito y Cuenca, causándoles pérdida de información , lo que en esencia se lo considera el activo más importante de cualquier organización, y estas empresas notificaron dicho daño a GMS[1] una de

las 5 empresas megaplataformas ubicadas en Ecuador, y este potente malware llega a los usuarios a través de correos electrónicos, el cual usó una fachada falsa con el asunto de “facturación electrónica”. (Comercio, 2015)

Siendo FELMOVA una empresa con 9 años de antigüedad, desea laborar bajo una guía de buenas prácticas, que corresponden a los controles de seguridad Física y del Entorno, que le servirán de base para la distribución y venta de productos no perecibles hacia sus clientes, con la implementación de mejores controles, que le permita tener un mejor detalle de productos, proveedores, y así establecerse como una empresa a la vanguardia del mercado ecuatoriano, pudiendo ampliar su catálogo de productos y su cartera de futuros clientes.

1.2. Descripción Del Problema.

Uno de los principales riesgos que puede tener toda empresa son los accesos no autorizados a sus instalaciones, y esto puede suceder por la puerta principal, paredes, puertas alternas y ventanas, por lo que se deben tomar las medidas necesarias como lo son la planificación, análisis, gestión, control, evaluación de riesgos que puedan atentar contra la seguridad de sus instalaciones.

Todo esto debido a la observación directa, que se realizó durante las primeras visitas a la empresa FELMOVA S.A, por lo que se concluye

que puede ocasionar posibles pérdidas económicas a la empresa, y que muchas organizaciones ante situaciones similares actúan posteriores a la ocurrencia de algún incidente, por ejemplo: personal deshonesto, hurtos internos, ya sea por falsear documentos o intrusión de personal no autorizado debido a controles inadecuados.

“La seguridad es un elemento capacitador de las ciudades del futuro” (Ciberseguridad, 2015)

Entre los temas que preocupan a la empresa son:

- El control de ingresos de proveedores a las instalaciones de la empresa,
- La Fuga de Información
- Mal manejo de productos entre colaboradores,
- Posible deterioro de productos almacenados en bodegas,
- Filtraciones por condiciones climáticas
- Daño de tuberías dentro de las bodegas,
- Controles inadecuados de carga y descarga de productos desde la bodega hacia el exterior,
- Demora en la entrega de productos a sus clientes.

Una de las maneras de reducir los riesgos que puedan afectar a los activos de la empresa, es la elaboración de normas internas. Es por esto que se propone en este estudio, las normas de buenas prácticas de

seguridad, para reducir la probabilidad de ocurrencia de un impacto debido a los riesgos a los que pueden estar expuestos sus activos.

En la figura 1 se muestra como están clasificadas las amenazas y a quienes pueden afectar, ya sean por fallas humanas, desastres naturales o ataques deliberados; las fallas humanas pueden ser con intención o sin ella, así mismo pueden ser internas o externas dependiendo si provienen desde dentro de la empresa o fuera de ella.

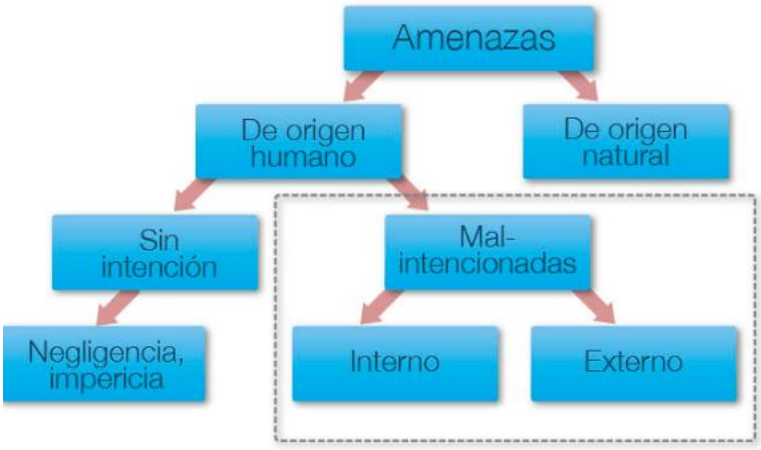


Figura 1. 1 Amenazas [2]

1.3. Solución Propuesta

Una de las maneras de protegerse de los accesos no autorizados a las zonas físicas de la empresa, es mediante una correcta gestión del

riesgo, identificando claramente las debilidades a las que podría estar expuesta la organización, planteando un esquema de seguridad, proponiendo políticas de seguridad actuales, mecanismos de detección de intrusos, concientización de usuarios que se ajuste a las necesidades de la empresa, es así como se intenta proteger los activos de diferentes condiciones físicas como el clima, desastres naturales, amenazas deliberadas o accidentales.

Partiendo de esta premisa el presente proyecto reúne la información necesaria para el DESARROLLO E IMPLEMENTACIÓN DE CONTROLES PARA EL DOMINIO DE SEGURIDAD FÍSICA Y AMBIENTAL PARA LA EMPRESA FELMOVA S.A UTILIZANDO LA NORMA ISO 27002: 2013 y así proponer la mejor protección en cuanto al acceso físico no autorizado hacia la empresa, ya sea por: la puerta principal, vallas, muros y puerta lateral que dispone la empresa, mediante las políticas y procedimientos que se difundirá a todo el personal.

La correcta implementación de las guías de buenas prácticas dentro de la empresa, ayudará a prevenir incidentes de seguridad que puedan generar pérdidas económicas e interrupciones en la continuidad del negocio, mediante la reducción de posibles impactos que los riesgos identificados pudieran ocasionar.

1.4. Objetivo General

Desarrollar e implementar controles para el dominio de seguridad física y ambiental para la empresa **FELMOVA S.A** usando la norma ISO 27002: 2013.

1.5. Objetivos Específicos

- Analizar la situación actual de la empresa **FELMOVA S.A**. en cuanto al manejo de buenas prácticas referentes a la Seguridad Física y Ambiental de la planta principal.
- Identificar los riesgos de las áreas críticas que pueda presentar la empresa, conforme los análisis a realizarse y posteriores evaluaciones, para que se tomen las medidas necesarias para su mejor manejo.
- Determinar las políticas necesarias y documentaciones aprobadas por parte de la Gerencia General, para que pueda ser implementada y difundida bajo el estándar **ISO 27002:2013.**
- Seleccionar el tipo de documentación: Manual de Procedimientos, instrucciones, descripción de procesos y registros que se necesitarán conforme lo designa el estándar **ISO 27002:2013**.
- Implantar y difundir a todo el personal, las políticas de seguridad y procedimientos basados en las buenas prácticas de seguridad,

buscando la reducción del impacto de posibles riesgos a los que pueda estar expuesta la empresa.

1.6. Alcance

El alcance de este proyecto abarca el análisis e implementación de los controles de Seguridad Física y del Entorno de la norma ISO 27002:2013 para la empresa **FELMOVA S.A**, en donde se crearán guías de buenas prácticas que deberán ser tomadas en cuenta para un mejor control de los accesos a las instalaciones de la empresa. Este trabajo cubrirá aspectos de procedimientos, normas y medidas, cuyo fin común es mantener y proteger sus activos, basándose en los pilares de la información que son: integridad, disponibilidad, confidencialidad y vigencia en cuanto a los procesos de ingreso, almacenaje, desembarque y despacho de los productos que allí se comercializan.

1.7. Metodología

Se va a utilizar la Metodología de Evaluación de Riesgos MAGERIT, que recomendará las medidas apropiadas para el control de Activos, identificando riesgos en el entorno de trabajo sean latentes o existentes, sus vulnerabilidades; recomendaciones apropiadas para conocer, prevenir, impedir y controlar riesgos identificados para poder reducirlos al mínimo.

MAGERIT es la metodología de Análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, en su versión 3 actualizada al año 2012.

La metodología MARGERIT contempla dos tipos de valoraciones [3]

- cualitativa
- cuantitativa.

La primera hace referencia al hecho de calcular un valor a través de una escala cualitativa, donde se valora el activo de acuerdo al impacto que puede causar en la empresa su daño o pérdida, en consecuencia, la escala se refleja en:

- Muy Alto (MA)
- Alto (A)
- Medio (M)
- Bajo (b)
- Muy bajo (MB)

La valoración cuantitativa también usa escalas de valores para poder estimar su costo que no solo es el valor que tuvo el activo al inicio sino también variables como: [3]

- valor inicial,

- costo de reposición,
- costo de configuración,
- costo de uso del activo y
- valor de pérdida de oportunidad.

MAGERIT diferencia los activos y los agrupa en varios tipos de acuerdo a la función que ejercen en el tratamiento de la información. Al momento de realizar el análisis de riesgos el primer paso es identificar los activos que existen en la organización y determinar el tipo.

Los resultados de los análisis de riesgos permitirán a la gestión de riesgos que puedan recomendar las medidas apropiadas que se deberán adoptar y conocer para prevenir, impedir, reducir o controlar los riesgos que se identifiquen para que se pueda reducir al mínimo las posibles pérdidas.

Esta metodología es de mucha utilidad para aquellas empresas que inicien con la gestión de la seguridad de la información, pues permite enfocarse en los resultados críticos de las empresas. Y lo mejor es que al estar alineado con los estándares de ISO su implementación se convierte en un apoyo para una posible certificación o mejorar sus sistemas de gestión.[4]

CAPÍTULO 2

MARCO TEÓRICO

2.1. Norma ISO/IEC 27001:2013

ISO/IEC 27001:2013 es una norma internacional que fue emitida por la Organización internacional de Normalización(ISO) y fue aprobado y publicado en el año 2013, que especifica los requisitos necesarios para establecer, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).

La ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información, fue redactada por los mejores especialistas en el tema, cuya metodología sirve para implementar la gestión de la seguridad de la información en cualquier organización,

basado en el ciclo Deming que es la mejora continua o PDCA (por las siglas Plan, Do, Check y Act).

Figura 2. 1 PDCA. Eduard Deming

La seguridad de la información define el logro, gestión y mantenimiento en tres características elementales que son: Confidencialidad, Integridad, y Disponibilidad, algunos opinan que se deben incluir también a: la vigencia y el “no repudio”, es decir que no sea negado, así como a la trazabilidad para saber quién y cuándo realizó alguna transacción.

La información siendo uno de los activos más importantes para cualquier actividad de negocios ya sea ésta operativa, de control o gestión, debido a que la alta gerencia se apoya en esta norma, con la finalidad de realizar una toma de decisiones más efectiva.

Las normas ISO 27001 incluyen normas de gestión de riesgos, métricas, auditoría, directrices, guías de implementación, etc.

Las medidas de seguridad o controles que se vayan a implementar, se presentan bajo la forma de políticas, procedimientos e implementación técnica.

Las normas ISO 27001 no sólo están relacionadas a la seguridad de TI, sino que lo están referente a la gestión de procesos, de recursos humanos, protección jurídica, protección física, etc.

Las normas ISO 27001 están orientadas a controles, más no a necesidades de la organización [5].

Una de las ventajas comerciales que cualquier empresa puede obtener al implementar esta norma es, la de mejorar los procesos de la organización en cuanto a qué deben hacer sus empleados, cuándo y con quién deben hacerlo, lo que les permitirá reducir el tiempo perdido [6]

Las normas de la familia ISO 27.000, fundamentalmente la ISO/IEC 27001 e ISO/IEC 27002, tienen como principales objetivos:

- Establecer un marco metodológico para un SGSI.
- La adopción de controles proporcionales a los riesgos percibidos.

- La documentación de políticas, procedimientos, controles y tratamiento de riegos.
- Identificación y asignación de responsabilidades al nivel adecuado.
- Formalización, seguimiento y revisión de los controles y riesgos, de forma sistemática (periódica) y metodológica.
- Generación y preservación de evidencias.
- Tratamiento de los incidentes de seguridad.
- Revisión y mejora continua del SGSI.
- Gestión de Riesgos - Uso de métricas para evaluar efectividad y eficiencia de los controles y del propio SGSI.

Las empresas de cualquier índole se enfrentan a una variedad de riesgos e inseguridades, por lo que se ha decidido proponer el desarrollo e implementación de Controles de la norma ISO 27002:2013 para el Dominio de la Seguridad Física y Ambiental.

Es la única norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI). La norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales. Ello ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por

procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

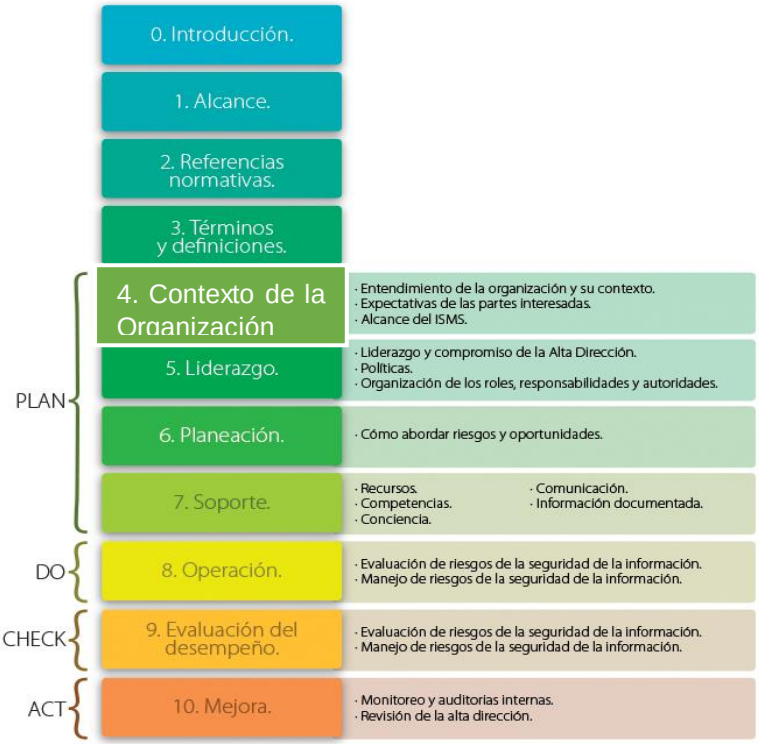


Figura 2. 2 Estructura del estándar ISO/IEC 27001:2013 [7]

2.2. Norma ISO/IEC 27002:2013

Publicado el 1 de julio de 2007. Esta norma no es certificable, y es una guía de buenas prácticas, que detalla los objetivos de control y controles recomendables en los aspectos de seguridad de la información. En cuanto a seguridad de la información la **ISO 27002:2013**, contiene 35 objetivos de control y 114 controles, agrupados en 14 dominios

(cláusulas) de seguridad [8]. Esta norma se encuentra publicada en español a través de la empresa **AENOR** y en Colombia NTC-ISO IEC 27002, así mismo se pueden encontrar en Perú, Chile, entre otros países latinoamericanos. (Distancia, s.f.).

Tabla 1 Dominios – Objetivos de Control y Controles ISO 27002:2013

DOMINIOS (11)	OBJETIVOS DE CONTROL (39)	CONTROLES (114)
1. Políticas de seguridad.	Política de seguridad de la información	2
2. Aspectos organizativos de la seguridad de la información	2.1. Organización interna. 2.2. Dispositivos para movilidad y teletrabajo.	5 2
3. Seguridad ligada a los recursos humanos	3.1. Antes de la contratación. 3.2. Durante la contratación. 3.3. Cese o cambio de puesto de trabajo.	2 3 1
4. Gestión de activos.	4.1. Responsabilidad sobre los activos. 4.2. Clasificación de la información. 4.3. Manejo de los soportes de almacenamiento.	4 3 3
5. Control de acceso.	5.1. Requisitos de negocio para el control de acceso 5.2. Gestión de acceso de usuario. 5.3. Responsabilidad del usuario. 5.4. Control de acceso a sistemas y aplicaciones.	2 6 1 5
6. Cifrado.	6.1. Controles criptográficos.	2
7. La seguridad física y ambiental.	7.1. Áreas seguras 7.2. Seguridad de los equipos.	6 9
8. Seguridad en la operativa.	8.1. Responsabilidades y procedimientos de operación 8.2. Protección contra código malicioso.	4 1

	8.3. Copia de seguridad. 8.4. Registro de actividad y supervisión. 8.5. Control del software en explotación. 8.6. Gestión de vulnerabilidades técnicas. 8.7. Consideraciones de auditorías de los sistemas de información	1 4 1 2 1
9. Seguridad en las telecomunicaciones.	9.1. Gestión de la seguridad en las redes. 9.2. Intercambio de información con partes externas.	3 4
10. Adquisición, desarrollo y mantenimiento de los sistemas de información	10.1. Requisitos de seguridad de los sistemas de información. 10.2. Seguridad de los procesos de desarrollo y soporte. 10.3. Datos de prueba	3 9 1
11. Relaciones con suministradores.	11.1. Seguridad de la información en las relaciones con suministradores. 11.2. Gestión de la prestación de servicios por suministradores.	3 2
12. Gestión de incidentes en la seguridad de la información	12.1. Gestión de incidentes de seguridad de la información y mejoras.	7
13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio	13.1. Continuidad de seguridad de la información. 13.2. Redundancias.	3 1
14. Cumplimiento	14.1. Cumplimiento de los requisitos legales y contractuales. 14.2. Revisiones de la seguridad de la información.	5 3

Estas buenas prácticas se pueden lograr aplicando apropiadas estrategias de control, siendo los estándares ya elaborados una

excelente fuente para el inicio de este proyecto, pero cabe recalcar que cada organización maneja políticas, culturas y recursos humano diferentes.

Dentro de la ISO IEC 27002 se extiende la información de los renovados anexos de ISO 27001, en donde se describen los dominios de control y mecanismos de control, en cuya nueva versión se muestran los controles que buscan mitigar el impacto o posibilidad de ocurrencia de los diferentes riesgos a los cuales pueda estar expuesta una organización. [9]

A continuación, se muestran los capítulos o cláusulas en las normas ISO 27002:2013 con sus objetivos de control.[10]

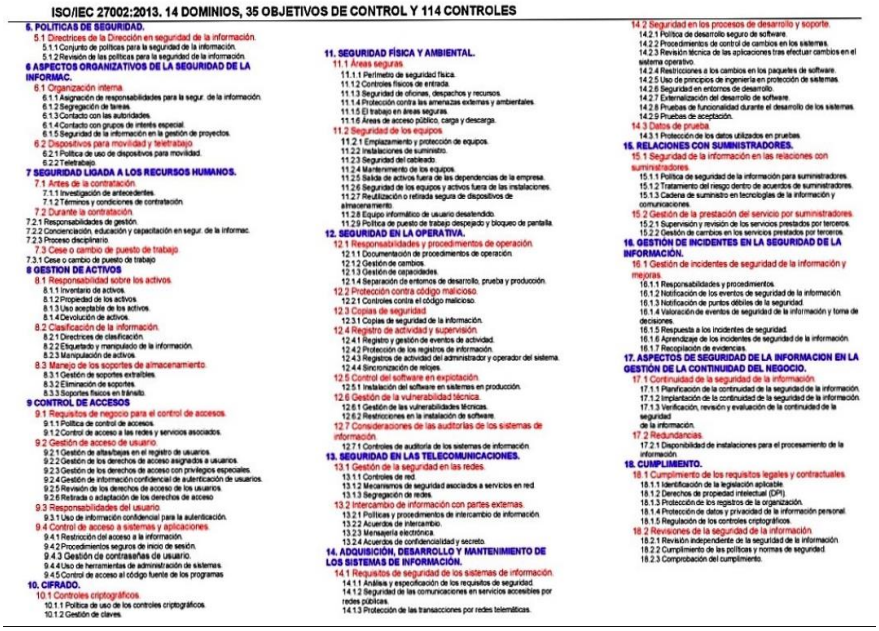
#	Cláusulas	Objetivos de Control
0	Introducción	
1	Alcance	
2	Referencias normativas	
3	Términos y definiciones	
4	Estructura de esta norma	
5	Políticas de Seguridad de la Información	5.1 Dirección de la gestión de la seguridad de la información.
6	Organización de la seguridad de la información	6.1 Organización interna 6.2 Dispositivos móviles y teletrabajo
7	Seguridad de los recursos humanos	7.1 Previo a la contratación 7.2 Durante el empleo 7.3 Terminación y cambio de empleo
8	Gestión de activos	8.1 Responsabilidad por los activos. 8.2 Clasificación de la información. 8.3 Manejos de los medios de almacenamiento
9	Control de acceso	9.1 Requerimientos de negocios del control de accesos. 9.2 Gestión de acceso de los usuarios. 9.3 Responsabilidades de los usuarios. 9.4 Control de acceso de sistemas y aplicaciones.
10	Criptografía	10.1 Controles criptográficos
11	Seguridad física y ambiental	11.1 Áreas seguras 11.2 Seguridad del equipamiento.
12	Seguridad de las operaciones	12.1 Procedimientos y responsabilidades operacionales. 12.2 Protección contra el malware. 12.3 Respaldo. 12.4 Registro y monitoreo 12.5 Control del software operativo. 12.6 Gestión de las vulnerabilidades técnicas. 12.7 Consideraciones de la auditoría de sistemas de información.
13	Seguridad de las comunicaciones	13.1 Gestión de la seguridad de redes. 13.2 Transferencia de información.
14	Adquisición, desarrollo y mantenimiento de sistemas	14.1 Requerimientos de seguridad de los sistemas de información. 14.2 Seguridad en los procesos de desarrollo y soporte. 14.3 Pruebas de datos.
15	Relaciones con proveedores	15.1 Seguridad de la información en las relaciones con proveedores. 15.2 Gestión de entrega de servicios de proveedores.
16	Gestión de incidentes de seguridad de la información	16.1 Gestión de incidentes y mejoras de la seguridad de la información.
17	Aspectos de seguridad de la información en la Gestión de Continuidad de Negocios	17.1 Continuidad de la seguridad de la información. 17.2 Redundancias.
18	Cumplimiento	18.1 Compromiso con los requerimientos legales y contractuales. 18.2 Revisiones de la seguridad de la información.

Figura 2. 3 Objetivos de Control y cláusulas

Además, proporciona directrices para implementar los controles indicados en ISO 27001, ya que está asociada con el Anexo A de la ISO IEC 27001:2013

El Anexo A contiene 14 dominios de seguridad que pueden ser utilizados para disminuir los riesgos de seguridad, y la norma ISO

27002:2013, puede ser muy útil porque, siempre proporciona directrices de cómo implementar esos controles.[8]



ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLITICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.

6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la segur. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.

7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en segur. de la informac.
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.

8 GESTION DE ACTIVOS
8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.
8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.
8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.

9 CONTROL DE ACCESOS
9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso
9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.
9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas

10. CIFRADO.
10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.
12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.
13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.
14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.
14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.
18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento.

Figura 2. 4 Dominios, Objetivos y controles de la norma ISO 27002:2013

Entre las categorías principales de seguridad existen catorce cláusulas:

A.5	Política de seguridad.
A.6	Organización de la seguridad de la información
A.7	Seguridad de los RRHH.
A.8	Gestión de activos.
A.9	Control de accesos.
A.10	Criptografía.
A.11	Seguridad física y ambiental.
A.12	Seguridad en las operaciones.
A.13	Transferencia de información.
A.14	Adquisición de sistemas, desarrollo y mantenimiento.
A.15	Relación con proveedores.
A.16	Gestión de los incidentes de seguridad.
A.17	Continuidad del negocio.
A.18	Cumplimiento con requerimientos legales y contractuales.

Figura 2. 5 Cláusulas o Dominios de la norma ISO 27002:2013

De estas 14 cláusulas , 4 son de carácter técnico, 1 físico y las 9 restantes son de gestión.

2.3. Anexo A.

El Anexo A refleja los controles que están descritos en la norma ISO-IEC 27002:2013, en especial para aquellas empresas que deseen certificarse ya que no están obligados a implementar todos los controles del anexo [8].

Se enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2013, a pesar que no es obligatorio la implementación de todos los controles, la organización deberá argumentar la no aplicabilidad (SOA) (ver Anexo 2) de los controles no implementados.

El Anexo A tiene un carácter normativo – un conjunto de objetivos de control y controles generales, pueden haber controles que apliquen pero que no sean viables ya sea por recursos requeridos técnicos o humanos [7] .

El Anexo A ha reducido controles a 114 y ha incrementado la cantidad de secciones a 14. En la revisión 2013 se eliminaron algunos requerimientos como las medidas preventivas y la necesidad de documentar determinados procedimientos. (Iso27000.es, 2013)

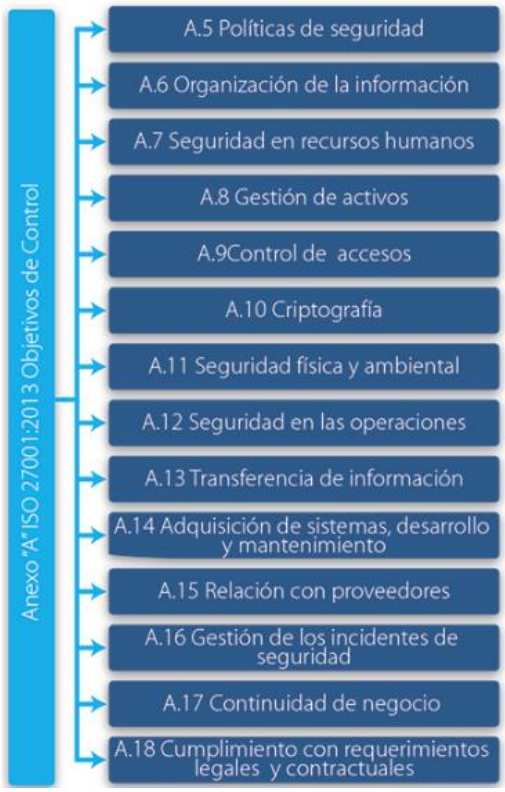


Figura 2. 6 Dominios de Seguridad - Anexo "A" de ISO 27001:2013 [7]

El “Anexo *A* – *Referencia de objetivos y controles”* continúa formando parte de este estándar, pero los anexos “B” y “C” se han eliminado.

2.4. Seguridad Física

Es importante tomar conciencia de que, a pesar de tener las seguridades máximas en la empresa, ya sean del tipo de ataques externos como: hackers, virus, ataques, ingeniería social, gusanos, keyloggers, malware, spyware etc., sino se tienen políticas claras para combatir incendios, desastres naturales, etc., estas medidas servirán, pero en forma limitada.

Es por esto que uno de los aspectos más olvidados al momento de diseñar un sistema de protección es, el hecho de minimizar las oportunidades para el atacante, que intenta ingresar físicamente a las instalaciones de la organización, y tomar algún elemento de suma importancia, sin necesidad de acceder en forma lógica

Aplicando procedimientos de seguridad física se tendrían los siguientes beneficios:

- Disminución de siniestros
- Aligerar carga de trabajo por mejorar sensación de seguridad
- Descartar falsas hipótesis si se presentan incidentes.
- Tener medios para contrarrestar accidentes.

Es así como la seguridad física se refiere a la “aplicación de barreras físicas y procedimientos de control, como medidas de prevención y control ante amenazas a ciertos recursos de información confidencial”. Es decir, son controles y mecanismos de seguridad dentro y alrededor del perímetro de la organización, así como los medios de acceso remoto hacia y desde el sitio.

2.5. Estándares De Seguridad Física.

Las organizaciones necesitan demostrar que realizan una gestión competente y efectiva de la administración de recursos que manejan, demostrando que adoptan medidas adecuadas para detectar e identificar riesgos.

Entre los estándares de seguridad NIST(National Institute for Standars and Technology hace referencia a que los requisitos mínimos de seguridad que cualquier sistema debería tener son los siguientes:[12]

- Identificación y Autenticación
- Roles
- Transacciones
- Limitaciones a los servicios
- Modalidad de acceso
- Ubicación y horario

Entre las medidas que se deben tomar en la seguridad física se tienen:[13] Factores Ambientales: fuego, humedad, Inundaciones, calor, frio, fallos en la energía.

- Interferencias humanas: deliberadas o accidentales

El origen de la seguridad física fue la guerra para proteger bienes o personas, en este sentido el enemigo debía vulnerar los sistemas de protección, control y contención para apoderarse del objetivo.[14]

Es por esto que los expertos de la guerra destacan cuatro categorías de seguridad física:

1. Las obstrucciones físicas: castillos, fuertes, puertas, candados..., que hacen difícil el acceso a los bienes protegidos.

2. Las técnicas de vigilancia: sistemas de alarma, técnicas de vigilancia y 'monitoreos' para alertar de cualquier movimiento sospechoso que se produjera en el perímetro.

3. Los sistemas de inteligencia: herramientas de análisis de información basados en los datos extraídos de la monitorización que simula escenarios para la toma de decisiones ante situaciones no previstas pero probables, que le permita tomar una ventaja operativa y táctica ante amenazas que pudieran afectar a los sistemas protegidos.

4. Los guardias o personal de seguridad: los especialistas en protección física, quienes toman las decisiones ante amenazas o fallos.

Figura 2. 7 Cuatro categorías de la Segurtidad Física [15]

En el ámbito informático, la seguridad física es un aspecto muy olvidado a veces, es por ello que, con la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas, se lo requiere ante posibles amenazas a recursos e información confidencial.

Como tal el Dominio de la Seguridad Física y el Entorno, se divide en los siguientes contenidos:

Áreas seguras

- Perímetro de seguridad física

- Controles físicos de entrada
- Seguridad de oficinas, despachos y recursos
- Protección contra las amenazas externas y ambientales
- El trabajo en áreas seguras
- Áreas de acceso público, carga y descarga

Seguridad de los equipos:

- Emplazamiento y protección de equipos
- Instalaciones de Suministro Eléctrico
- Salida de activos fuera de las dependencias de la empresa.
- Seguridad de los equipos y activos fuera de las instalaciones.
- Reutilización o retirada segura de dispositivos de almacenamiento
- Equipo informático de usuario desatendido
- Política de puesto de trabajo despejado y bloqueo de pantalla

2.6. Amenazas Previstas En La Seguridad Física

Las amenazas se pueden hacer realidad a través de fallas de seguridad, que también se las llama vulnerabilidades y que deben ser controladas al máximo para que el ambiente que se desea proteger esté libre de riesgos ante cualquier incidente de seguridad.

La seguridad física es uno de los aspectos más olvidados del ámbito informático, esto puede ocasionar que un atacante logre su objetivo y

tenga acceso al sitio que desea ingresar más fácilmente de lo que uno se imagina. (Borghello, 2010)

Siendo **MAGERIT** la metodología a utilizarse, se toma de ella la siguiente clasificación de amenazas:

- **Accidentes**: aquellas situaciones no provocadas como: accidentes físicos: inundación, incendio, terremoto, explosión, etc. averías, interrupciones de los servicios esenciales: cortes en la energía eléctrica, telecomunicaciones, etc, y accidentes mecánicos o electromecánicos: choques, caídas, radiación, etc.
- **Errores**: Son aquellas situaciones cometidas en forma involuntaria: errores en el uso de sistemas, errores en el diseño conceptual de aplicaciones, errores en el desarrollo de aplicaciones, errores de aplicación, errores de monitorización, errores de compatibilidad entre aplicaciones o errores inesperados (virus, troyanos, etc.)
- **Amenazas intencionales presenciales**: provocadas por el propio personal de la organización de forma voluntaria las cuales podemos citar: acceso físico no autorizado, acceso lógico no autorizado, interceptar en forma pasiva la información, indisponibilidad de recursos, ya sean humanos (bajas, vacaciones, abandono, enfermedad, etc.) o técnicos (bloqueo de sistema, etc.) y filtración

de datos a terceras organizaciones, ya sean datos personales (LOPD) o técnicos.

- **Amenazas intencionales remotas**: amenazas provocadas por terceras personas, es decir, por personas ajenas a la organización y que consiguen dañarla. Se puede citar a: acceso lógico no autorizado, suplantación del origen, gusanos o denegaciones de servicios.

Figura 2. 8 Amenazas de Seguridad [16]

2.6.1. Desastres

Son aquellas situaciones que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

También se lo define como la Interrupción grave en el funcionamiento de una comunidad, causando pérdidas a nivel

humano, material o ambiental, suficientes para que la comunidad afectada pueda salir adelante por sus propios medios.

Los desastres se clasifican de acuerdo a su origen natural (accidental) o tecnológico, industrial.

Los **desastres naturales** pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

Los **desastres de origen industrial** pueden ocurrir de forma accidental, producidos por actividad humana de tipo industrial y pueden ocurrir de manera accidental o deliberada.

Los **desastres industriales** pueden ser:

- Contaminación
- Fallos eléctricos
- Explosiones
- Derrumbes
- Accidentes de Tráfico
- Sobrecarga /eléctrica

Algunos **desastres naturales** a tener en cuenta:[17]

- Terremotos y vibraciones
- Tormentas eléctricas
- Inundaciones y humedad

- Incendios y humos

Las precauciones que se deben de tomar en cada caso son:

Para el caso de un **sismo**:

- No situar equipos en sitios altos para evitar caídas,
- No colocar elementos móviles sobre los equipos para evitar que caigan sobre ellos,
- Separar los equipos de las ventanas para evitar que caigan por ellas o qué objetos lanzados desde el exterior los dañen,
- Utilizar fijaciones para elementos críticos,
- Colocar los equipos sobre plataformas de goma para que esta absorba las vibraciones

Para el caso de una **tormenta eléctrica**:

- Desconectar los equipos antes de una tormenta (qué por fortuna suelen ser fácilmente predecibles).

Para las **inundaciones** y/o **humedad**:

- Cuando entre en contacto con el agua, el equipo queda automáticamente inutilizado, bien por el propio líquido o bien por los cortocircuitos que genera en los sistemas electrónicos. Contra ellas se puede instalar sistemas de detección que

apaguen los sistemas si se detecta agua y corten la corriente en cuanto estén apagados. Hay que indicar que los equipos deben estar por encima del sistema de detección de agua, sino cuando se intente parar ya estará mojado.

Para el caso de **incendio** y **humo**:

- Se utilizarán sistemas de extinción que, aunque dañen los equipos evitará un mal mayor.

2.6.2. Vulnerabilidad.

Debilidad aprovechada por una amenaza o debilidades de un activo o de sus medidas de protección que facilitan el éxito de una amenaza potencial.[3]

También se refiere al grado de resistencia y/o exposición de un elemento o elementos frente a una situación de peligro, puede ser física, social, cultural, económica, institucional, otros.

Se lo relaciona con ciertas condiciones inherentes a los activos o presentes en su entorno que facilitan que las amenazas se materialicen llevando a esos activos a ser vulnerables. Mediante el uso de las debilidades existentes es que las amenazas logran materializarse, o sea, las amenazas siempre están presentes,

pero si no logra identificar la debilidad no podrá ocurrir ningún impacto. [18]

Vulnerabilidad Física.

Se la relaciona con el material o tipo de material utilizado y el tipo de construcción de las viviendas, establecimientos económicos (comerciales e industriales), de servicios (salud, educación, sedes públicas), e infraestructura económica (hidroeléctricas, carreteras, puentes y canales de riego).

La vulnerabilidad es el grado de debilidad a la que está expuesta un elemento, frente a la ocurrencia de peligro natural. Su probabilidad se expresa en términos de porcentajes de 0 a 100.

La vulnerabilidad es entonces una condición anterior a que ocurra un desastre, es decir cuando no se ha invertido lo suficiente en obras o acciones de prevención y mitigación y su nivel de riesgo es demasiado alto.

Para su análisis, la vulnerabilidad debe fomentar la identificación y caracterización de elementos expuestos en un área geográfica es decir a los efectos adversos de un peligro.

2.6.3. Disturbios / Sabotajes

Se lo considera un desastre ocasionado por el hombre, además de que se lo considera una especie, de vandalismo, que resulta fácil de provocar y los daños son muy costosos.

Un desastre puede ocasionar efectos y ser categorizado en dos escenarios generales:

- Un evento localizado que pueda interrumpir las operaciones de la organización y que sus servicios no estén disponibles para su uso, por lo que requerirá la reubicación total o parcial de las operaciones críticas del negocio a un sitio de Recuperación Alterno.
- La negación de acceso al edificio por un acto terrorista por ej. (Cepeda, 2011)

El sabotaje se lo considera como un riesgo artificial en el sentido de ser dañino y perjudicial para cualquier lugar y que se lo realiza con el objeto de detener de manera parcial o total todas las actividades, ocasionando daños en estructuras de edificios, maquinarias y equipos. [19]

El sabotaje puede ser: interno y externo.

- El sabotaje **interno** se refiere al cometido por empleados de la organización.
- El sabotaje **externo**: errores humanos, mala organización, falta de protección, fallas en las medidas de seguridad.[20]

Figura 2. 9 Evaluación del Riesgo Informático[21]

2.6.4. Fallas Eléctricas, Fallas En Los Equipos

Es considerada un desastre industrial el mal funcionamiento del sistema eléctrico. Puede ser sabotaje o un hecho aislado ajeno a la empresa. El fluido eléctrico puede sufrir perturbaciones o fluctuaciones de tensión, lo cual puede producir cortos circuitos, destrucción parcial o total de equipos de cómputo o alteraciones físicas de los locales.

2.7. Peligro

Es la probabilidad de que ocurra un fenómeno natural o tecnológico que puede ocasionar mucho daño en un período determinado en una localidad. Se logra identificar en algunos casos con apoyo de la ciencia y tecnología.

Peligro es la fuente del riesgo y se refiere a una acción que puede causar daño.

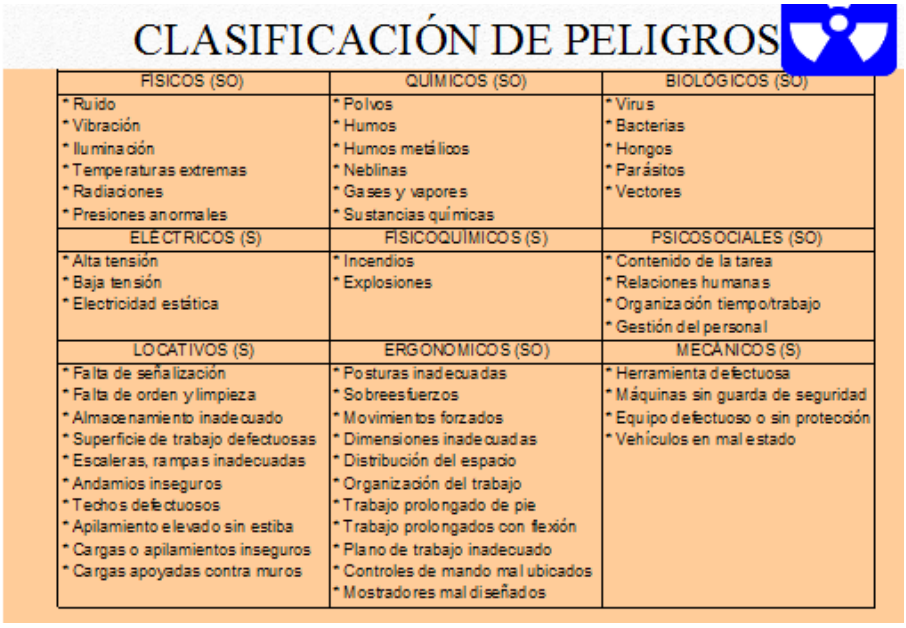


Figura 2. 10 Clasificación de los Peligros

Figura 2. 11 Matriz de Peligro y Vulnerabilidad

La figura 2.11 muestra una matriz que prioriza riesgos en una empresa mediante el análisis de vulnerabilidades específicas por cada amenaza y que puede ser ampliada para obtener un mayor detalle.

2.8. Riesgo.

Probabilidad de que ocurra (materialice) un fenómeno natural o tecnológico muy dañino durante un lapso de tiempo en un sitio o varios lugares.

Es un evento, el cual es incierto y tiene un impacto negativo.

2.9. Mitigar

Se refiere a la reducción de los efectos de un desastre, al tratar de disminuir la vulnerabilidad. Las medidas de prevención que se toman a nivel de ingeniería, normas legales, planificación y otros se los realiza

con el objetivo de proteger la vida humana, de bienes materiales contra cualquier desastre natural, biológico y tecnológico.

2.10. Dimensiones De La Seguridad.

Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza.[23]

Es imposible encontrar un sistema absolutamente seguro, se lo puede catalogar de fiable, y esto sólo sería en el caso de que se garanticen tres aspectos:

- **Confidencialidad** accede a la información mediante autorización controlada. Es una propiedad de difícil recuperación.
- **Integridad** modifica la información sólo con autorización. Su carencia afecta directamente el correcto desempeño de las funciones de la empresa.
- **Disponibilidad** la información del sistema debe permanecer accesible sólo con autorización. Su carencia supone una interrupción del servicio.

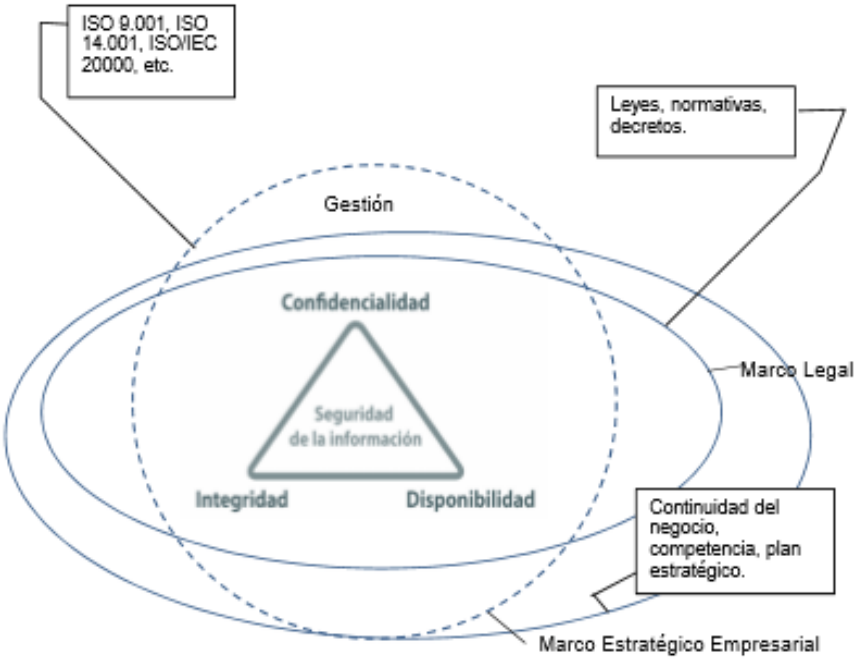


Figura 2. 12 Fuente ISO 27000

La figura 13 muestra los Pilares de la Seguridad De La Información: Confidencialidad, Integridad y Disponibilidad, pertenecientes a la norma ISO/IEC 27001, la cual debe enmarcarse en el contexto del negocio, del marco legal y la estrategia empresarial.

2.11. Controles En La Seguridad Física.

La seguridad física serán aquellas medidas que se tienen en cuenta para prevenir el acceso físico o entrada de personas hacia una instalación o área protegida, con la finalidad de proteger a las personas, activos fijos, infraestructura de agresiones internas y externas

ocasionadas por el hombre o la naturaleza, y así garantizar la continuidad del negocio.

Los controles son los medios para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, de gestión o de tipo legal.

Se recomienda tomar medidas o controles como :[24]

1. Medidas activas: Las realiza el hombre.

- ✓ Vigilancia, Observación e Inspecciones.
- ✓ Identificación, registro y control de personas, paquetes y vehículos para el control de acceso.
- ✓ Labores de patrullaje.
- ✓ Evaluaciones de Riesgo.
- ✓ Sistemas Biométricos.

2. Medidas pasivas:

- ✓ Barreras (Cerca perimétrica).
- ✓ Alumbrado protector.

- ✓ Dispositivo de detección (alarmas) para detectar intrusos o incendios.
- ✓ Mecanismos de cierre (cerraduras) de llave, combinación o electrónicas.

2.12. Controles En La Seguridad De Los Equipos.

Según Juan Pablo Nieto Muñoz, TFM-Mistic, propone una serie de controles como se muestra a continuación en la Figura 14: [25]

Objeto de control	Control	Aplica
Seguridad de los equipos	**Objetivo: Evitar pérdidas, daños, robos o circunstancias que pongan en peligro los activos, o que puedan provocar la interrupción de las actividades de la organización.**	
Emplazamiento y protección de equipos	Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos derivados de las amenazas y peligros de origen ambiental así como las ocasiones de que se produzcan accesos no autorizados.	SI
Instalaciones de suministro	Los equipos deben estar protegidos contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro.	SI
Seguridad del cableado	El cableado eléctrico y de telecomunicaciones que transmite datos o que da soporte a los servicios de información debe estar protegido frente a interceptaciones o daños.	SI
Mantenimiento de los equipos	Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad.	SI
Seguridad de los equipos fuera de las instalaciones	Teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de las instalaciones de la organización, deben aplicarse medidas de seguridad a los equipos situados fuera dichas instalaciones.	SI
Reutilización o retirada segura de equipos	Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y todas las licencias de software se han eliminado o bien se han borrado o sobreescrito de manera segura, antes de su retirada.	SI
Retirada de materiales propiedad de la empresa	Los equipos, la información o el software no deben sacarse de las instalaciones, sin una autorización previa.	SI

Figura 2. 13 Tabla de controles de la ISO 27001:2013

Estos controles se los aplica con el objetivo de realizar un análisis del estado de la seguridad, es decir medir la efectividad de dichos controles, y así poder contrastarlos, para que se realicen los correctivos necesarios en caso de ser posible detectar los incidentes de seguridad con anticipación.

Es por ello que se agrega en los anexos la documentación necesaria como son las Políticas de Seguridad.

2.13. Metodología De Análisis Y Gestión De Riesgo

Es el proceso cuantitativo o cualitativo que permite evaluar los riesgos.

Existen tres tipologías de métodos utilizados para determinar el nivel de riesgos de la organización. Los métodos pueden ser: Métodos Cualitativos – Métodos Cuantitativos – Métodos Semicuantitativos.

El primer paso de la fase de Análisis es identificar los activos a proteger o evaluar. La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo ya establecidos con anterioridad.

La función de la evaluación consiste en ayudar a alcanzar un nivel razonable de consenso en torno a los objetivos en cuestión, y asegurar un nivel mínimo que permita desarrollar indicadores operacionales a partir de los cuales medir y evaluar.

Los resultados obtenidos del análisis, van a permitir aplicar alguno de los métodos para el tratamiento de los riesgos, que involucra identificar el conjunto de opciones que existen para tratar los riesgos, evaluarlas, preparar planes para este tratamiento y ejecutarlos.

Listado de metodologías para el análisis de riesgos en seguridad de la información:

- Metodología MAGERIT
- Metodología CORAS
- Metodología NIST SP 800-30.
- Metodología OCTAVE.
- Metodología CRAMM
- Metodología MEHARI

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que considera que la gestión de riesgos es una piedra angular en las guías de buen gobierno.[22]

MAGERIT es una metodología que se esfuerza por enfatizarse en dividir los activos de la organización en variados grupos, para identificar más riesgos y poder tomar contramedidas para evitar así cualquier inconveniente.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para la organización; pero también pueden suceder ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

La metodología MAGERIT es una de las más utilizadas ya que se encuentra en inglés y en español.

En MAGERIT el método de Análisis de Riesgos consta de las siguientes fases:

MAR.1 – Caracterización de los activos

MAR.11 – Identificación de los activos

MAR.12 – Dependencias entre activos

MAR.13 – Valoración de los activos

MAR.2 – Caracterización de las amenazas

MAR.21 – Identificación de las amenazas

MAR.22 – Valoración de las amenazas

MAR.3 – Caracterización de las salvaguardas

MAR.31 – Identificación de las salvaguardas pertinentes

MAR.32 – Valoración de las salvaguardas

MAR.4 – Estimación del estado de riesgo

MAR.41 – Estimación del impacto

MAR.42 – Estimación del riesgo

CAPÍTULO 3

LEVANTAMIENTO DE INFORMACIÓN

3.1. Magerit

MAGERIT en la actualidad se encuentra en la versión 3.0 y es el acrónimo de "Metodología de Análisis y Gestión de Riesgos de los sistemas de Información". Es una metodología desarrollada en España como resultado del avance vertiginoso de las tecnologías de información y para hacerle frente a diversos riesgos relacionados con la seguridad informática.

MAGERIT es un método formal que sirve para investigar riesgos de un sistema de información y de su entorno previo un análisis que evalúa el impacto de una posible violación de seguridad de la organización y nace para minimizar los riesgos asociados al uso de Sist

emas Informáticos y Telemáticos, garantizando la autenticación, confidencialidad, integridad y disponibili dad de dichos sistemas y generando así, confianza en cualquier empresa.

MAGERIT se basa fundamentalmente en analizar el impacto que puede tener para las Instituciones las violaciones de seguridad, con la finalidad de identificar amenazas que afecten a la vulnerabilidad de la información. Esta metodología presenta una guía de cómo se lleva el análisis de riesgos paso a paso.

Además, que se le considera una aproximación metódica para que se pueda determinar el riesgo, por lo que se deben considerar los siguientes pasos:

1. Determinar los **activos** relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (costo) supondría su degradación.

2. Determinar a qué **amenazas** están expuestos aquellos activos

3. Estimar el **impacto**, definido como el daño sobre el activo derivado de la materialización de la amenaza.

4. Estimar el **riesgo**, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

La siguiente figura muestra como es el proceso del análisis de riesgos [3]:

Figura 3. 1 Elementos de Análisis de Riesgos

Los resultados obtenidos del análisis, utilizando la herramienta PILAR bajo los parámetros de MAGERIT para el tratamiento de los riesgos, involucra identificar el conjunto de opciones que existen para tratar los riesgos, evaluarlas, preparar planes para este tratamiento y ejecutarlos.[26]

La CSAE (Consejo Superior de Administración Electrónica) recomienda la utilización de esta metodología como respuesta a la gran demanda de las empresas para lograr sus objetivos de servicio.

3.1.1. Descripción De La Metodología

En cinco pasos se detallarán los pasos a seguir:

Paso 1: Definir Activos

Se deberá llevar a cabo un inventario de equipo de cómputo, software y mobiliario, para determinar cuál es la información crítica que se tiene que proteger, así como los activos que contiene la organización, etc., que son requeridos para que los usuarios estén en posibilidad de llevar a cabo sus actividades normales.

Paso 2: Determinar Amenazas

Al determinar las amenazas que perjudican a un activo, habrá que valorar su influencia en el valor del activo, en dos aspectos: Degradación, es decir conocer cuán perjudicado resultaría el activo y por la Probabilidad, es decir cuán probable o improbable es que se materialice la amenaza. La probabilidad de ocurrencia se modela de forma cualitativa y cuantitativa. Ver tabla 2

Tabla 2 Probabilidad de Ocurrencia

	Cualitativamente			Cuantitativamente		
MA	Muy alta	Casi seguro	Fácil	100	Muy frecuente	A diario
A	Alta	Muy alto	Medio	10	Frecuente	Mensualmente
M	Media	Posible	Difícil	1	Normal	Una vez al año
B	Baja	Poco probable	Muy difícil	1/10	Poco frecuente	Cada varios años
MB	Muy baja	Muy raro	Extremadamente difícil	1/100	Muy poco frecuente	siglos

Paso 3. Determinar Salvaguardas-Controles.

Son los procedimientos o mecanismos tecnológicos que reducen el riesgo. Al revisar la seguridad, controles físicos y ambientales existentes, evaluando si son los adecuados respecto a las posibles amenazas. Se debe estar preparado para cualquier imprevisto, y verificar que dentro de la organización se cuente con los elementos necesarios para salvaguardar los activos.

Existen diversos tipos de protección prestados por las salvaguardas:

- Prevención.- Cuando reduce oportunidades que ocurra un incidente

- Disuasión.- Aquellas salvaguardas que actúan antes del incidente y los atacantes no se atreven a atacar.

- Eliminación.- Cuando es eliminado un incidente y no ocurre.

- Minimización del impacto.- Cuando el impacto es limitado y se acotan las consecuencias de un incidente.

- Corrección.- Tras producirse el daño, la salvaguarda lo repara.

- Recuperación.- La salvaguarda permite volver al estado anterior luego de ocurrido el incidente.

- Monitorización.- Salvaguardas que realizan seguimiento de lo que ocurre.

- Detección.- Detecta un ataque cuando se informa de que el ataque está ocurriendo.

- Concienciación.-Actividades de formación de las personas anexas al sistema que pueden tener una influencia sobre él.

- Administración.- Relacionadas con los componentes de seguridad del sistema.

Para medir los aspectos organizativos, se puede emplear una escala de madurez de eficacia. Ver tabla 3.

Tabla 3 Eficacia y Madurez de Salvaguardas

FACTOR	NIVEL	SIGNIFICADO
0%	L0	Inexistente
	L1	Inicial / ad hoc
	L2	Reproducible, pero intuitivo
	L3	Proceso definido
	L4	Gestionado y medible
100%	L5	Optimizado

Paso 4: Impacto Residual

El sistema queda en una situación de posible impacto cuando en su proceso de gestión existe un conjunto de salvaguardas desplegadas y una medida de madurez.

Paso 5. Riesgo Residual

El sistema queda en una situación de posible riesgo cuando en su proceso de gestión existe un conjunto de salvaguardas desplegadas y una medida de madurez.

3.2. Herramienta Pilar

PILAR es el acrónimo de procedimiento informático lógico para el análisis y gestión de riesgos, Las siglas de PILAR provienen de “Procedimiento Informático Lógico para el Análisis de Riesgos”.

Es una herramienta desarrollada por el Centro Nacional De Inteligencia para soportar el análisis de riesgos de sistemas de información basado en la metodología MAGERIT.

PILAR dispone de una biblioteca estándar de propósito general, y es capaz de realizar calificaciones de seguridad respecto de normas ampliamente conocidas como son:

- ISO/IEC 27002:2013 - Código de buenas prácticas para la Gestión de la Seguridad de la Información.

Esta herramienta [PILAR] permite realizar todas las actividades como lo son las fases de análisis de riesgos y la gestión de riesgos.

- Determinación de Activos e identificación, dependencia y valoración
- Determinación de Amenazas
- Estimación de Impactos
- Determinación de los Criterios de aceptación del riesgo
- Determinación de las Medidas de seguridad necesarias o Salvaguardas

Esta aplicación permitirá hacer un análisis de riesgos sobre aspectos de la valoración de: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Además de que se pueda realizar cálculos de impacto y riesgo acumulado así como el impacto y riesgo repercutido.

PILAR permitirá hacer análisis cuantitativo y cualitativo, en este estudio se realizará sólo el análisis cualitativo.

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

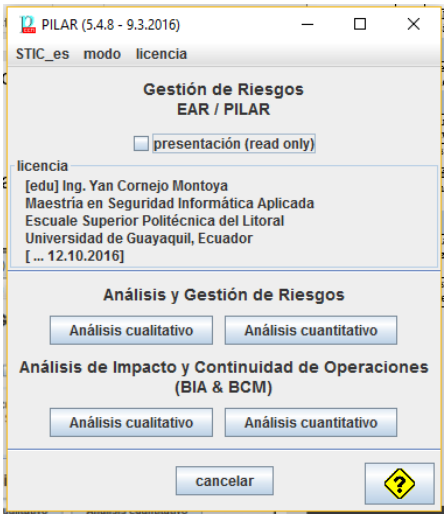


Figura 3. 2 Aplicativo PILAR

3.2.1. Descripción Y Resultados

- La falta de definición de políticas claras de seguridad de información entre el personal de la organización, hace el lugar propicio para que las vulnerabilidades existentes, puedan materializar las amenazas y provocar ataques.
- Fortalecer y crear una cultura de seguridad en la información, que pueda crear conciencia y responsabilidad.
- A nivel general el porcentaje de conformidad que dio como resultado el check list, sobrepasa el 50%, lo que permite concluir que el nivel de seguridad física dentro de las instalaciones está en un nivel aceptable porque el gerente general es quién aplica controles entre su personal a cargo, pero que se puede mejorar aplicando otros criterios que se recomiendan en este proyecto con la finalidad de que mejore la seguridad en la organización, como son las Guías de Buenas Prácticas de las Normas ISO/IEC 27002:2013.
- Realizar un plan de capacitación anual al interior de la organización para preparar a los empleados informando sobre disposiciones y reglamentos que deben cumplir con la finalidad de que se puedan evitar posibles riesgos.
-

3.3. Análisis De Riesgos

Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

Permite determinar cómo es, cuanto vale y que tan protegido se encuentra el sistema.

El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las actividades con fundamento.

Es el proceso que realiza una predicción de lo que pasará a futuro basados en hechos históricos para que se pueda determinar el impacto y tomar alternativas de solución.

El análisis de riesgos permite tomar decisiones de gestión y asignar recursos con perspectiva, sean tecnológicos, humanos o financieros

El análisis de los riesgos se realiza a través de tareas según la metodología MAGERIT.:[18]

Tareas del Método de Análisis de Riesgos

– Caracterización de los activos

- 1.1– Identificación de los activos

- 1.2 – Dependencias entre activos
- 1.3 – Valoración de los activos

– Caracterización de las amenazas

- 2.1 – Identificación de las amenazas
- 2.2 – Valoración de las amenazas

– Caracterización de las salvaguardas

- 3.1 – Identificación de las salvaguardas pertinentes
- 3.2 – Valoración de las salvaguardas

– Estimación del estado del riesgo

- 4.1 – Estimación del impacto
- 4.2 – Estimación del riesgo

Tarea 1:

Caracterización de los Activos

Esta actividad busca identificar los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia. Se compone de 3 sub-tareas:

- **Identificación de los Activos**

Esta actividad se basa en recolectar la información necesaria para identificar los activos, mediante entrevistas al personal, solicitando diagramas de proceso y de flujos de datos. De esta manera, se puede medir el alcance del proyecto y obtener las relaciones entre los activos.

- **Dependencias entre Activos**

El objetivo de esta tarea es identificar y valorar las dependencias entre activos, es decir, conocer la medida en que un activo de orden superior se puede ver perjudicado por una amenaza sobre un activo de orden inferior; resultando diagramas de dependencia.

- **Valoración de los Activos**

El objetivo es identificar en qué dimensión es valioso el activo, para lo cual a la organización significara una pérdida en caso de que fuese afectado. El resultado de esta actividad es el informe denominado “modelo de valor”.

Tarea 2:

Caracterización de las Amenazas

Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia o probabilidad y daño causado o degradación. Se compone de 2 sub-tareas:

- **Identificación de las amenazas**

  Se debe identificar las amenazas más relevantes sobre cada activo, se lo consigue analizando los informes y registros de incidentes y vulnerabilidades. Además, realizando árboles de ataque, los cuales permiten estudiar y analizar cómo se puede atacar un objetivo permitiendo identificar qué salvaguardas se necesitan desplegar para impedirlo.

- **Valoración de las amenazas**

  El objetivo es estimar la frecuencia de ocurrencia de cada amenaza sobre cada activo, estimando la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse. El resultado de esta actividad es el informe denominado “mapa de riesgos”.

Tarea 3:

Caracterización de las Salvaguardas

Esta actividad busca identificar las salvaguardas desplegadas en el sistema a analizar, calificándolas por su eficacia frente a las amenazas que pretenden mitigar. Se compone de 2 sub-tareas:

- **Identificación de las salvaguardas pertinentes**

  Esto se logra analizando los informes de productos y servicios, indicadores de impacto y riesgo residual y los modelos de activos y amenazas del sistema.

- **Valoración de las salvaguardas**

  Luego de tener el listado de salvaguardas, conviene determinar la eficacia sobre los activos considerando:

  - La idoneidad de la salvaguarda para el fin perseguido
  - Calidad de implantación
  - Formación de los responsables de su configuración y operación
  - Existencia de controles de medida de su efectividad.

  El resultado de esta actividad se concreta en varios informes: declaración de aplicabilidad, evaluación de salvaguardas, y de insuficiencias o vulnerabilidades del sistema de protección.

Tarea 4:

- **Estimación del Estado del Riesgo**

Esta actividad procesa todos los datos recopilados en las actividades anteriores para:

- Realizar un informe del estado de riesgo: estimación de impacto y riesgo.

- Realizar un informe de insuficiencias: deficiencias o debilidades en el sistema de salvaguardas. Esta actividad consta de dos tareas:

- **Estimación del Impacto**

En esta tarea se estima el impacto al que están expuestos los activos del sistema:

- Impacto potencial.- Al que se encuentra expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas - controles, actualmente desplegadas.

- Impacto residual.- Al que se encuentra expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas.

- **Estimación del Riesgo**

  En esta tarea se estima el riesgo al que están sometidos los activos del sistema:[27]

  - Riesgo Potencial.- Al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, pero no las salvaguardas-controles, actualmente desplegadas.

  - Riesgo Residual.- Al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas-controles, actualmente desplegadas.

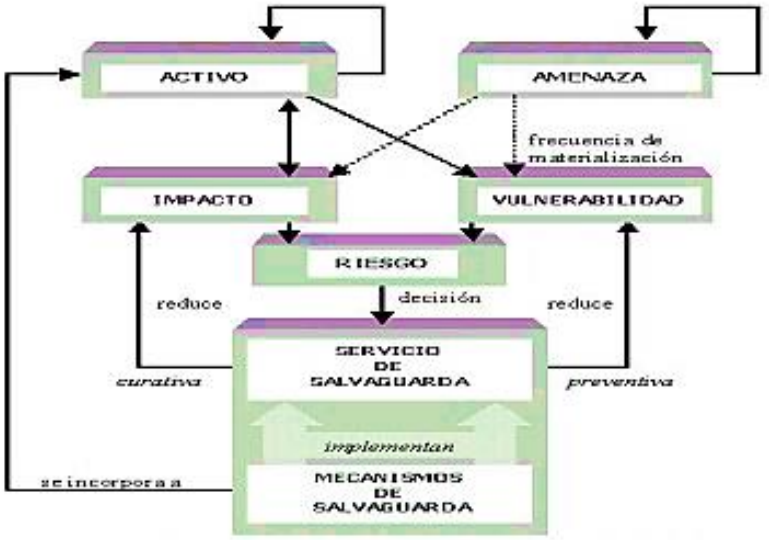


Figura 3. 3 Descripción del proceso de Análisis y Gestión de Riesgos

La figura 3.3 muestra los pasos que se deberían seguir para tratar con cautela las valoraciones de activos, verificar existencia de amenazas, riesgos y aplicar correctamente las salvaguardas-controles necesarios si fuera el caso.

En resumen, que un análisis de riesgos no es una tarea que hay que tomar a la ligera. Es una tarea de suma importancia, que requiere esfuerzo y coordinación. Por lo tanto, debe ser planificada y justificada.

3.3.1. Inventario y Valoración De Activos

Los activos son todos los elementos que una organización posee para el manejo de su información (**hardware, software, recurso humano, etc.).** MAGERIT diferencia los activos agrupándolos en varios tipos de acuerdo a la función que ejercen en el tratamiento de la información.

Tipos De Activos A Determinar:

La información es el activo esencial en toda empresa. Y mediante PILAR se identifica activos como:

[D] Datos / Información Los datos son el corazón que permite a una organización prestar sus servicios. Son en cierto sentido un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado en forma de bases de

datos) o será transferido de un lugar a otro por los medios de transmisión de datos.

[SW] Aplicaciones (Software) Se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos, permitiendo la explotación de la información para la prestación de los servicios.

[HW] Equipos informáticos (Hardware) Bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

[SI] Soportes de información Se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

[AUX] Equipamiento auxiliar Se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

[L] Instalaciones. Acogen equipos informáticos y de comunicaciones.

[P] Personas que explotan u operan todos los elementos anteriores citados

[IS]Servicios. Auxiliares que sirven para organizar el sistema

Valoración de Activos

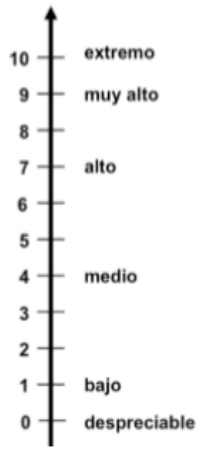
MAGERIT considera dos tipos de valoraciones: cualitativa y cuantitativa.

En este caso, solo se considerará el estudio sobre valoraciones cualitativas, cuyos rangos de valores son:

- Muy Alto (**MA**)
- Alto (**A**)
- Medio (M)
- Bajo (b)
- Muy bajo (MB)

La siguiente gráfica corresponde a una escala de valoración logarítmica, cuyo objetivo es realizar una valoración cualitativa,

que responden a valoraciones de la opinión personal del personal de la organización.



valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Figura 3. 4 Valoración de Activos utilizada en las dimensiones

En la figura 18 se muestran dos escalas: una detallada y otra resumida, en donde la tabla resumida se la usa en análisis de riesgos con poco detalle.

La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión.

DIMENSIONES DE VALORACION:

Son los atributos que hacen valioso a un activo. Una dimensión se refiere a la faceta de un activo que no depende de otras.

Las dimensiones sirven para valorar las consecuencias de la materialización de una amenaza.

DIMENSIONES:

- [**D**] Disponibilidad
- [**I**] Integridad de los datos
- [**C**] Confidencialidad de los datos
- [**A**] Autenticidad de los usuarios y de la información
- [**T**] Trazabilidad del servicio y de los datos

- **Disponibilidad**

  La disposición de los servicios a ser usados cuando sea necesario. Su carencia supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

- **Integridad.**

  Mantenimiento de las características de completitud y corrección de datos. Sin ella la información puede ser manipulada, corrupta o incompleta, su carencia afecta directamente al correcto desempeño de las funciones de una organización.

- **Confidencialidad.**

  La información solo debe llegar a las personas autorizadas, su carencia puede ocasionar fugas, filtraciones de información, así

como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, lo que conlleva a incumplimiento de leyes y compromisos con respecto a la custodia de datos.

- **Autenticidad**

  Caracteristica que garantiza la fuente de donde proceden los datos.Su carencia puede ocasionar suplantación de identidad.

- **Trazabiilidad**

  Asegura quién hizo una actividad y en qué momento. Esencial para analizar **incidentes, perseguir atacantes.**

3.3.2. Determinación de Activos

Un activo es algo que representa un valor o una utilidad para cualquier organización. Los activos precisan protección para asegurar las operaciones del negocio y la continuidad de la empresa.[28]

Siguiendo la Metodología MAGERIT para consultar el catálogo de activos figura 3.5

Tipos de activos	Descripción
Datos	Bases de datos, documentación (manuales de usuario, contratos, normativas, etc.)
Aplicaciones Informáticas (SW)	Sistemas de información, herramientas de desarrollo, aplicativos desarrollados y en desarrollo, sistemas operativos, aplicaciones de servidores etc.
Equipos Informáticos(Hw)	Equipos de oficina (PC, portátiles, servidores, dispositivos móviles, etc.)
Redes	Dispositivos de conectividad de redes (router, swicth, concentradores, etc.)
Equipamiento auxiliar	UPS,
Instalación	Cableado estructurado, instalaciones eléctricas.
Servicios	Conectividad a internet, servicios de mantenimiento, etc.
Personal	Personal informático (administradores, webmaster, desarrolladores, etc.), usuarios finales y personal técnico.

Figura 3. 5 Relación de Activos de seguridad de información

Detalle De Activos

En la actualidad resulta imprescindible incorporar a las organizaciones las tecnologías de información y comunicaciones (TIC's), pero esto los expone a muchos riesgos como: la divulgación, modificación, pérdida o interrupción de la información (López & Gutierrez, 2013).

Es así como la información es uno de los activos más importantes y que representa un activo muy valioso por lo que se debe brindar las medidas de protección para proteger dicha información.

Como activos de información se encuentran: bases de datos, software del sistema, equipos informáticos y de comunicaciones, es decir todo lo relacionado al almacenamiento y envío de información.

En reunión con el gerente general de la empresa FELMOVA S.A., al realizarse la encuesta se determinaron los siguientes activos de información, ver tabla 4.

Tabla 4 Tabla De Activos

ACTIVOS
DATOS
Bases de datos
Contraseñas
Datos clasificados
Datos públicos
SERVICIOS
Correo electrónico
Despacho de Mercadería
SOFTWARE- APLICACIONES
Antivirus
Sistema Operativo
Sistema de Respaldo- Backup
Desarrollo a medida(subcontratado)

Sistema de Cobranzas
Caja
Sistema de Facturación
HARDWARE- EQUIPO INFORMÁTICO
Modem
Pc's
Laptop
Servidor dedicado
Impresoras
Sistema de circuito cerrado
SOPORTE DE INFORMACION
Información financiera del cliente
Políticas de operación financiera
Manejo de cartera de clientes
Información general de la empresa
Medios de Respaldo

3.3.3. Ponderación De Dimensiones De Los Activos.

Considera el análisis de cada uno de sus elementos. Es lo que hace valioso a un activo. Esta ponderación servirá para valorar las consecuencias de la materialización de una amenaza, ver tabla 5.

- [D] Disponibilidad
- [I] Integridad De Los Datos
- [C] Confidencialidad de Los Datos
- [A] Autenticidad de Los Usuarios y de la Información
- [T] Trazabilidad del Servicio y de los Datos.

Tabla 5 Activos Valorados

	DIMENSIONES				
Activos	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
DATOS					
Bases de datos	6	6	6		
Contraseñas	6	6	6		
Datos clasificados	6	6	6	6	6
Datos públicos	6	6	7	6	6
SERVICIOS					
Correo electrónico	5	5	6	7	7
Despacho de Mercadería	7	7	7	6	6
SOFTWARE- APLICACIONES					
Antivirus	7	7	7		
Sistema Operativo	7	6	6		
Sistema de Respaldo- Backup	5	6	6		
Desarrollo a medida(subcontratado)	8	8	8		
Sistema de Cobranzas	9	8	8	8	8
Caja	9	8	8	8	8
Sistema de Facturación	8	8	8	8	8
HARDWARE – EQUIPO INFORMATICO					
Modem	5	5			
Pc	5	7	9	7	7
Laptop	5	8	6		
Servidor dedicado	8	7	7		
Impresoras	5				
Circuito cerrado	6	5			
SOPORTE DE INFORMACION					
Información financiera del cliente	5	5	5		
Políticas de operación financiera	6	6	6		
Manejo de cartera de clientes	6	6	6		
Información general de la empresa	5	5	5		
Medios de Respaldo	6	6	6		

3.3.4. Determinación De Las Amenazas

Una amenaza es un perjuicio potencial provocado por un incidente deseado o no, hacia los activos de una organización empresarial. Si se llegara a concretar la amenaza puede estar en peligro la integridad, confidencialidad, autenticidad y disponibilidad de un activo.

Las amenazas pueden centrarse en un activo específico y reaccionar en cadena a través de todas las dependencias de los activos allí presentes.

Identificación De Las Amenazas

La identificación de las amenazas y de la probabilidad de ocurrencia deben ser obtenidos de los propietarios o usuarios del activo, personal de recursos humanos, gestión de instalaciones, especialistas en la seguridad de la información, expertos en seguridad física, departamento legal, autoridades meteorológicas, compañías de seguros y autoridades de gobierno nacional.

También se debe considerar los aspectos de ambiente y cultura.

Las Amenazas pueden ser:

- **De origen natural**

Hay accidentes naturales (terremotos, inundaciones, ...). Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.

- **Del entorno (de origen industrial)**

Hay desastres industriales (contaminación, fallos eléctricos, ...) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.

- **Defectos de las aplicaciones**

Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, vulnerabilidades.

- **Causadas por las personas de forma accidental**

Las personas con acceso al sistema de información pueden ocasionar problemas no intencionados, típicamente por error o por omisión.

- **Causadas por las personas de forma deliberada**

Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien

con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

No todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir.

Valoración De Las Amenazas

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.

Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos:

Degradación: cuán perjudicado resultaría el -valor del- activo

Probabilidad: cuán probable o improbable es que se materialice la amenaza

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera**.**

Tabla 6 Degradación del valor

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Tabla 7 Probabilidad de Ocurrencia

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

Los tipos de amenazas van relacionadas con las dimensiones de los activos como lo demuestra la siguiente tabla: [29]

Tabla 8 Relación de amenazas con las dimensiones de los activos

[D]	*[I]*	*[C]*	*[A_*]*	*[T_*]*
E.1 E.2 E.4 E.24	E.1 E.2 E.4 E.9 E.10	E.2 E.4 E.9	E.2 E.4 E.9	E.2 E.3 E.4 E.9
A.4 A.7 A.24	A.4 A.5 A.6 A.9 A.10 A.11	A.4 A.5 A.6 A.9 A.11	A.4 A.5 A.9 A.11	A.4 A.9 A.13

Cuya nomenclatura de Amenazas es la siguiente:

Tabla 9 Nomenclatura de Amenazas

I5	Avería de origen físico o lógico
E1	Errores de los usuarios
E2	Errores del administrador
E3	Errores de monitorización-log
E4	Errores de configuración
E9	Errores de encaminamiento
E10	Errores de Secuencia
E24	Caída del sistema por agotamiento de recursos
A4	Manipulación de la configuración
A5	Suplantación de identidad del usuario
A6	Abuso de privilegios de acceso
A7	Uso no previsto
A9	Re-encaminamiento de mensajes
A10	Alteración de secuencia
A11	Acceso no autorizado
A13	Repudio
A24	Denegación de servicio

La tabla 9 muestra las amenazas más comunes a las que se expone cualquier organización.

Se agrupó a los activos y se muestran las amenazas, degradación y probabilidad de ocurrencia conforme a la encuesta realizada al gerente general de la empresa FELMOVA, ver tabla 10.

Tabla 10 Activos encontrados

GRUPO	NOM	AMENAZAS	DIMENSIONES			TIPOS DE ACTIVOS					Degradacion					P
			D	I	C	S	SW	HW	SI	P	S	SW	HW	SI	P	
[N] Desastres Naturales	N1	Fuego	X			X	X	X	X	X	M	P	MA	P	MA	B
	N2	Daños por agua	X					X	X		P	P	A	P	P	B
	N	Desastres naturales	X	X				X	X	X	P	P	MA	P	MA	M
[I] De origen Industrial	I1	Fuego	X			X	X	X	X	X	M	P	MA	P	MA	B
	I2	Daños por agua	X					X	X		P	P	A	P	P	B
	I.*	Desastres Naturales	X					X	X		P	P	MA	P	MA	M
	I3	Contaminación mecánica	X					X			P	P	P	P	P	B
	I4	Contaminación electromagnética	X				X	X			P	P	M	P	P	B
	I5	Avería de origen Físico o lógico	X				X	X			P	P	M	P	P	M
	I6	Corte del suminsitro eléctrico	X			X	X	X	X		P	P	M	P	P	B
	I7	Condiciones inadecuadas de temperatura y/o humedad	X				X	X		X	P	P	M	P	M	M
	I8	Fallo de servicios de comunicaciones	X								P	P	A	P	M	B
	I9	Interrupción de otros servicios y suministros esenciales	X			X					P	P	P	P	P	B
	I 10	Degradación de los soportes de almacenamiento de informa	X				X		X		P	P	P	A	P	B
	I 11	Emanaciones Electromagnéticas			X			X			P	P	MA	P	P	B
[E] Errores y fallos no Intencionados	E1	Errores de los usuarios	X	X	X	X	X				P	A	P	P	P	B
	E3	Errores de monitorización		X			X				P	P	P	A	P	B
	E4	Errores de configuración		X		X	X				P	A	A	P	P	B
	E7	Deficiencias en la organización	X							X	P	P	P	M	A	M
	E8	Difusión de Software dañino	X	X	X		X				M	A	A	P	P	M
	E15	Alteración de la información		X			X				A	P	P	A	M	M
	E17	Degradación de la información		X			X			X	A	P	P	A	A	M
	E18	Destrucción de la información	X				X				A	A	P	A	P	M
	E19	Divulgación de información			X		X			X	P	A	P	P	M	M
	E20	Vulnerabilidades de los programas- Sw	X	X	X		X				P	A	P	P	P	M
	E21	Errores de mantenimiento- actualización de programas	X	X			X				P	A	P	P	P	M
	E23	Errores de mantenimiento- actualización de equipos	X					X			P	P	A	P	P	M
	E24	Caída del sistema por agotamiento de recursos	X			X		X			P	A	M	P	P	M
	E28	Indisponibilidad de personal	X							X	M	P	P	M	A	M
[A] Ataques Intencionados	A1	Deterioro físico en el equipo	X					X			P	P	A	P	P	M
	A2	Deterioro de componentes del equipo	X					X			P	P	A	P	P	M
	A3	Desactualización de programas	X	X		X	X	X			P	A	P	P	P	M
	A4	Manipulación de la configuración	X	X	X	X	X	X	X	X	M	M	P	M	M	M
	A5	Suplantación de la identidad del usuario		X	X		X				M	M	P	M	M	M
	A6	Abuso y privilegio de acceso	X		X		X	X	X		P	MB	MB	MB	P	MB
	A7	Uso no previsto	X			X	X				A	A	A	A	A	M
	A11	Acceso no autorizado		X	X		X			X	M	M	M	M	A	M
	A13	Repudio		X		X	X				M	M	M	M	A	M
	A14	Interceptación de información - escucha			X		X	X		X	P	P	P	P	A	B
	A15	Modificación de la información		X			X			X	A	A	P	A	A	B
	A18	Destrucción de la información	X				X			X	A	A	P	A	A	B
	A19	Divulgación de la información			X		X			X	P	A	P	A	P	B
	A22	Manipulación de los programas	X	X	X		X				P	A	P	A	P	B
	A24	Denegación de servicio	X				X				P	A	P	P	P	B
	A25	Robo	X		X		X	X	X		P	B	B	B	P	MB
	A28	Indisponibilidad del personal	X							X	A	A	A	A	A	M
	A29	Extorsión	X	X	X					X	P	P	P	P	P	MB
	A30	Ingeniería social	X	X	X					X	P	A	P	P	A	M

Luego se muestran agrupadas las amenazas por Probabilidad De Ocurrencia:

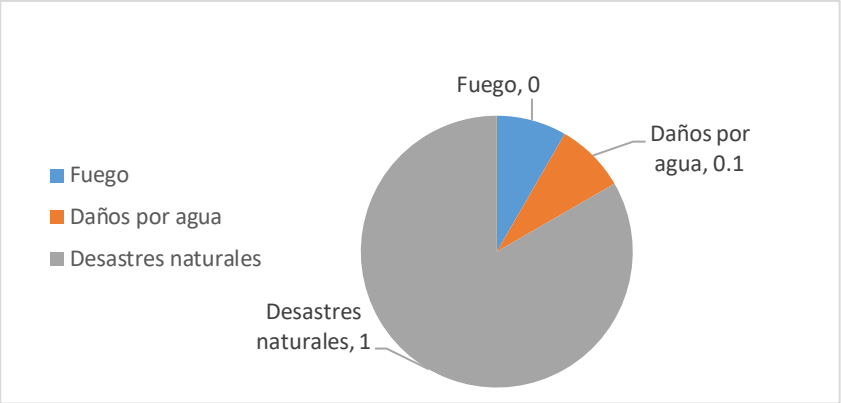


Figura 3. 6 Probabilidad de Ocurrencia de Desastres Naturales

La figura 20 muestra que es más probable que ocurra un daño por desastre natural debido a los últimos acontecimientos en nuestro país por los constantes movimientos telúricos en algunas zonas durante este año 2016.

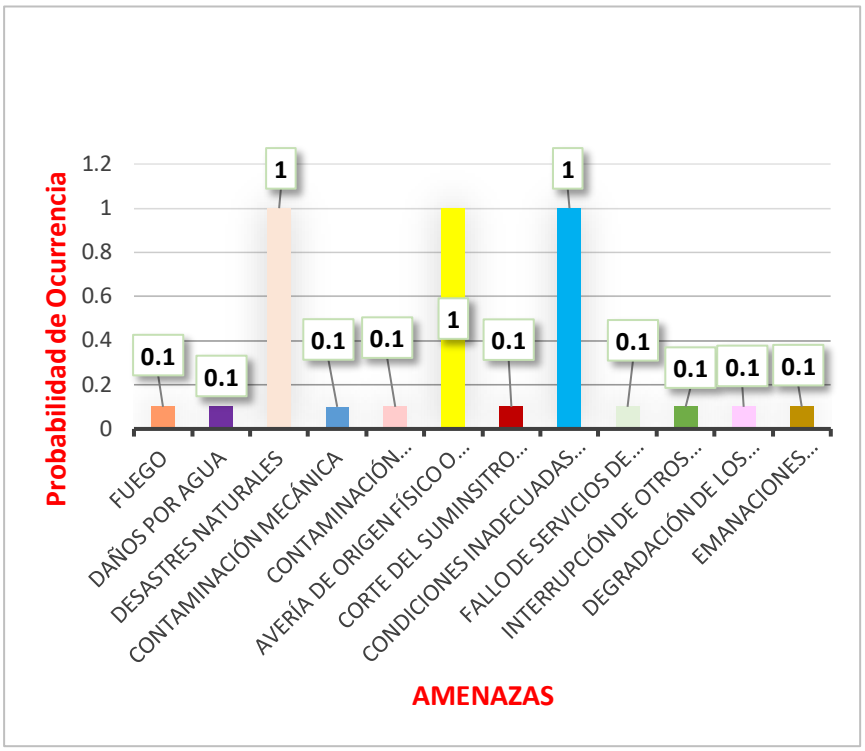


Figura 3. 7 Probabilidad de Ocurrencia de Origen Industrial

En la figura 3.7 las amenazas que se presentan por probabilidad de ocurrencia y que son de ORIGEN INDUSTRIAL más susceptible de materializarse son : las Condiciones Inadecuadas, Avería de origen Físico y por Desastres Naturales.

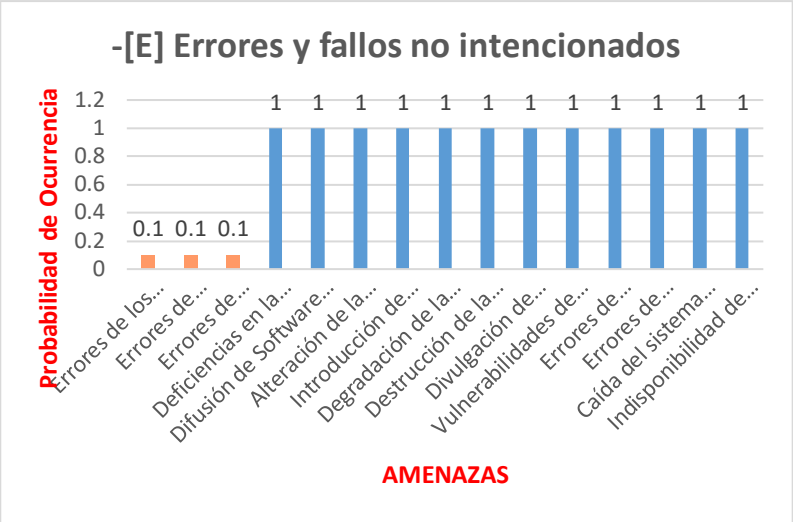


Figura 3. 8 Probabilidad de Errores y Fallos no intencionados

En esta Figura 3.8 se muestra que la **Probabilidad De Ocurrencia de Errores Y Fallos No Intencionados,** las amenazas expuestas serían las que están de color celeste como se detalla a continuación.

- Deficiencias en la organización
- Difusión de Software dañino
- Alteración de la información
- Introducción de información incorrecta
- Degradación de la información
- Destrucción de la información
- Divulgación de información
- Vulnerabilidades de los programas-Sw
- Errores de mantenimiento-actualización de programas
- Errores de mantenimiento-actualización de equipos

- Caída del sistema por agotamiento de recursos
- Indisponibilidad de personal

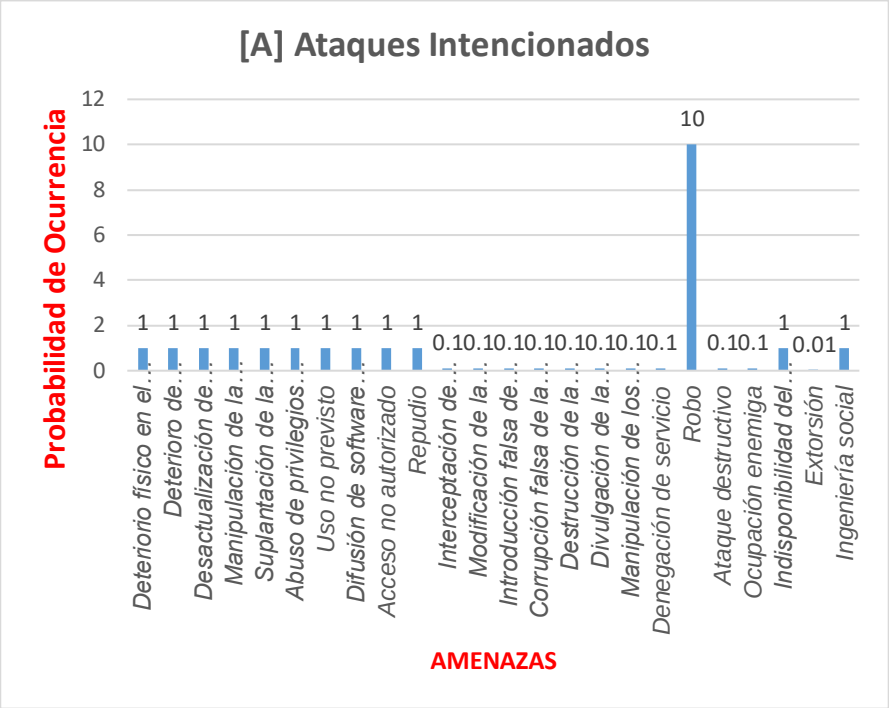


Figura 3. 9 Probabilidad de Ocurrencia de Ataques Intencionados

La figura 3.9 muestra que la Probabilidad de Ocurrencia de un Ataque Intencionado sería con más incidencia el **Robo**, además se registra que por denuncias recabadas por medios de información, las zonas más peligrosas o de más frecuencias de cometer infracciones es la zona Norte conformada por el sector industrial donde está ubicada la empresa FELMOVA, existen dos

publicaciones de Diario El Universo que mencionan que el comercio de la zona de la Ave Carlos Julio Arosemena, se ve afectado por la delincuencia [44], incluso se detalla en capítulo 6 un incidente que sufrió la misma empresa.

Degradación De Activos.

Es cuando un activo pierde una parte de su valor al ser víctima de una amenaza.

La degradación mide el daño causado por un incidente en el supuesto caso de que ocurriera.

Puede haber una valoración de Degradación Nominal como lo muestra la Tabla 11:

Tabla 11 Degradación Nominal

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

O se puede trabajar con una tabla con valoración numérica con porcentajes, como lo indica la tabla 12.

Tabla 12 Valoración numérica por Degradación

NIVELES	DEGRADACION
5%	Baja
30%	Media
50%	Alta
80%	Muy alta
100%	Completa

De igual manera se muestran agrupadas las amenazas por degradación de activos según la tabla mostrada anteriormente:

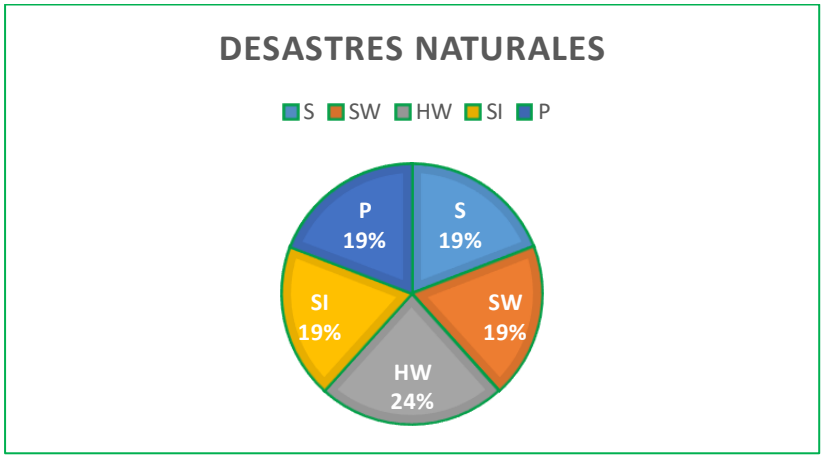


Figura 3. 10 Porcentajes de Afectación de Activos por Desastres Naturales

Muestra la figura 3.10 que la capa de activos declarado como **Hardware** [**HW**] es el más afectado en cuanto a las amenazas tipificadas como Desastres Naturales, y el resto de activos -capas- se ven afectados también en un porcentaje bastante alto, pero en menor proporción.

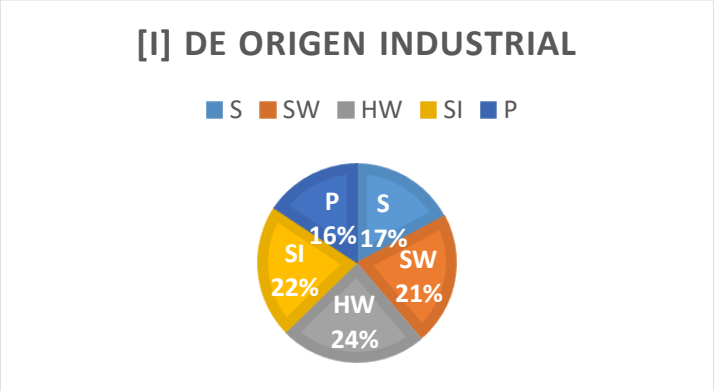


Figura 3. 11 Porcentajes de Afectación de Activos por Origen Industrial

En esta clasificación de activos como lo muestra la Figura 25, también se visualiza que la capa Activo- **Hw** es la más afectada, por las amenazas de Origen Industrial, así como se ven afectados los grupos de activos de **SI** y **SW**.

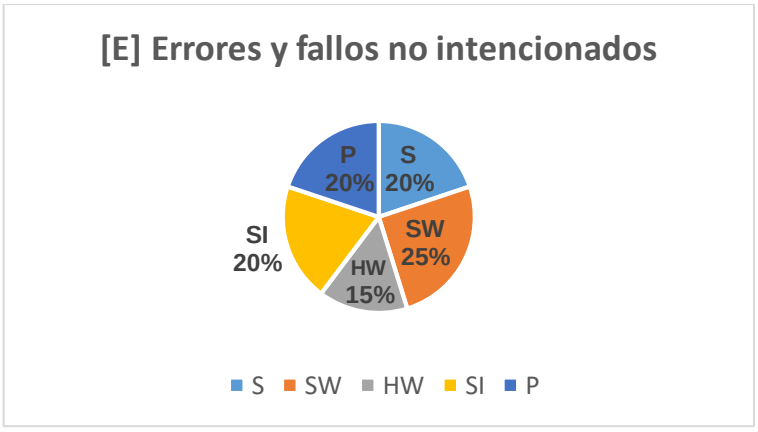


Figura 3. 12 Porcentajes de Afectación de Activos por Errores y Fallos no intencionados

En la figura 3.12 este grupo de activos con la amenaza denominada Errores y Fallos no Intencionados afecta en mayor proporción al **Sw**, y a **S.I**.

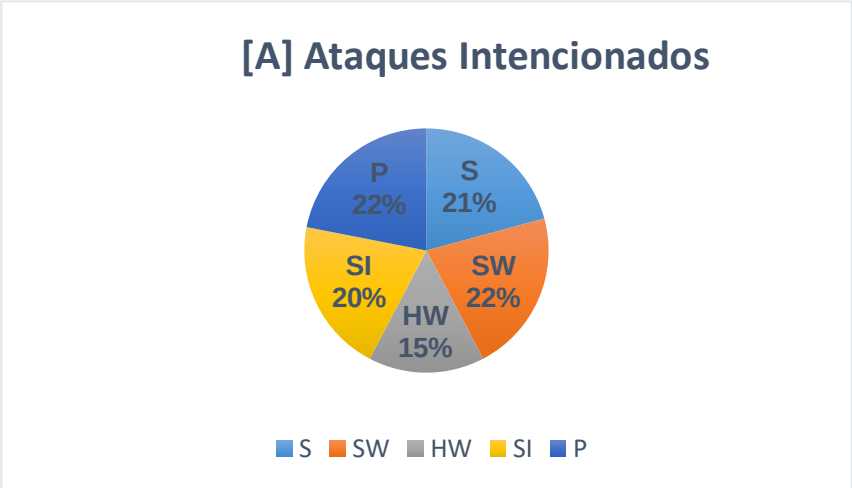


Figura 3. 13 Porcentajes de Afectación de Activos por Ataques Intencionados

En la figura 3.13 los ataques intencionados afectan en mayor proporción a la capa - activo **P(persona)** y al **SW**, debido a que desvaloriza la confianza e integridad de ellos.

Vulnerabilidades

Se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza, o aquellas debilidades de los activos o de sus medidas de protección que facilitan la materialización de una amenaza potencial.

También se lo conoce como agujero, falla, error en la seguridad del sistema de información.

Es decir, se refiere a las ausencias de las salvaguardas pertinentes para proteger el valor propio o acumulado sobre un activo.

Se considera a la vulnerabilidad como una relación entre un activo y una amenaza.

En si la vulnerabilidad como tal no causa daño si no se presenta una amenaza. Es por esta razón que si existe una vulnerabilidad que no tenga ninguna amenaza no necesitará ningún control, sin embargo, se debe monitorear por si ocurre un cambio.

Y sino se toma precauciones esa amenaza puede materializarse.

Las amenazas y vulnerabilidades que no causan impacto no son de importancia.

3.3.5. Cálculo Del Riesgo

El objetivo aquí es identificar y valorar los riesgos, ya que el riesgo es un indicador de lo que probablemente suceda por causa de las amenazas.

Identificación Del Riesgo

La empresa debe tener en claro que la seguridad es un proceso que nunca termina.

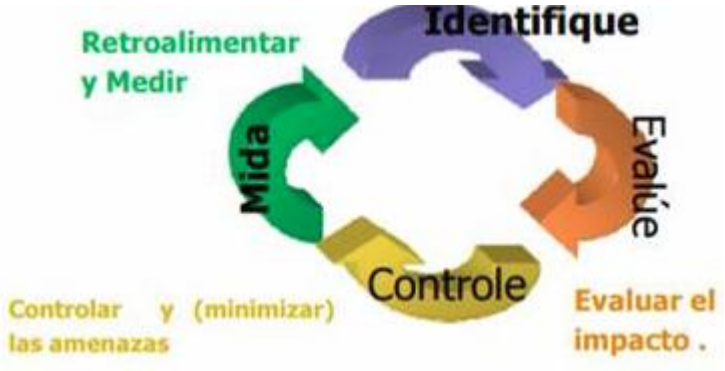


Figura 3. 14 Proceso de Seguridad

Los activos están expuestos a riesgos, por ello es importante identificar los que son mas susceptibles y están más expuestos y que a continuación se describe la relación entre amenazas, vulnerabilidad y riesgo:

Figura 3. 15 Relación entre Amenazas Vulnerabilidad y Riesgo

Amenaza(Condicion) + Impacto(Consecuencia Vulnerabilidad) = Riesgo

Evaluados e identificados los riesgos, se ha seleccionado los activos con un nivel alto de riesgos.

Valoración Del Riesgo

Para valorar el riesgo primero se realiza la identificación de activos, segundo se identifica las amenazas sobre cada activo y por último se estima la vulnerabilidad de las amenazas sobre cada activo, luego se podrá realizar una sencilla evaluación para esta operación.

El nivel de riesgo se divide en cuatro zonas:

- **Bajo**: el nivel de riesgo es bajo y es necesario emplear salvaguardas adicionales.
- **Medio**: El nivel de riesgos es medio y se deberá poner en consideración si se deben implantar salvaguardas para evitarlos.
- **Alto**: El nivel de riesgos es alto y es una obligación implantar salvaguardas para mitigar riesgos.
- **Crítico**: el nivel de riesgo es preocupante porque se deben utilizar obligatoriamente salvaguardas para minimizarlos.

En el análisis de riesgos se debe valorar 4 tipos de riesgos:

• **Riesgo inherente**: referente a la valoración del riesgo sin ningún tipo de control.

• **Riesgo residual**: referente a la valoración del riesgo que persiste luego de haber establecido medidas de control.

• **Riesgo repercutido**: toma en cuenta el valor propio del activo combinándolo con la degradación causada por una amenaza y la frecuencia estimada de la misma.

• **Riesgo acumulado**: toma en cuenta el valor propio de un activo y el valor de los activos que dependen de él, combinándolo con la degradación causada por una amenaza y la frecuencia estimada de la misma.

Impacto Y Riesgo

El impacto se refiere a las consecuencias cuando aparecen las amenazas.

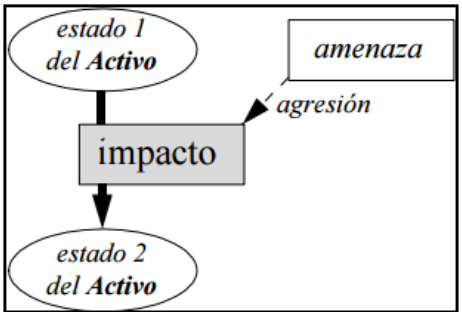


Figura 3. 16 Impacto versus Activos y Amenazas [30]

El IMPACTO y el RIESGO se mitigan por medio de SALVAGUARDAS, viéndose reducidos a valores residuales

MAGERIT considera tres grandes grupos de **Impactos**, según que sus consecuencias sean reductoras del estado de seguridad del Activo agredido directamente (en este caso el Impacto se compone de su Gravedad intrínseca y un Agravante o Atenuante circunstancial); o indirectamente (y en este caso, de forma cualitativa o cuantitativa).

Entonces el Impacto será:

• **Cualitativo con pérdidas funcionales** (de los subestados de seguridad = ahora llamado dimensiones) del Activo

• o bien **Cualitativo con pérdidas orgánicas** (de fondo de comercio, daño de personas)

• o bien **Cuantitativo**, si las consecuencias se pueden traducir a dinero.

El impacto en las organizaciones puede causar:

- Interrupción de actividades
- Sanciones por incumplimiento de normas
- Destrucción y pérdida de activos TIC's
- Desventaja competitiva
- Pérdida de imagen

Por lo que el **Impacto** puede ser de dos tipos: **Acumulado** y **Repercutido** [31]

Para calcular el impacto se tiene la siguiente fórmula;

- **Impacto acumulado= valor acumulado * degradación**

  Se calcula sobre un activo considerando:

  - Su valor acumulado (el propio más el acumulado por los activos que dependen de él)
  - Las amenazas al que está expuesto

- **Impacto Repercutido = valor propio * degradación**

  Se calcula sobre un activo considerando:

- Su valor propio
- Las amenazas a las que está expuesto el activo.

Valoración De Amenazas E Impacto

Se puede calcular el impacto en base a tablas sencillas de doble entrada:

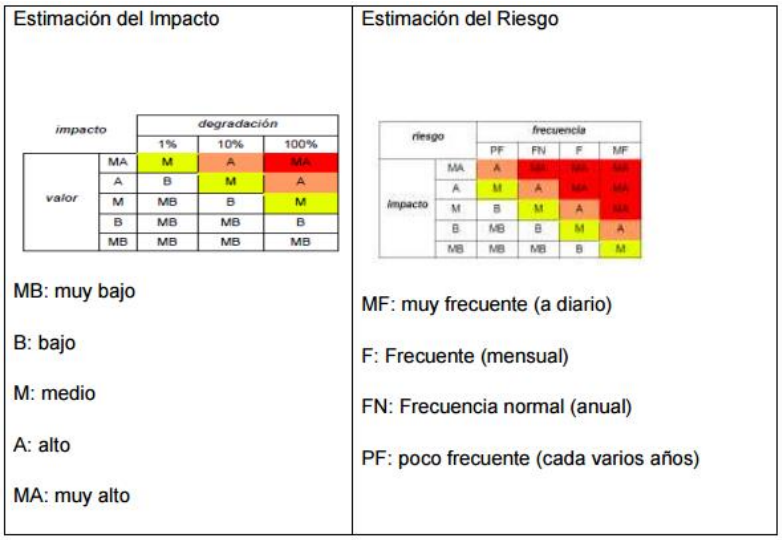


Figura 3. 17 Estimación del Impacto y del Riesgo

Aquellos activos que reciban una calificación de impacto muy alto (MA) deberían ser objeto de atención inmediata.

Estimación Del Estado Del Riesgo

Informe que detalla para cada activo el impacto y el riesgo potenciales y residuales frente a las amenazas.

Riesgo acumulado. En el cálculo del riesgo acumulado, se usará el impacto acumulado sobre el activo**.**

Riesgo repercutido. En el cálculo del riesgo repercutido, se usará el impacto repercutido sobre el activo**.**

Riesgo = Valor del Activo x Vulnerabilidad x Impacto

Valoración De Amenazas – Riesgos.

riesgo		*probabilidad*				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Figura 3. 18 Magerit – Método de Análisis de Riesgos- AI03

Es un proceso general del análisis del riesgo y la evaluación del riesgo.

Es decir que lo que hay que tomar en cuenta es la relación entre amenaza-incidente-impacto, es una condición que se deberá revisar al momento de dar prioridad a ciertas acciones de seguridad para proteger los activos de la organización.

A continuación, se muestra la tabla 13 donde los diferentes activos agrupados por capas muestran su frecuencia de posibles amenazas y su degradación en caso de llegar a materializarse.

Tabla 13 Valoración numérica por Degradación y Frecuencia

NIVELES	DEGRADACIÓN	PERIODICIDAD	FRECUENCIA
25%	Poco(P)	360	A diario
50%	Medio(M)	12	Mensualmente
75%	Alto (A)	4	Cuatro veces al año
100%	Muy Alto (MA)	2	Dos veces al año
		1	Una vez al año
		1/12	Cada varios año

Tabla 14 Identificación de Amenazas -Frecuencia - Degradación. Fuente: Autor

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	DEGRADACION
DATOS	Bases de datos/Contraseñas/Datos clasificados/Datos Públicos	Incendio	1	25%
		Inundaciones		
		Desastres Naturales		
		Contaminación mecánica		
		Corte de Suministro eléctrico		
		Condiciones inadecuadas de temperatura y/o humedad		
		Errores de Mantenimiento/ Actualización de equipos - HW		
		Robo		
		Alteración de la información		
		Abuso de privilegios		
		Ingreso de información incorrecta		
		Degradación de los soportes de almacenamiento de inform		
		Divulgación de la información		
		Errores de usuarios		
		Ingeniería Social		
		Destrucción de la información		
SW	Inventario de Datos / Soporte de Información/ Sist. Operativo/servidor	Errores de l Administrador	2	25%
		Errores de usuarios		
		Errores de monitorización - log		
		Ingreso de información incorrecta		
		Errores de Mantenimiento/ Actualización de equipos - HW		
		Caída del sistema por agotamiento de recursos		
		Denegación de servicio		
		Errores de configuración		
		Deficiencias en la organización		
		Difusión de Software dañino		
		Alteración de la información		
		Introducción de información incorrecta		
		Degradación de la información		
HW	Equipos medios	Fuego	2	25%
		Daños por agua		
		Desastres Naturales		
		Contaminación mecánica		
		Contaminación electromagnética		
		Avería de origen Físico o lógico		
		Corte del suminsitro eléctrico		
		Condiciones inadecuadas de temperatura y/o humedad		
		Errores de mantenimiento- actualización de equipos		
		Caída del sistema por agotamiento de recursos		
		Emanaciones Electromagnéticas		
		Deterioro físico en el equipo		
		Deterioro de componentes del equipo		
		Desactualización de programas		
		Manipulación de la configuración		
		Abuso y privilegio de acceso		
		Interceptación de información - escucha		
SERVICIOS	Entrega de Productos a clientes	Fuego	2	25%
		Corte del suministro eléctrico		
		Interrupción de otros servicios y suministros esenciales		
		Indisponibilidad del personal		

Tabla 15 Identificación de Amenazas y Vulnerabilidades. Fuente: Autor

CAPAS	ACTIVOS	AMENAZAS	VULNERABILIDADES
DATOS	Bases de datos/Contraseñas/Datos clasificados/Datos Públicos	Incendio	Edificación no apropiada y poco segura.
		Inundaciones	
		Desastres Naturales	
		Contaminación mecánica	
		Corte de Suministro eléctrico	Cálculo inapropiado de consumo de energía eléctrica y poca previsión de crecimiento.
		Condiciones inadecuadas de temperatura y/o humedad	Mala coordinación de mantenimientos de equipos
		Errores de Mantenimiento/ Actualización de equipos – HW	Poco conocimiento en manejo de equipos.
		Robo	Evaluación poco cuidadosa de la fuerza de trabajo
		Alteración de la información	Ausencia de políticas de contraseñas
		Abuso de privilegios	
		Ingreso de información incorrecta	
		Degradación de los soportes de almacenamiento de	Ausencia de etiquetado (clasificación) de la información
		Divulgación de la información	Wifi Abierta y mala configuración de seguridad
		Errores de usuarios	Manejo incorrecto de errores
		Ingeniería Social	Desconocimiento de políticas de seguridad
		Destrucción de la información	Ausencia de políticas de contraseñas
SW	Inventario de Datos / Soporte de Información / Sist. Operativo/Servidor	Errores del Administrador	Manejo incorrecto de errores
		Errores de usuarios	
		Errores de monitorización – log	
		Ingreso de información incorrecta	Mala administración de accesos físicos y lógicos.
		Errores de Mantenimiento/ Actualización de equipos – HW	Poco conocimiento en manejo de equipos.
		Caída del sistema por agotamiento de recursos	Cálculo inapropiado de consumo de energía eléctrica y no previsión de crecimiento.
		Denegación de servicio	Puertas traseras activas
		Errores de configuración	Mala administración de accesos físicos y lógicos.
		Deficiencias en la organización	Desconocimiento de políticas de seguridad
		Difusión de Software dañino	Mala administración de accesos físicos y lógicos.
		Alteración de la información	
		Introducción de información incorrecta	Ausencia de procedimientos de manejo de información clasificada
		Degradación de la información	Desconocimiento de políticas de seguridad
HW	Equipos medios	Fuego	Edificación no apropiada y poco segura.
		Daños por agua	
		Desastres Naturales	
		Contaminación mecánica	
		Contaminación electromagnética	
		Avería de origen Físico o lógico	Mala coordinación de mantenimientos de equipos
		Corte del suministro eléctrico	Cálculo inapropiado de consumo de energía eléctrica y poca previsión de crecimiento.
		Condiciones inadecuadas de temperatura y/o humedad	Mala coordinación de mantenimientos de equipos
		Errores de mantenimiento- actualización de equipos	Poco conocimiento en manejo de equipos.
		Caída del sistema por agotamiento de recursos	Cálculo inapropiado de consumo de energía eléctrica y poca previsión de crecimiento.
		Deterioro físico en el equipo	Mala coordinación de mantenimientos de equipos
		Deterioro de componentes del equipo	
		Desactualización de programas	Documentación técnica y operativa escasa o desactualizada
		Manipulación de la configuración	Deficiente administración de usuarios y permisos
		Abuso y privilegio de acceso	Inexistente cifrado de información y mala administración de contraseñas.
		Interceptación de información – escucha	Inexistente cifrado de información y mala administración de contraseñas.
Servicios	Entrega de Productos a Clientes	Fuego	Edificación no apropiada y poco segura.
		Corte del suministro eléctrico	Cálculo inapropiado de consumo de energía eléctrica y poca previsión de crecimiento.
		Interrupción de otros servicios y suministros esenciales	Desconocimiento de políticas de seguridad
		Indisponibilidad del personal	Evaluación poco cuidadosa de la fuerza de trabajo

Como Manejar El Riesgo

Para manejar el riesgo se tienen las siguientes opciones: [3]

- **Evitar**: o sustituir el activo por otro que no se vea afectado por la amenaza o eliminar la actividad que lo produce.

- **Reducir o Mitigar**: Tomando como medida oportuna un nivel de riesgo que lo sitúe por debajo del umbral, tal es que se lo consigue por medio de :
    - Reducir la probabilidad o frecuencia de ocurrencia, tomando una medida preventiva.
    - Reducir el impacto de la amenaza o acotar el impacto, fijando controles y revisando cómo funcionan las medidas preventivas.
- **Transferir o Asignarlo A Terceros**: A veces la organización no tiene los medios y debe contratar a un externo con capacidad para reducir y gestionar el riesgo. A los terceros se los considera a los proveedores o los seguros.
- **Asumir o Aceptar**. Se asume el riesgo bien porque está por debajo del umbral o porque los costes para tratarle son elevados pero su probabilidad de ocurrencia es muy baja o porque la empresa no desea desaprovechar una oportunidad de negocio, aunque sea arriesgada.

Figura 3. 19 Opciones de Tratamiento de Riesgo

A continuación se muestran los mapas de calor de los tipos de Activos: Hardware, Software, Datos, y Servicios según las amenazas a las que pueden estar expuestos como : Desastres Naturales, Origen Industrial, Errores no intencionados y Fallos intencionados

Anteriormente ya se mostró en las tablas 8 y 9 una lista en detalle de las posibles amenazas a las que puede ser susceptible la organización.

MAPA DE RIESGO INHERENTE

No. Riesgo	Amenaza
❶	Infección de sistemas a través de unidades portables sin escaneo
❷	Exposición o extravío de equipo, unidades de almacenamiento, etc.
❸	Pérdida de datos por error hardware
❹	Falta de mantenimiento físico (proceso, repuestos e insumos)

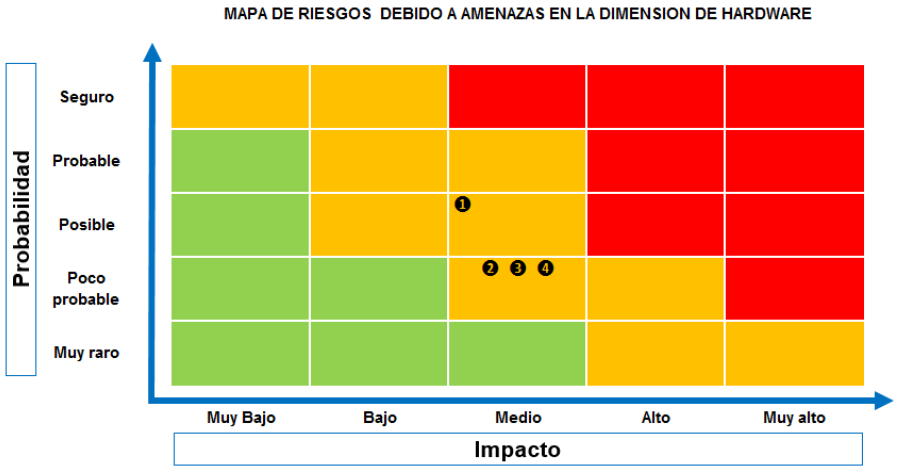


Figura 3. 20 Amenazas en la dimensión de hardware

En la figura 3.20 se muestra en el mapa de riesgos como las amenazas asociadas al Tipo de Activo Hardware tienen una probabilidad de ocurrencia y un impacto si llegaran a materializarse.

MAPA DE RIESGO INHERENTE

No. Riesgo	Amenaza	C
❶	Alteración de la información	
❷	Abuso de privilegios	
❸	Ingreso de información incorrecta	
❹	Degradación de los soportes de almacenamiento de informac	
❺	Divulgación de la información	
❻	Errores de usuarios	
❼	Ingeniería Social	
❽	Destrucción de la información	

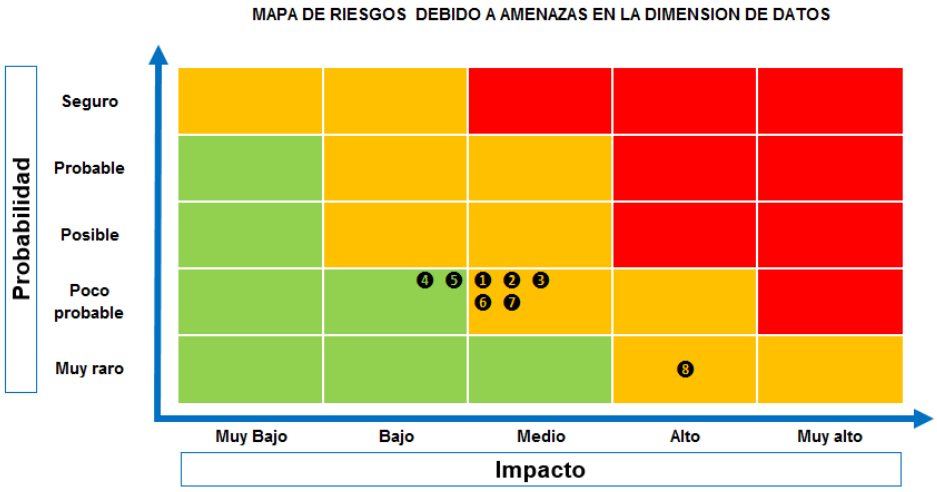


Figura 3. 21 Amenazas en la dimensión de Datos

En la figura 3.21 se muestra en el mapa de riesgos las amenazas asociadas al Tipo de Activo Datos con una probabilidad de ocurrencia y un impacto si llegaran a materializarse.

MAPA DE RIESGO INHERENTE

No. Ries	Amenaza
❶	Errores del Administrador
❷	Errores de usuarios
❸	Ingreso de información incorrecta
❹	Errores de Mantenimiento/ Actualización de equipos - HW
❺	Caída del sistema por agotamiento de recursos
❻	Denegación de servicio
❼	Errores de configuración
❽	Deficiencias en la organización
❾	Difusión de Software dañino
❿	Alteración de la información
⓫	Alteración de la información
⓬	Degradación de la información
⓭	Destrucción de la información
⓮	Divulgación de información
⓯	Vulnerabilidades de los programas- Sw

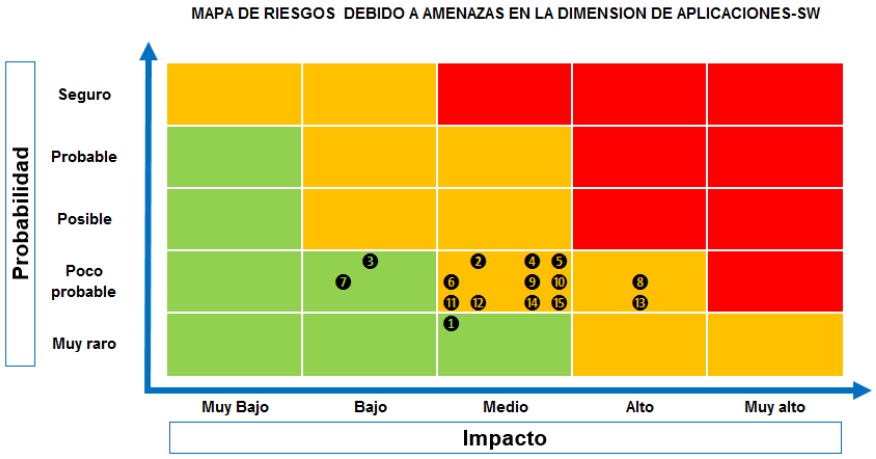


Figura 3. 22 Amenazas en la dimensión de SW

En la figura 3.22 se muestra en el mapa de riesgos las amenazas asociadas al Tipo de Activo Aplicaciones, ya que son los más vulnerables porque almacenarán la información de la empresa con una probabilidad de ocurrencia y un impacto si llegaran a materializarse.

MAPA DE RIESGO INHERENTE

No. Riesgo	Amenaza
❶	Desastres Naturales
❷	De origen Industrial
❸	Errores no Intencionados
❹	Errores Intencionados

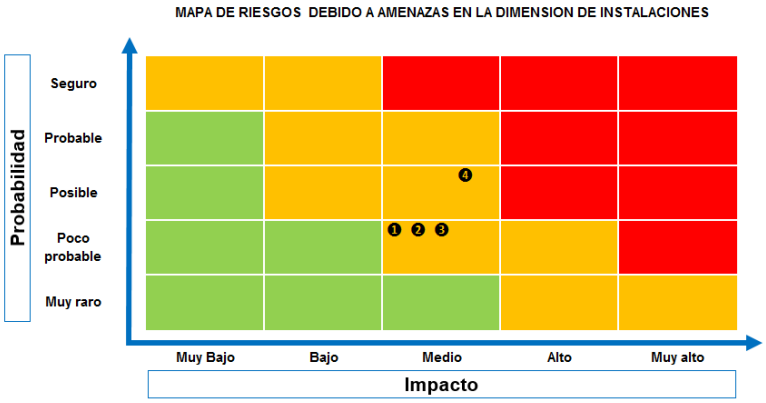


Figura 3. 23 Amenazas en la dimensión de Instalaciones

En la figura 3.23 se muestra en el mapa de riesgos las amenazas asociadas al Tipo de Activo Instalaciones con una probabilidad de ocurrencia y un impacto si llegaran a materializarse.

MAPA DE RIESGO INHERENTE

No. Riesgo	Amenaza
❶	Fuego
❷	Corte del suminsitro eléctrico
❸	Interrupción de otros servicios y suministros esenciales
❹	Indisponibilidad del personal

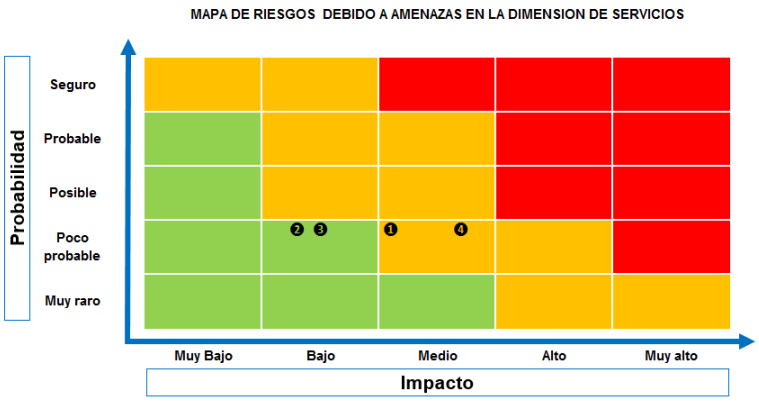


Figura 3. 24 Amenazas en la dimensión de SW

En la figura 38 se muestra en el mapa de riesgos las amenazas asociadas al Tipo de Activo Servicios y que puedan causar algún daño sobre los activos, con una probabilidad de ocurrencia y un impacto si llegaran a materializarse.

Riesgo Acumulado

Usando el aplicativo PILAR, se puede apreciar en la gráfica, que el **riesgo acumulado** en la situación potencial de la empresa, muestra niveles altos y críticos del activo **HARDWARE y DATOS**.

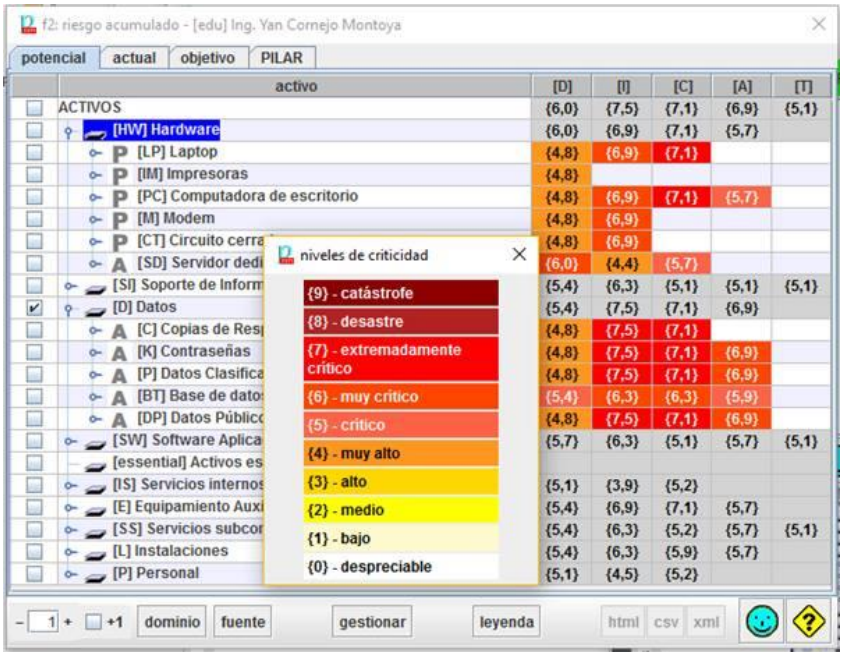


Figura 3. 25 Riesgo Acumulado Estado Potencial (Hw, Datos)

Pero gestionando con aplicativo PILAR se tiene esta nueva valoración sugerida:

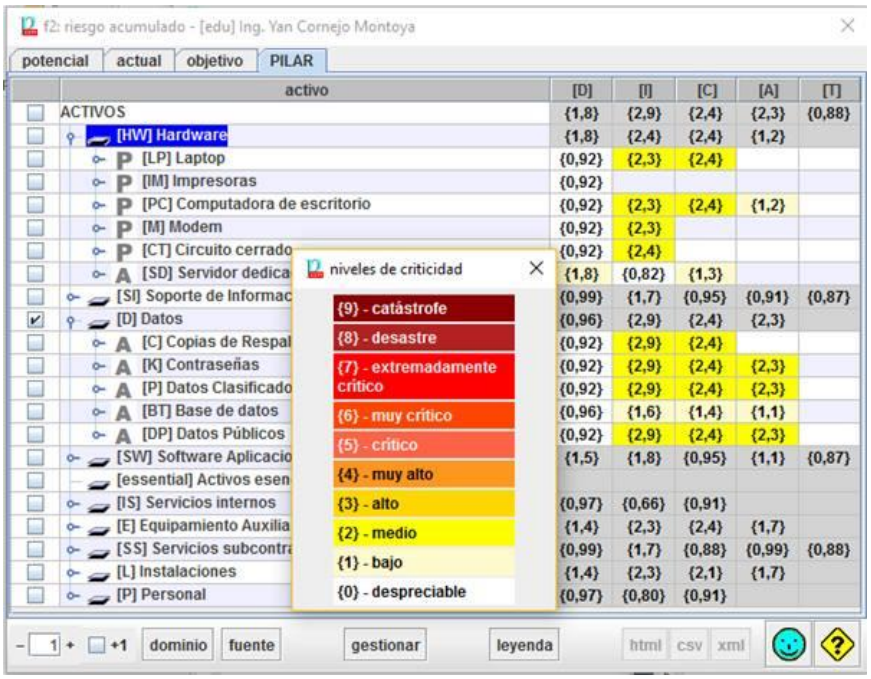


Figura 3. 26 Riesgo Acumulado Aplicando PILAR (Hw, Datos)

En donde al aplicar salvaguardas el riesgo acumulado residual es menor al riesgo acumulado potencial, cambian a color amarillo debido a los controles aplicados.

Riesgo Repercutido.

En los riesgos repercutidos, en la situación actual con el aplicativo PILAR se muestra la figura 3.27:

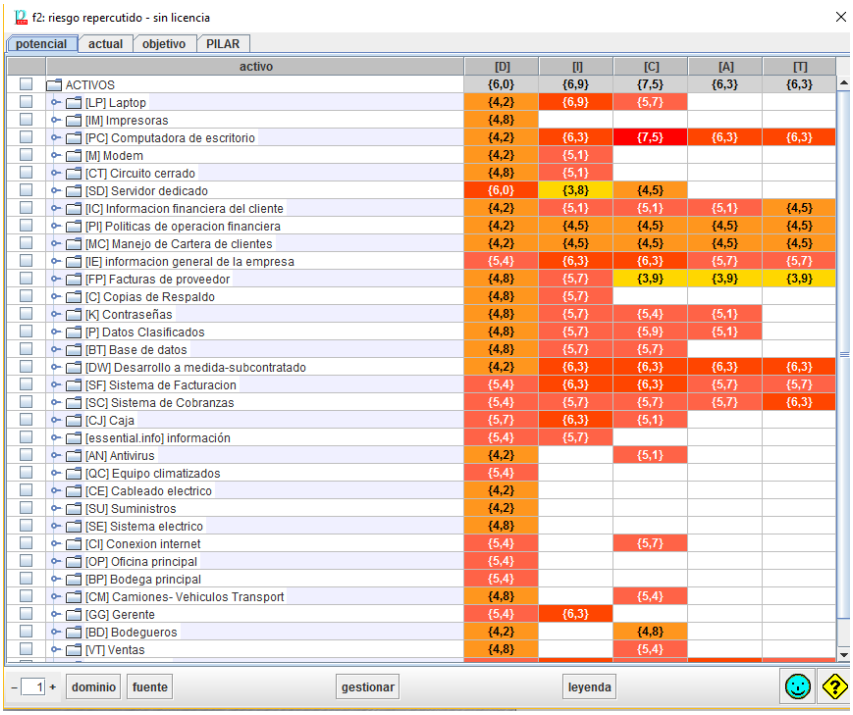
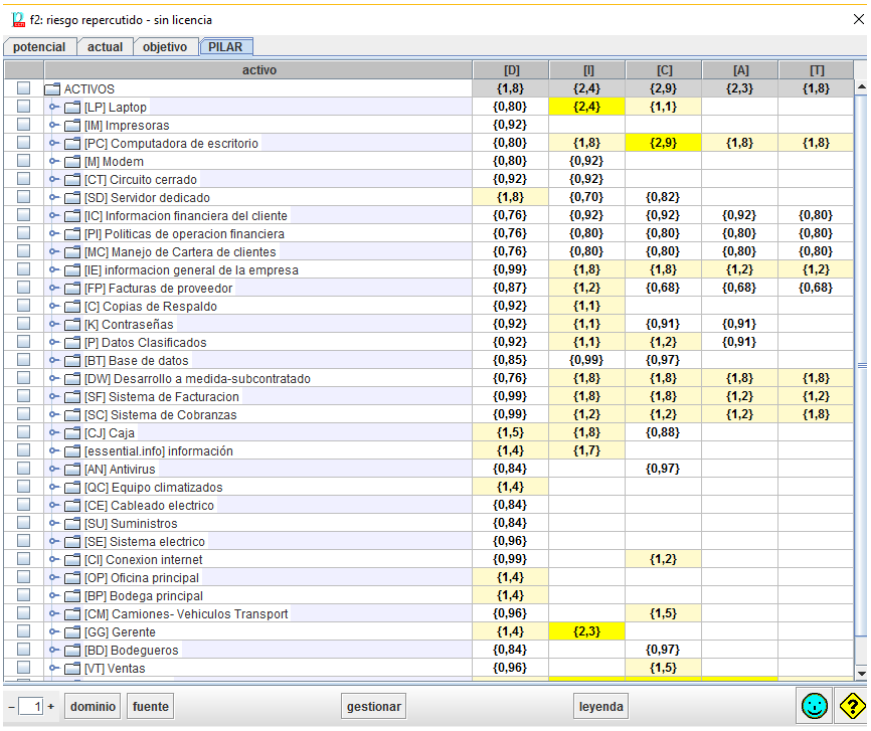


Figura 3. 27 Riesgo Repercutido

Y aplicando salvaguardas en situación con PILAR se tiene:



activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{1,8}	{2,4}	{2,9}	{2,3}	{1,8}
[LP] Laptop	{0,80}	{2,4}	{1,1}		
[IM] Impresoras	{0,92}				
[PC] Computadora de escritorio	{0,80}	{1,8}	{2,9}	{1,8}	{1,8}
[M] Modem	{0,80}	{0,92}			
[CT] Circuito cerrado	{0,92}	{0,92}			
[SD] Servidor dedicado	{1,8}	{0,70}	{0,82}		
[IC] Informacion financiera del cliente	{0,76}	{0,92}	{0,92}	{0,92}	{0,80}
[PI] Politicas de operacion financiera	{0,76}	{0,80}	{0,80}	{0,80}	{0,80}
[MC] Manejo de Cartera de clientes	{0,76}	{0,80}	{0,80}	{0,80}	{0,80}
[IE] informacion general de la empresa	{0,99}	{1,8}	{1,8}	{1,2}	{1,2}
[FP] Facturas de proveedor	{0,87}	{1,2}	{0,68}	{0,68}	{0,68}
[C] Copias de Respaldo	{0,92}	{1,1}			
[K] Contraseñas	{0,92}	{1,1}	{0,91}	{0,91}	
[P] Datos Clasificados	{0,92}	{1,1}	{1,2}	{0,91}	
[BT] Base de datos	{0,85}	{0,99}	{0,97}		
[DW] Desarrollo a medida-subcontratado	{0,76}	{1,8}	{1,8}	{1,8}	{1,8}
[SF] Sistema de Facturacion	{0,99}	{1,8}	{1,8}	{1,2}	{1,2}
[SC] Sistema de Cobranzas	{0,99}	{1,2}	{1,2}	{1,2}	{1,8}
[CJ] Caja	{1,5}	{1,8}	{0,88}		
[essential.info] información	{1,4}	{1,7}			
[AN] Antivirus	{0,84}		{0,97}		
[QC] Equipo climatizados	{1,4}				
[CE] Cableado electrico	{0,84}				
[SU] Suministros	{0,84}				
[SE] Sistema electrico	{0,96}				
[CI] Conexion internet	{0,99}		{1,2}		
[OP] Oficina principal	{1,4}				
[BP] Bodega principal	{1,4}				
[CM] Camiones- Vehiculos Transport	{0,96}		{1,5}		
[GG] Gerente	{1,4}	{2,3}			
[BD] Bodegueros	{0,84}		{0,97}		
[VT] Ventas	{0,96}		{1,5}		

Figura 3. 28 Riesgo Repercutido Residual aplicando Salvaguardas

En donde el **riesgo repercutido residual** es menor al **riesgo repercutido** potencial, debido a la sugerencia de salvaguardas propuesta por el aplicativo PILAR.

Identificación Y Valoración De Impactos

Un impacto es el resultado del daño que causa o puede causar sobre el activo derivado de la materialización de una amenaza.

De acuerdo al tipo de pérdida se muestran como se evalúan los impactos, ya que causarán degradación en alguna de las

siguientes características: confidencialidad, integridad y disponibilidad.[32]

- **Pérdida de Confidencialidad**: hace referencia a la protección de la información contra la divulgación no autorizada. El impacto producido por un evento de estas características, sea en forma no autorizada, intencional o inadvertida, puede variar entre la pérdida de confianza en la institución hasta la posibilidad de acciones legales contra la misma

- **Pérdida de Integridad**: Se refiere al requerimiento de que el activo o la información sea protegido contra la modificación no autorizada. Se pierde integridad si se realizan cambios no autorizados en los sistemas o se pierde parte de los datos almacenados sea por un evento accidental o intencionado.

- **Pérdida de Disponibilidad**: El hecho de que la información o un sistema no esté disponible para sus usuarios, ya sea por la pérdida de datos o la destrucción de elementos necesarios, puede afectar a la efectividad operacional y consecuentemente al cumplimiento de la misión de una organización.

Figura 3. 29 Niveles de calificación del impacto utilizado en PILAR

Impacto Acumulado.

Es el que se calcula en base a :

- Su valor acumulado
- Las amenazas a las que se expone

El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada.

El impacto es mayor cuanto mayor es la valoración propia o acumulada sobre un activo.

El impacto es mayor en cuanto mayor sea la degradación del activo atacado.

El impacto acumulado, al calcularse sobre los activos, permite determinar las salvaguardas que se necesitarán para: protección de equipos, copias de respaldo, etc.

En el **Impacto Acumulado Potencial** – figura 3.30 -se muestra la siguiente valoración en la situación actual en el tipo de Activos Software (SW).

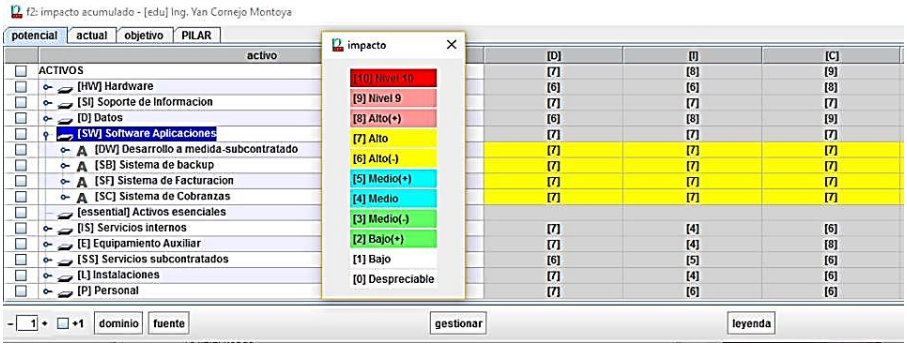


Figura 3. 30 Impacto Acumulado estado Potencial

Pero gestionando con PILAR muestra un cambio, ya que sería el **Impacto Acumulado Residual** que mostraría una valoración menor porque se ha aplicado las salvaguardas-controles que sugiere PILAR:

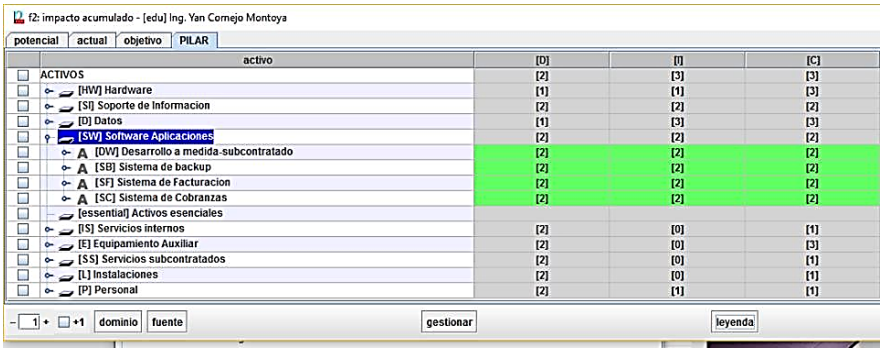


Figura 3. 31 Impacto Acumulado aplicando PILAR

Como se puede apreciar en la figura 3.20, baja la valoración a 2, esto debido a que PILAR aplica las salvaguardas correspondientes conforme a la norma ISO 27002:2013

Impacto Repercutido

El **impacto Repercutido** es el que se calcula sobre un activo en base a :

- Su valor propio
- Las amenazas a que están expuestos los activos de los que depende

El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada.

El impacto será mayor si el valor del activo es alto.

El impacto será mayor si el activo atacado sufre una mayor degradación.

El impacto repercutido permitirá calcularse sobre los activos cuya valoración permitirá que se determine las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Esto con el afán de ayudar a tomar decisiones críticas en un análisis de riesgos en cuanto a la aceptación de un nivel de riesgo.

En el aplicativo PILAR se muestra el **Impacto Repercutido – Figura 3.32 -** en situación actual de uno de los activos de información como es el Sistema de Facturación.

[SF] Sistema de Facturacion	[7]	[7]	[7]
[D] disponibilidad	[7]		
[I] integridad de los datos		[7]	
[C] confidencialidad de los datos			[7]
[A] autenticidad de los usuarios y de la información			
[T] trazabilidad del servicio y de los datos			

Figura 3. 32 Impacto Repercutido situación Actual

En donde el programa PILAR, aplicando las salvaguardas nos muestra el **Impacto Repercutido Residual** que es menor que el actual – Figura 3.33.

☑ [SF] Sistema de Facturacion	[2]	[2]	[2]
☐ [D] disponibilidad	[2]		
☐ [I] integridad de los datos		[2]	
☐ [C] confidencialidad de los datos			[2]
☐ [A] autenticidad de los usuarios y de la información			
☐ [T] trazabilidad del servicio y de los datos			

Figura 3. 33 Impacto Repercutido aplicando PILAR

Esto es debido a que las salvaguardas reducen el riesgo de que se materialicen posiblemente las amenazas en los activos.

3.3.6. Salvaguardas

Las salvaguardas son medidas de protección frente a las amenazas y pueden convertirse en procedimientos para ayudar a prevenir riesgos e impactos.

Implantar las salvaguardas en la organización ayudará a prevenir, impedir, reducir o controlar a los riesgos identificados.

ciclo de vida	*protección del valor*
• Especificación del servicio • Desarrollo del servicio • Despliegue del servicio • Operación del servicio • Terminación del servicio	[A_S] → • Control de acceso [T_S] → • Registro de actuaciones • Registro de incidencias [D] → • Plan de continuidad

Figura 3. 34 Salvaguardas por Activos/ Servicios

La figura 3.34 muestra una clasificación de salvaguarda que propone MAGERIT para activos de servicios. El ciclo de vida tiene relación con el funcionamiento continuo del servicio, y la

protección del valor se refiere a las acciones a tomar en la organización, tomando en cuenta las dimensiones de valoración del servicio.[29]

Para la selección de controles, MAGERIT propone una variedad de las mismas, por lo que se debe seleccionar cual sería la más efectiva como protección contra las amenazas. Por lo que se debería hacer las siguientes preguntas:

- ¿Qué tipos de activos se va a proteger?
- ¿De qué amenazas necesitamos protegernos?
- ¿Existen controles alternativos?
- ¿Cuáles son las dimensiones de seguridad que requieren protección?

Es decir que los controles limitan el factor de degradación de valor.

Los controles también se caracterizan no sólo por su existencia sino por su eficacia frente al riesgo.

El control de acceso es un servicio de controles recurrente que se aplica a muchos tipos de activos: acceso a los servicios, acceso a las aplicaciones, acceso al sistema operativo, acceso a los soportes de información, acceso físico a las instalaciones, etc.

Los mecanismos de identificación y autenticación son muchos y se pueden combinar:

- Contraseñas
- Certificados digitales
- Dispositivos (tokens – tarjetas)
- Características biométricas.

Los controles presentan respuesta al riesgo, basados en procedimientos, políticas empresariales, soluciones técnicas (hardware, software, comunicaciones y seguridad física).

Los **controles** permitirán mantener a los sistemas más protegidos, ya que son mecanismos tecnológicos que reducirán el riesgo de la siguiente manera:

- Reduciendo la frecuencia de las amenazas: medidas preventivas para limitar la materialización de la amenaza.
- Limitando el impacto: medidas correctoras y en menor medida las detectivas, las cuales mitigan el impacto ante la materialización de la amenaza o lo que es lo mismo, disminuyen el factor de degradación de valor.

Las salvaguardas según el catálogo de MAGERIT contempla un listado, por lo que se debería formular preguntas como:

• ¿Qué tipo de activos se va a proteger?

• ¿De qué amenazas necesitamos protegernos?

• ¿Existen salvaguardas alternativas?

• ¿Cuáles son las dimensiones de seguridad que requieren protección?

MAGERIT proporciona un catálogo de salvaguardas (ver Anexo 3) de acuerdo a las recomendaciones de la ISO/IEC 27001, y 27002. De la siguiente forma: [33]

- Protecciones generales u horizontales
- Protección de los datos / información
- Protección de las claves criptográficas
- Protección de los servicios
- Protección de las aplicaciones (software)
- Protección de los equipos (hardware)
- Protección de las comunicaciones
- Protección de los soportes de información
- Protección de los elementos auxiliares

- Seguridad física – Protección de las instalaciones
- Salvaguardas relativas al personal *"Son aquellas que se refieren a las personas que tienen relación con el sistema de información".*
- Salvaguardas de tipo organizativo

A continuación, se detallan los procedimientos de cada una de las salvaguardas que se recomiendan para este estudio, conforme al catálogo mencionado.

Este catálogo clasifica las diferentes protecciones materiales, tecnológicas, organizativas y procedimentales sobre los activos de información de cualquier organización, pudiendo agregarse o eliminarse en caso de no aplicabilidad.

También el realizar una correcta valoración de las salvaguardas se puede optimizar el cálculo de los riesgos, por lo que MAGERIT sugiere lo siguiente: [33]

1. La Reducción de la probabilidad de las amenazas: "Se *llaman salvaguardas preventivas. Las ideales llegan a impedir completamente que la amenaza se materialice".*

2. La Limitación del daño causado: "Hay *salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación*

Por lo que aplicando un buen conjunto de salvaguardas sobre los activos de información que presenten riesgos, puede traer beneficios a todos los stakeholders interesados.

Tabla 16 Tratamiento de Riesgos: Servicios Fuente: Autor

CAPAS	ACTIVOS	AMENAZAS	VULNERABILIDADES	OPCIÓN DE TRATAMIENTO DE RIESGO	SALVAGUARDAS - CONTROLES
software	Inventario de Datos / Soporte de Información/ Sist. Operativo/servidor	[I.5] Avería de origen físico o lógico	· I.5.1 Fallo en los programas	Reducción	• A.7.1.2 Términos y condiciones del empleo (A.5) • A.9.1.2 Acceso a redes y a servicios de red (E.8)
			· I.5.2 Acceso no permitido		
		[E.1] Errores de los usuarios	• E.1.1 Error en ingreso de datos • E.1.2 Errores de uso del sistema		• A.9.2.3 Gestión de derecho de acceso privilegiado (E.8, A.5,E.15)
		[E.8] Difusión de software dañino	E.8.1 Propagación no intencional de virus		• A.9.2.4 Gestión de información de autenticación secreta de usuarios (I.5.2, E.19,A.5)
		[E.15] Alteración accidental de información	• E.15.1 Desconocimiento del procedimiento • E.15.2 Pobre inducción del sistema		• A.9.3.1 Uso de información de autenticación secreta (I.5.2, E.19,A.5)
		[E.18] Destrucción de información	E.18.1 Pérdida accidental de información		• A.9.4.1 Restricción de acceso a la información (I.5, E.1)
		[E.19] Fuga de información	E.19.1 Revelación de información por indiscreción ya sea verbalmente, medios electrónicos o papel.		• A.9.4.5 Control de acceso a códigos fuentes de programas(I.5, E.20,E.21)
		[E.20] Vulnerabilidad de los programas	• E.20.1 Defectos del código • E.20.2 Operación errónea		• A.14.2.7 Desarrollo contratado externamente (I.5, E.21,E.20)
		[E.21] Errores de mantenimiento y actualización de programas	• E.21.1 Procedimientos y controles ineficientes para pase de programas a producción. • E.21.2 Procedimientos y controles ineficientes para revisiones de software contratado externamente. • E.21.3 No cumple con reglas del negocio		• A.14.2.8 Pruebas de seguridad de sistemas (I.5, E.21,E.20)
		[A.5] Suplantación de identidad del usuario	• A.5.1 Desconocimiento por parte del personal de las políticas de seguridad • A.5.2 Desconocimiento de responsabilidades en referencia a la labor que realiza. • A5.3 Contraseñas débiles -fáciles de averiguar		
DATOS	Bases de datos/Contraseñas/Datos clasificados/Datos Públicos	[N.1] Incendio	• N.1.1 Escaso equipo contra incendios. • N.1.2 Mala política de escritorio limpio. • N.1.3 No cumplimiento de reglamento interno en lo que se refiere a normas de buena conducta	Reducción	• A.9.1.1 Política de control de acceso(A.7, N.1.1)
		[N.2] Inundación	• N.2.1 Sistema de climatización sin mantenimiento. • N.2.2 Mala disposición de tuberías en pisos superiores.		• A.18.2.2 Cumplimiento en las políticas y normas de seguridad(A.7)
		[N.*] Desastres naturales	• N.3.1 Diseño antisísmico no adecuado.		• A.6.1.3 Contacto con
		[I.3] Contaminación mecánica	• I.3.1 Mala disposición y almacenamiento de documentos. • I.3.2 Control de perímetro de acceso incierto.		• A.11.1.4 Protección contra amenazas externas y ambientales (N.1.1, N.1.3, N.2, N.*,A.26, I.3, I.7)
		[A.18] Destrucción de información	A.18.1 Ausencia de etiquetado (clasificación) de la informació		• A.11.2.9 Política de pantalla y escritorio limpio (N.1.2)
		[I.7] Condiciones inadecuadas de temperatura o humedad	I.7.1 Sitios de almacenamiento desprotegidos		• A.17.1.1 Planificación de la continuidad de la seguridad de la información (A.7, I.9)
		[I.9] Interrupción de otros servicios y suministros esenciales	I.9 No disponibilidad de recursos de los cuales depende la operación, como papel o tóner.		• A.18.1.3 Protección de registros (A.7)
		[A.7] Manipulación de documentación.	• A.7.1 Deficiente manejo de información clasificada • A7.2 Mala difusión de políticas de seguridad. • A.7.3 Documentación con fallas estructurales no acordes a la organización		• A.5.1.1 Políticas para la seguridad de la información (A.7, I.9, A.18)

HARDWARE	Equipos medios	[N.1] Incendio	• N.1.1 Escaso equipo contra incendios. • N.1.2 Mala política de escritorio limpio. • N.1.3 No cumplimiento de reglamento interno en lo que se refiere a normas de buena conducta. • N.1.4 Fallo en revisión de conexiones eléctricas	Reducción	• A.6.1.3 Contacto con autoridades **(N.1.1)**
		[N.2] Inundación	• N.2.1 Sistema de climatización sin mantenimiento. • N.2.2 Mala disposición de tuberías de pisos superiores		• A.9.1.1 Política de control de acceso **(N1.1)**
		[N.*] Desastres naturales	• N.3.1 Diseño antisísmico no adecuado.		• A.11.1.4 Protección contra amenazas externas y ambientales **(N.1.1, N.1.3, N.2.1, N.2.2, I.6.1,I.7.1,N.3)**
		[I.7] Condiciones inadecuadas de temperatura o humedad	• I.7.1 Deficiencia en la climatización		• A.11.2.1 Instalación y protección de equipos **(I.6.1,I.7.1)**
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	• E.23.1 Desconocimiento de procedimientos o controles de actualización de equipos.		• A.11.2.9 Política de pantalla y escritorio limpio **(N.1.2)**
		[I.6] Corte del suministro eléctrico	• I.6.1 Falla en mantenimiento de UPS.		• A.11.2.3 Seguridad del cableado **(N.1.4)**
		[E.2] Errores del administrador	E.2.1 Desconocimiento en instalación de equipar		• A.11.2.4 Mantenimiento de equipos **(I.6.1, E.23.1, E.2.1, I.5.1, A.23.2)**
		[A.7] Uso no previsto	• A.7.1 Perfiles de seguridad no establecidos		• A.11.2.8 Equipos de usuario desatendido**(A.23.2)**
		[A.23] Manipulación de los equipos	• A.23.1 Sabotaje de hardware por falla en políticas de administración de equipos. • A.23.2 Mala administración de mantenimiento de equipos. • A.23.2 Overflow por falta de verificación de capacidades del equipo	Reducción	• A.8.1.2 Propiedad de los activos**(A.23.1)**
		[I.5] Avería de origen físico o lógico	• I.5.1 Fallos en los equipos por defecto de origen		• A.8.1.3 Uso aceptable de
		[E.15] Alteración accidental de la información	• E.15.1 Alteración accidental de datos sobre todo en los recabados por dispositivos tales como: Tablets o cámaras		• A.9.1.1 Política de control de acceso**(A.7.1)**
		[E.18] Pérdida accidental de la información	• E.18.1 Pérdida accidental de información sobre todo en dispositivos tales como: Tablets o cámaras.		• A.8.1.1 Inventario de equipos**(E.25.1)**
		[E.25] Pérdida de equipos	• E.25.1 Insuficiente control de manejo de inventarios		
SERVICIOS	Entrega de Productos a Clientes	[N.1] Incendio	• N.1.1 Escaso equipo contra incendios. • N.1.2 Mala política de escritorio limpio • N.1.3 Fallo en revisión de conexiones eléctricas	Reducción	• A.6.1.3 Contacto con autoridades (E.28.2) • A.11.1.4 Protección contra amenazas externas y ambientales(E.28.2) • A.6.1.2 Separación de deberes (E.28.1)• A.13.2.4 Acuerdos de confidencialidad y no divulgación(A.30.3) • A.16.2.2 Cumplimiento en las políticas y normas de seguridad(E.7,E1,A.7,A.6) • A.7.1.2 Términos y condiciones del empleo(A.5) • A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información(A.5,A.6,A.7)
		I.*] Daño eléctrico	• I.1.1 Aumento o disminución de voltajes no controlados. • I.1.2 Sobrecarga de regletas o tomacorrientes. • I.1.3 Mala política de escritorio limpio		
		E.7] Deficiencias en la Organización	• E.7.1 Acciones no coordinadas • E.7.2 Errores por omisión • E.7.3 Roles mal definidos • E.7.4 Desconocimiento de procedimientos		
		[E.28] Indisponibilidad del personal (no intencionado)	• E.28.1 Enfermedad • E.28.2 Alteraciones en el orden publico		
		[E.1] Errores de los usuarios	• E1.1 Mala difusión de políticas de seguridad. • E1.2 Roles de seguridad no asignados o comunicados • E1.3 Empoderamiento inexistente en lo que se refiere a políticas de seguridad • E1.4 Personal con tareas rutinarias		
		[A.5] Suplantación de identidad del usuario	• A.5.1 Privilegios y accesos pobres para acceso a equipos.		
		[A.7] Uso no previsto	A.7.1 Uso de recursos del sistema para temas de interés pers		

Tratamiento de Riesgos se muestran los controles propuestos según las amenazas que se presenten como medidas de control.

Caracterización De Las Salvaguardas.[34]

Una salvaguarda es un mecanismo tecnológico que reducirá el riesgo. Hay muchos tipos de amenazas unas requieren elementos técnicos (programas o equipos), otras requieren seguridad física y/o política de personal.

Aquí se identifican las salvaguardas efectivas junto a la eficacia de ellas para mitigar el riesgo.

Existen varias etapas de estudio entre ellas:

- Primera etapa : POTENCIAL
- Segunda etapa SITUACION ACTUAL
- Tercera etapa : OBJETIVO

Las cuales constan de las siguientes subtareas:

- Identificación de las salvaguardas pertinentes
- Valoración de las salvaguardas.

Identificación De Las Salvaguardas

Su principal objetivo es utilizar la salvaguarda conveniente para proteger el sistema, para que reduzca y evite el riesgo.

Las Estrategias que adopta la salvaguarda frente al incidente serán:

- CR: Correctivas (gestión de incidentes)
- IM: Minimizar impacto (Desconexión de equipos)
- RC: Recuperación del incidente (Copias de seguridad)
- DT: Detección (Detectores de incendios)
- MN: Monitorización (Registros de actividad)
- EL: Eliminación (Eliminar cuentas de empleados que ya no están)
- PR: Preventiva (autorización previa de usuarios)
- DR: Disuasoria (Vallas, guardias de seguridad)
- AD: Administrativas (Inventario de Activos)

- AW: Concienciación (Cursos de concientización)
- STD: Basada en Normas
- PROC: Basadas en procedimientos
- CERT: Basadas en productos certificados(Firewalls)

A continuación, la figura 3.35 muestra los tipos de Salvaguardas en MAGERIT utilizados en aplicativo PILAR

EFECTO	TIPO
Preventivas: Reducen la probabilidad	[PR] preventivas. [DR] disuasorias. [EL] eliminatorias.
Acortan la degradación	[IM] Minimizadoras. [CR] correctivas. [RC] recuperativas.
Consolidan el efecto de las demás.	[MN] de monitorización. [DC] de detección. [AW] de concienciación. [AD] administrativas.

Figura 3. 35 Tipos de Salvaguardas – Magerit Libro I

Valoración De Salvaguardas

Determinar la eficacia de las salvaguardas pertinentes.

El objetivo de estas tareas es conocer que se necesita para proteger el sistema y de esa manera mantener protegido al sistema según las necesidades de la empresa.

La salvaguarda frente a una situación de interrupción de servicio se caracteriza por un tiempo de reacción, es decir lo que se demore en restablecer el servicio.

Si se califica la eficacia de una salvaguarda se refiere al tiempo de respuesta garantizada.

Ese grado de eficacia se lo puede comparar con la degradación, puesto que una salvaguarda no puede empeorar la situación de un activo en presencia de una amenaza.

La eficacia de la salvaguarda reducirá el riesgo en base al grado de eficacia del activo que esté protegiendo.

Además, las salvaguardas se caracterizan más que por su existencia, por su eficacia frente al riesgo que pretenden controlar. Entre una eficacia del 0% para aquellas que faltan y el 100% para aquellas que son idóneas y que están perfectamente implantadas, se estimará un grado de eficacia real en cada caso concreto.

PILAR contempla Salvaguardas y grupos de salvaguardas para el estudio realizado en la empresa FELMOVA S.A.

En la figura 3.36 en la ventana de riesgo repercutido se presiona el botón gestionar

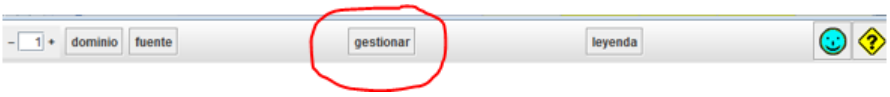


Figura 3. 36 Riesgo Repercutido

y muestra la eficacia de las salvaguardas Figura 3.37.

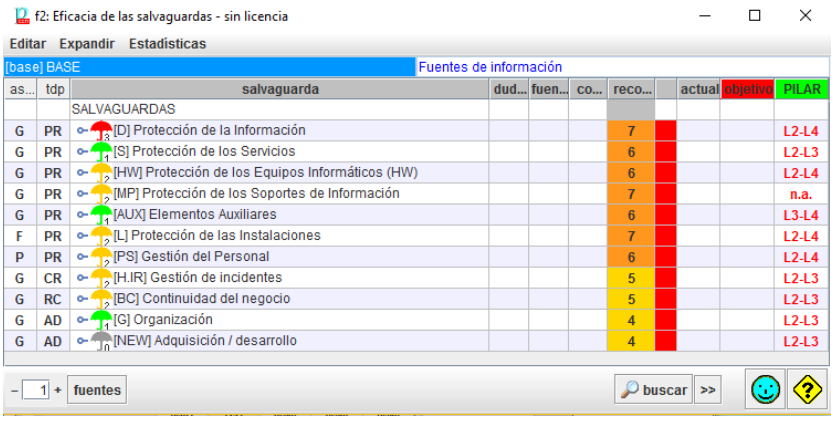


Figura 3. 37 Salvaguardas en PILAR empresa FELMOVA

En donde las salvaguardas(controles) y grupos de salvaguardas se las identifica por un ícono en forma de paraguas y un subíndice.

- 0: Interesante.
- 1: Importante. Tiene un peso mayor que una salvaguarda gris.
- 2: Muy importante. Tiene un peso mayor que una salvaguarda verde.
- 3: Crítica. Tiene un peso mayor que una salvaguarda amarilla.

El peso de las salvaguardas los aplica el programa PILAR a la hora de calcular

- El impacto y riesgo residuales (*ya vistos en punto – pag 58)*
- El valor de la recomendación

En el Panel de control en la parte superior izquierda están las columnas de **Aspecto** y **Estrategia.**

- **Aspecto**: Indica el aspecto de seguridad en el que protege la salvaguarda. El aspecto de la salvaguarda está relacionado con la clase de los activos cuyas amenazas mitigará.

  Los valores posibles son:

  - G: Gestión.
  - T: Técnico.
  - P: Personal.
  - F: Seguridad física.

  Se trata de un valor informativo (no se puede editar).

- **Estrategia**: Indica la estrategia que adopta la salvaguarda ante los incidentes para mitigar las amenazas.

Los valores posibles son:

o RI: Reduce o limita el impacto de las amenazas.

o RF: Reduce la frecuencia en que se materializan la amenazas.

o M: Mixta (RI + RF)

o D: Detecta el incidente para provocar una rápida reacción.

o R: Medida de recuperación tras incidentes.

Eficacia De Las Salvaguardas [1]

Es la medida de cuán eficaz es una salvaguarda y que pueden ser perfectas y eficaces al 100%. En la práctica, la eficacia es menor:

- Porque la salvaguarda no está completamente desplegada
- Porque la salvaguarda no está completamente operacional
- Porque la salvaguarda no está perfectamente gestionada

La eficacia de las salvaguardas se utiliza para estimar el impacto y el riesgo residuales sobre los activos.

La eficacia de las salvaguardas se mide en términos de madurez.

Cuando los niveles de madurez se traducen a porcentajes de la eficacia, PILAR utiliza lo que muestra la figura 3.38 :

nivel	significado	eficacia
L0	inexistente	0%
L1	inicial / ad hoc	10%
L2	reproducible pero intuitivo	50%
L3	proceso definido	90%
L4	gestionado y medible	95%
L5	optimizado	100%

Figura 3. 38 Porcentajes de la Eficacia PILAR

Valor seleccionable (nivel de madurez)	Valor mostrado	Significado
No es aplicable	n.a.	La salvaguarda no tiene sentido en el sistema.
¿...?	?	Desconoce cuál es el nivel de madurez, pero va a consultarlo y a introducirlo más tarde.
[Vacío]		Desconoce cuál es el nivel de madurez, y no va a consultarlo porque no es relevante.
0 - Inexistente	L0	*Procedimiento:* No se realiza. *Elemento:* No se tiene. *Documento:* No se tiene.
1 - Inicial / ad hoc	L1	*Procedimiento:* Se está empezando a hacer, o sólo lo hacen algunas personas. *Elemento:* Se tiene, pero no se usa apenas. *Documento:* Se está preparando su elaboración.
2 - Reproducible, pero intuitivo	L2	*Procedimiento:* Todos lo hacen igual, pero no está documentado. *Elemento:* Se tiene, pero se está terminando de afinar. *Documento:* Se está elaborando.
3 - Proceso definido	L3	*Procedimiento:* Todos lo hacen igual y está documentado. *Elemento:* Se tiene y funciona correctamente. *Documento:* Se tiene.
4 - Gestionado y medible	L4	*Procedimiento / Elemento / Documento:* Se obtienen indicadores.
5 - Optimizado	L5	*Procedimiento / Elemento / Documento:* Se revisa el mismo y los indicadores, se proponen mejoras y se aplican.

Figura 3. 39 Eficacia de las Salvaguardas – Niveles de Madurez

Tipos de protección en salvaguardas - Magerit

— PR – prevención	— AD – administrativa	— DR – disuasión	— EL – eliminación
— IM minimización del impacto	— CR – corrección	— RC – recuperación	— AW – concienciación
— DC – detección	— MN – monitorización	— std – norma	— proc – procedimiento
— cert – certificación o acreditación			

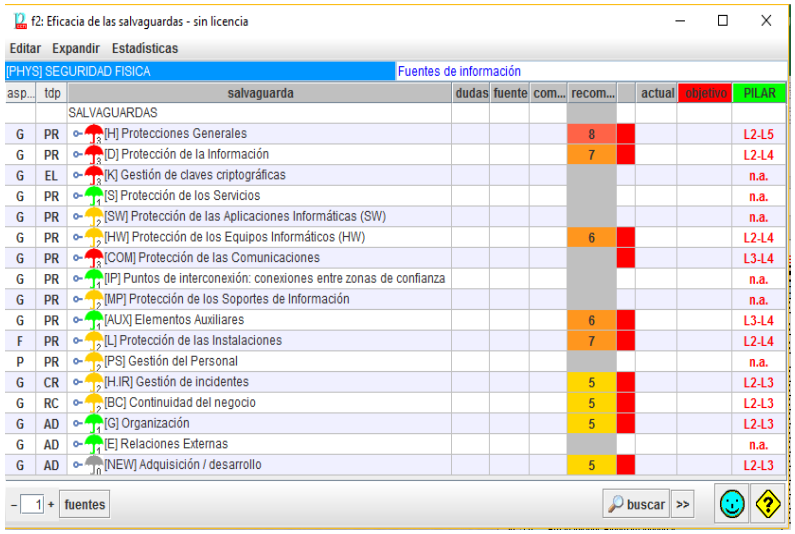


Figura 3. 40 Eficacia de las Salvaguardas

Pero aplicando las salvaguardas sugeridas en PILAR en el impacto Acumulado se muestra en la Figura 3.41:

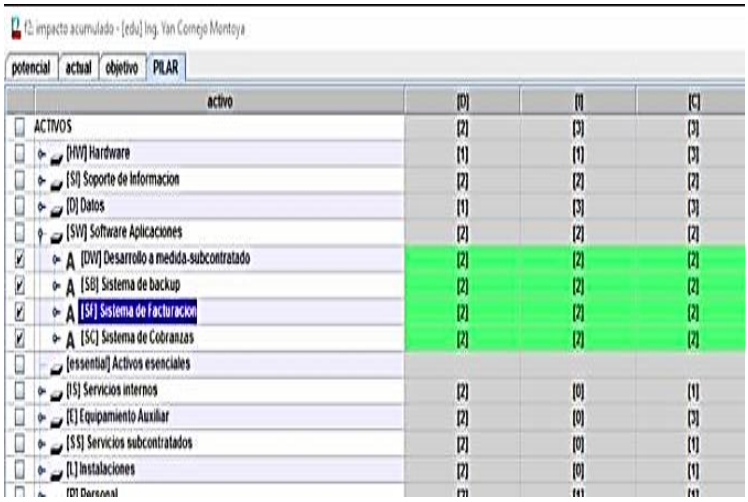


Figura 3. 41 Impacto acumulado aplicando salvaguardas

Se logra minimizar su impacto como se aprecia en los colores según la tabla.

Ejemplo: Recomendación de Controles

Demostración de reporte de PILAR sobre clases de activos con sus posibles amenazas expuestas.

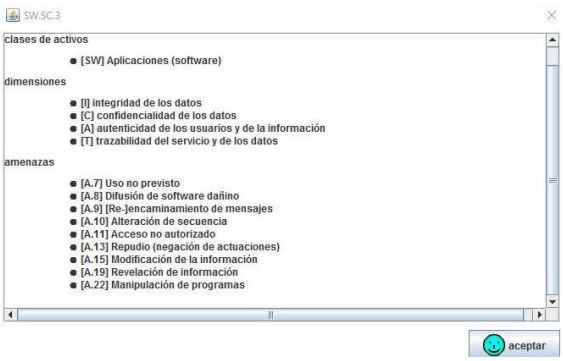


Figura 3. 42 Clases de activos versus posibles amenazas expuestas

MAGERIT destaca que las técnicas en salvaguardas van a variar con los continuos cambios tecnológicos debido a ciertas situaciones como:

- Aparición de nuevas tecnologías
- Cambios en los activos a considerar
- Evolución en probabilidades de atacantes

Por lo que como consecuencia el catálogo de salvaguardas se debería ajustar a quienes participan en la organización, a fin de que sus resultados sirvan de apoyo y que cumplan la función de mitigación y prevención de riesgo.

En la evaluación de riesgos se va a implantar controles o salvaguardas con la finalidad de reducir el riesgo.

Las salvaguardas pueden tener vulnerabilidades, por lo que se necesitan hacer pruebas y seguimiento a las mismas. La seguridad absoluta no existe, por ello hay que aceptar el manejo de riesgos.

Hay que considerar que las salvaguardas son medidas de mitigación que debe tener conocimiento la alta gerencia para que tome medidas de prevención, pero no son obligatorias y se puede

optar por un enfoque de mitigación acorde a los resultados obtenidos.

Responsabilidades

Tabla 17 Tabla de Responsabilidades

Áreas	Rol	Responsabilidades
Facturación	Asistente	✓ Llevar un control y seguimiento de las facturas emitidas. ✓ Cumplir con la emisión de facturas conforme a despacho de productos salidos de bodega. ✓ Notificar los riesgos que pueden llegar a amenazar la continuidad de la operación. ✓ Trabajar en conjunto con la Gerencia General para clarificar los riesgos del negocio y diseñar planes de acción. ✓ Presentar a la Gerencia General un reporte mensual de los productos facturados para determinar las estrategias más convenientes y medidas apropiadas ✓ Cumplir con las políticas de seguridad de la empresa.
Ventas	Asistente	✓ Revisar y coordinar el funcionamiento del Área de Ventas ✓ Trabajar en conjunto con la Gerencia General para clarificar los riesgos del negocio y diseñar planes de acción al momento de no cumplir con las metas planificadas en la fuerza de ventas. ✓ Supervisar el trabajo del equipo. ✓ Coordinar la renovación de clientes. ✓ Reportar las faltas o errores en cuanto a responsabilidades de la fuerza de ventas.

		✓ Cumplir con las políticas de seguridad de la empresa.
Cobranzas	Asistente	✓ Cumplir con el funcionamiento del Área de Cobranzas ✓ Trabajar en conjunto con la Gerencia General para clarificar los riesgos del negocio y diseñar planes de acción al momento de caer en mora un cliente. ✓ Cumplir con las políticas de seguridad de la empresa.
Contabilidad	Asistente	✓ Cumplir con el funcionamiento del Área de Contabilidad ✓ Cumplir con las emisiones de Roles de Pago a empleados ✓ Cumplir con las declaraciones al SRI ✓ Revisar y generar los contratos a empleados ✓ Revisar y gestionar las liquidaciones en caso de salida de empleados ✓ Revisar y gestionar lo referente a cuentas bancarias para los pagos y cobros en general.
Inventario	Asistente	✓ Cumplir con el funcionamiento del Área de Inventario ✓ Revisar en forma permanente el inventario cada día en forma f;isica y l;ógica según cronograma planificado por determinada línea de producto.
Caja	Asistente	✓ Trabajar en conjunto con la Gerencia General para clarificar los riesgos del negocio y diseñar planes de acción. ✓ Cumplir con las políticas de seguridad de la empresa.
Bodega	Jefe	✓ Coordina la logística de entrega y recepción de mercadería. ✓ Trabajar en coordinación con Facturación Para llevar un control y seguimiento de los despachos de productos. ✓ Revisar y coordinar el funcionamiento del Área de Bodega. ✓ Controlar el funcionamiento del Área de Bodega

		✓ Trabajar en conjunto con la Gerencia General para clarificar los riesgos que puedan presentarse en almacenado y despacho de productos. ✓ Presentar a la Gerencia General un reporte mensual de los productos por caducar a fin de determinar las estrategias más convenientes medidas apropiadas. ✓ Supervisar el trabajo del equipo. ✓ Cumplir con las políticas de seguridad de la empresa. ✓ Reportar las faltas o errores en cuanto a responsabilidades de quienes conforman el área de Bodega.
Personal	Gerente General	✓ Planear, Organizar, Dirigir y Controlar, el funcionamiento del Área de Contratación. ✓ Planear, Organizar, Dirigir y Delegar el funcionamiento del Área de Bodega. ✓ Planear, Organizar, Dirigir, y Delegar el funcionamiento del Área de Facturación ✓ Planear, Organizar, Dirigir, Controlar y Delegar el funcionamiento del Área de Caja. ✓ Planear, Organizar, Dirigir, Controlar y Delegar el funcionamiento del Área de Ventas. ✓ Planear, Organizar, Dirigir, Controlar y Delegar el funcionamiento del Área de Cobranzas. ✓ Proponer políticas y procedimientos para la Gestión Integral de Riesgos. ✓ Coordinar la atención y resolución de problemas y requerimientos ✓ Evaluar e identificar los riesgos informáticos que pueden llegar a amenazar la continuidad del negocio. ✓ Garantizar la disponibilidad de los sistemas.

		✓ Implementar procedimientos para la recuperación del sistema en caso de fallos. ✓ Diseñar el DRP de acuerdo a los riesgos que se encuentra expuesto el negocio. ✓ Alinear la estrategia de tecnologías de la información con las del negocio. ✓ Promover entre su equipo de trabajo buenas prácticas en materia de gestión de documentos y archivos. ✓ Desarrollar controles apropiados para dar soporte a la continuidad del negocio. ✓ Monitorear el cumplimiento o cometimiento de faltas o errores en cuanto a responsabilidades de los empleados. ✓ Verificar los datos suministrados por los clientes y que estos sean actualizados de forma periódica a medida que sean requeridos al momento de solicitar crédito en mercadería ✓ Difundir las políticas de seguridad de la empresa. ✓ Cumplir con las políticas de seguridad de la empresa. ✓ Difundir las políticas y delineamientos establecidos para la continuidad del negocio. ✓ Cumplir con las políticas y delineamientos establecidos para la continuidad del negocio. ✓ Monitorear el trabajo del equipo. ✓ Definir y dirigir la estrategia comercial. ✓ Analizar y desarrollar esquemas de mercado de ingreso de nuevos productos y servicios a ser ofertados a los clientes. ✓ Coordinar la renovación de clientes. ✓ Definir procedimientos y métodos para la correcta

		✓ administración del riesgo operativo.

Los empleados y personal perteneciente a la empresa FELMOVA que tengan responsabilidades sobre manejo de información y/o activos de información deben cumplir con los lineamientos indicados en la tabla anterior con el fin de mantener la confidencialidad, integridad y disponibilidad de la información.

CAPÍTULO 4

ANÁLISIS Y DISEÑO DE LOS CONTROLES DE LA SEGURIDAD FÍSICA Y DEL AMBIENTE.

4.1. Estándares De Seguridad Física

La seguridad en el ámbito informático cuesta tiempo, dinero y sobre todo esfuerzo. Es posible tener niveles mínimos de seguridad, pero el tener o lograr una protección adicional requiere gastos más considerables por lo que habría que hacer un estudio sobre la relación costo/ beneficio sobre dichas medidas que se desean implementar.

Por ello se necesitaría hacerse las siguientes preguntas:

¿Qué se quiere proteger?

Es importante determinar el valor de ciertos activos como el HW y demás tareas que se están ejecutando para la empresa, y esta valoración no es la misma para todo el personal, lo que conlleva a responder distintos valores de dichos activos.

¿Contra qué se quiere proteger?

Para no caer en gastos innecesarios, es de suma importancia determinar a qué riesgos reales estaría expuesta la organización.

Por lo que habría varios métodos como los de prevención, detección y según lo que esté dispuesta la organización sería la inversión que podría estar realizando a la organización en elegir una medida de protección.

¿Cuánto tiempo, dinero y esfuerzo se está dispuesto a invertir?

Se relaciona a lo que la organización está dispuesta a invertir.

Tiempo. Hay que dedicarle tiempo para asignar un nivel de seguridad alto, configurando los parámetros de seguridad del sistema, el ambiente de trabajo de los usuarios, revisar y fijar los permisos de acceso a los archivos, ejecutar programas de monitoreo de seguridad, revisar las bitácoras del sistema, etc.

Esfuerzo. El nivel adecuado de seguridad debe significar un esfuerzo considerable por parte del encargado, sobre todo si hay problemas de seguridad.

Dinero. Tener los medios económicos necesarios mínimos para que se pueda adquirir los productos de seguridad que se vayan a utilizar, ya sean programas o equipos.

Y lo más importantes es que es prácticamente imposible hacer que un sistema sea totalmente seguro, debido a que no se puede prever todas las posibles amenazas aun cuando la seguridad se incremente a niveles muy altos, ya que siempre habrá una manera de obtener acceso no autorizado.

La seguridad de la información es el resultado de un sistema de políticas y procedimientos designados a identificar, controlar y proteger la información y cualquier equipamiento empleado junto con su almacenamiento, transmisión y procesamiento.

Los controles de seguridad deben ser documentados, describiendo los riesgos y que controles están asociados a los mismos, además de que los cambios sobre los controles deben ser valorados, antes de que los cambios sean puestos en marcha.

Cualquier novedad de seguridad debe ser registrada y comunicada acorde a los procedimientos de la organización, para que se tomen los mecanismos necesarios para dichas situaciones.

4.2. Evaluación De Riesgos

Proceso de comparar el riesgo estimado con un criterio de riesgo dado para determinar la importancia del riesgo.[35]

Se relaciona con identificar las amenazas, vulnerabilidades y riesgos a los que están expuestos los equipos, sobre el entorno de trabajo y tecnológico de la organización para generar después un plan de implementación de controles que puedan asegurar un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información. [36]

Las dimensiones de valoración están dadas en base a la fuente de la amenaza, su capacidad y la naturaleza de la vulnerabilidad, y así establecer medidas preventivas que puedan aplicarse, así como también, es necesario identificar los riegos en todas las instalaciones de la empresa realizando una evaluación de éstos en función de las consecuencias e impacto que puedan ocasionar.

La evaluación de los riesgos de seguridad debería:

- ser realizada con una periodicidad acordada;

- ser registrada;
- ser mantenida durante los cambios (cambios de necesidades del negocio, de procesos o de configuraciones)
- ayudar a entender qué podría impactar uno de los servicios gestionados;
- proveer de información para las decisiones referentes a los tipos de controles a establecer.

Al realizar la evaluación de riesgos en forma regular como son: los cambios en la organización, tecnología, procesos y objetivos de negocio, posibles amenazas, eficacia de controles en el entorno organizacional y que puedan tener influencia en riesgos evaluados, riesgos residuales y riesgos aceptados.

A continuación, se muestran porcentajes de afectación de impactos en la empresa FELMOVA S.A. si llegase a materializarse alguna amenaza.

Tabla 18 Porcentajes de Afectación por Impactos

Impactos	
Pérdida de productividad de los empleados	23
Alteración-Fuga de información	14
Daño - Pérdida de activos	17
Interrupción del servicio	25
Información para la toma de decisiones inoport	21
	100

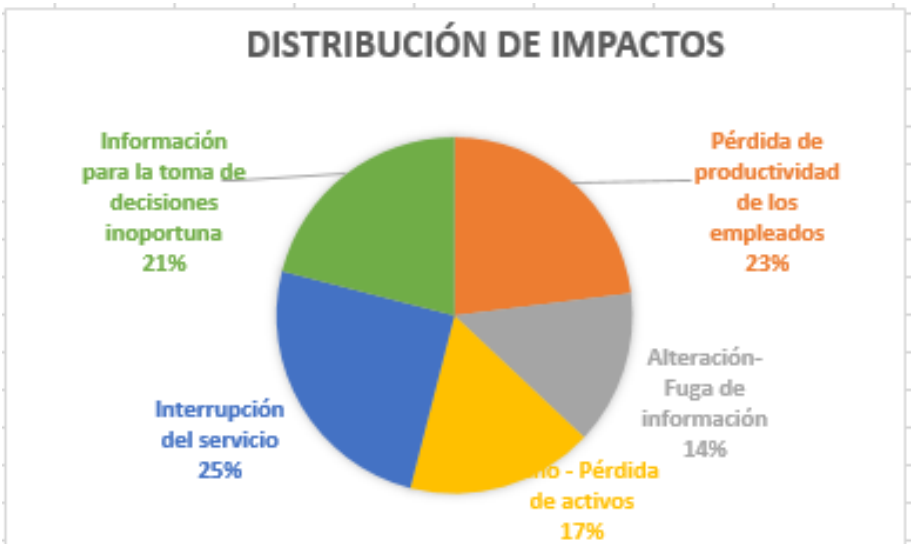
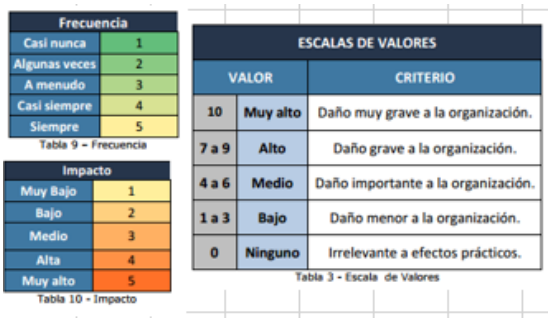


Figura 4. 1 Distribución de Impactos

Estos valores de porcentajes se los obtuvo a partir de calificaciones obtenidas con aplicativo PILAR conforme, a los activos de información ya determinados en el capítulo 3.



Frecuencia	
Casi nunca	1
Algunas veces	2
A menudo	3
Casi siempre	4
Siempre	5

Tabla 9 – Frecuencia

Impacto	
Muy Bajo	1
Bajo	2
Medio	3
Alta	4
Muy alto	5

Tabla 10 - Impacto

ESCALAS DE VALORES		
VALOR		CRITERIO
10	Muy alto	Daño muy grave a la organización.
7 a 9	Alto	Daño grave a la organización.
4 a 6	Medio	Daño importante a la organización.
1 a 3	Bajo	Daño menor a la organización.
0	Ninguno	Irrelevante a efectos prácticos.

Tabla 3 - Escala de Valores

Figura 4. 2 Escalas, Frecuencias e Impactos que aplica Magerit

Tabla 19 Valoración por capas de amenazas, Frecuencias, Impacto y Valor Riesgo .Fuente : Autor

Capa-Activo	Amenaza	Frecuencia	Impacto	Valor de Riesgo
Hardware	Incendio	1	3	3
	Inundaciones	1	4	4
	Desastres Naturales	2	5	10
	Contaminación mecánica	2	3	6
	Corte de Suministro elétrico	2	2	4
	Condiciones inadecuadas de temperatura y/o humedad	2	3	6
	Errores de Mantenimiento/ Actualización de equipos - HW	2	3	6
	Robo	2	5	10
Datos	Incendio	1	5	5
	Inundaciones	1	5	5
	Desastres Naturales	2	2	4
	Contaminación mecánica	1	3	3
	Corte de Suministro eléctrico	2	3	6
	Condiciones inadecuadas de temperatura y/o humedad	2	3	6
	Errores de Mantenimiento/ Actualización de equipos - HW	2	4	8
	Robo	2	5	10
	Alteración de la información	1	3	3
	Abuso de privilegios	1	4	4
	Ingreso de información incorrecta	3	3	9
	Degradación de los soportes de almacenamiento de inform	2	3	6
	Divulgación de la información	2	3	6
	Errores de usuarios	2	3	6
	Ingeniería Social	2	3	6
	Destrucción de la información	1	3	3
Aplicaciones / SW	Errores de l Administrador	1	3	3
	Errores de usuarios	2	3	6
	Errores de monitorización - log	2	2	4
	Ingreso de información incorrecta	2	1	2
	Errores de Mantenimiento/ Actualización de equipos - HW	2	3	6
	Caída del sistema por agotamiento de recursos	1	4	4
	Denegación de servicio	1	3	3
	Errores de configuración	1	3	3
	Deficiencias en la organización	1	3	3
	Difusión de Software dañino	1	4	4
	Alteración de la información	2	4	8
	Introducción de información incorrecta	2	4	8
	Degradación de la información	2	4	8
	Destrucción de la información	1	4	4
	Divulgación de información	2	4	8
	Vulnerabilidades de los programas- Sw	2	4	8
	Errores de mantenimiento- actualización de programas	1	4	4
	Caída del sistema por agotamiento de recursos	1	3	3
	Indisponibilidad de personal	2	3	6
	Errores de mantenimiento	2	3	6
	Suplantación de identidad	2	2	4

En donde se puede apreciar que el mayor riesgo que se ve afectado por capa de activo como se indica a continuación:

Capa HW: Desastres Natuales y Robo con un valor de riesgo de 10

Capa Datos : Ingreso de información incorrecta = 9 y Robo con un valor de riesgo de 10

Capa SW : alteración de Información, Divulgación de Información, Degradación de la información, Vulnerabilidades de los programas con un valor de 8.

Con base a los resultados ya obtenidos en el análisis de riesgos se toman en cuenta las siguientes consideraciones:

- Para cada activo, si el nivel de riesgo es aceptable, el proceso concluye
- Caso contrario se define una estrategia de tratamiento (evitar, transferir o mitigar)
- Luego se establecen controles o salvaguardas, pero no garantiza que el nivel de riesgo sea el mínimo.
- Si es mitigación, los controles pueden ser preventivos o correctivos.

4.3. Determinación De Controles

La norma es una recopilación de las mejores recomendaciones en la práctica de la seguridad de la información, sin embargo, de ser requerida la implementación de un control no incluido, la norma lo

permite, ya que no todos los controles y lineamientos son aplicables para todas las organizaciones. El desarrollo y adopción de un nuevo control, debe ser adecuadamente documentado de forma que facilite una futura revisión y comprensión por parte de los auditores, directivos, miembros y socios comerciales de la organización.

Tomando en cuenta, el tamaño de la empresa a la cual se dirige el presente estudio, no se pretende que invierta en la obtención de una certificación internacional ISO 27001, que representa una inversión económica considerable, sino desarrollar una guía para que incluyan las mejores prácticas recomendadas por la norma NTE INEN ISO/IEC 27002 y que sean aplicables a su realidad, la cual contiene un anexo que resume los dominios de control de la norma ISO 27002:2013[7],las cuales están desglosadas al detalle en el anexo 1:

- Política de Seguridad
- Organización de seguridad de la información
- Seguridad de los Recursos Humanos
- Gestión de los Activos
- Control de Accesos
- Cifrado
- Seguridad Física y Ambiental
- Operaciones de Seguridad

- Seguridad de las Comunicaciones:
- Adquisición de sistemas, desarrollo y mantenimiento:
- Relaciones con los Proveedores
- Gestión de Incidencias
- Seguridad de la Información para la Gestión de la Continuidad del Negocio
- Cumplimiento

ACTIVO	RIESGO	SEGURIDAD C	D	I	CONTROLES
Portátil	Propagación de virus en la red			X	Configuración de acceso limitado a redes
					Monitoreo de puertos

ACTIVO	RIESGO	SEGURIDAD C	D	I	CONTROLES
Portátiles y/o Computadoras	Robo equipo	X	X	X	Adquirir póliza contra robo de equipos
					Restringir la salida de equipos de las instalaciones
					Mejorar los niveles de seguridad en las instalaciones
	Robo información	X	X		Encriptar información en los discos duros de los equipos
					Respaldar información automática en servidores
					Implementar contraseña de arranque en la BIOS de los equipos
					Implementar contraseña de inicio de sesión en los equipos
	Infiltración de Virus	X	X	X	Adquirir antivirus con licenciamiento empresarial
					Mantener antivirus actualizado en los equipos
					Tener antivirus activo en todos los equipos
					Bloquear panel de configuración de antivirus para usuarios finales
	Perdida de información por error de Hardware		X	X	Respaldar información automática en servidores
					Adquirir equipos de cómputo de alta calidad con perfil empresarial
					Realizar pruebas de esfuerzo en los equipos de cómputo antes de hacer renovación tecnológica
					Hacer renovación tecnología con un mínimo de 3 años
					Realizar mantenimiento preventivo en los equipos al menos 2 veces al año en equipos de escritorio
					Realizar mantenimiento preventivo en los equipos al menos 6 veces al año en equipos móviles
	Perdida de información por error de Usuario	X	X	X	Respaldar información automática en servidores
					Brindar capacitaciones periódicas a los usuarios en la importación del manejo de la información

Figura 4. 3 Controles asignados por Activos de Información

En la gráfica 4.3 se detalla los controles que deben cumplir acorde a los riesgos que pueda tener un activo.

Medidas de Prevención contra el Sabotaje.

- Establecer y aplicar un eficiente sistema de identificación, registro y control de personas, paquetes y vehículos.
- Disponer de un adecuado sistema de detección de intrusos y de artefactos explosivos.
- Supervisiones constantes en las áreas de trabajo, para detectar posibles saboteadores internos.
- Elaborar y divulgar internamente los Planes de Emergencia, en caso de sabotajes.
- Mantener en lo posible registros de personas con antecedentes de actividades subversivas o de sabotaje, coordinar con los Organismos de Seguridad del Estado.
- Llevar un control de los Empleados y Obreros descontentos, ya que pueden ser saboteadores potenciales.
- Conducir Operaciones de Inteligencia para detectar posibles Planes de Sabotaje de personas contrarias
  (Enemigos, Competencia Empresarial, entre otros).

- Entre otros.

4.4. Plan De Implementación.

Al finalizar el Plan de Implementación de los controles bajo la guía de la norma ISO/IEC 27002:2013, se obtendrán los siguientes resultados:

- Ordenar las actividades de la organización a través de un Sistema de gestión.
- Alcanzar los objetivos propuestos.
- Contar con una política de seguridad de la información, que permita alinear las normas y procedimientos definidos en la organización.
- Identificar y administrar de forma eficiente los riesgos encontrados en la organización y mitigarlos de forma adecuada antes de que se conviertan en un problema mayor.
- Concientizar al personal con la implementación de un Plan de Divulgación de las Políticas de Seguridad y.
- Lograr que el personal de la empresa reporte incidentes de seguridad, con el fin de prevenir eventos que puedan afectar la continuidad del negocio.

A continuación, se propone un cronograma como propuesta de implementación de las actividades donde a modo general se observan el tiempo y los recursos requeridos.

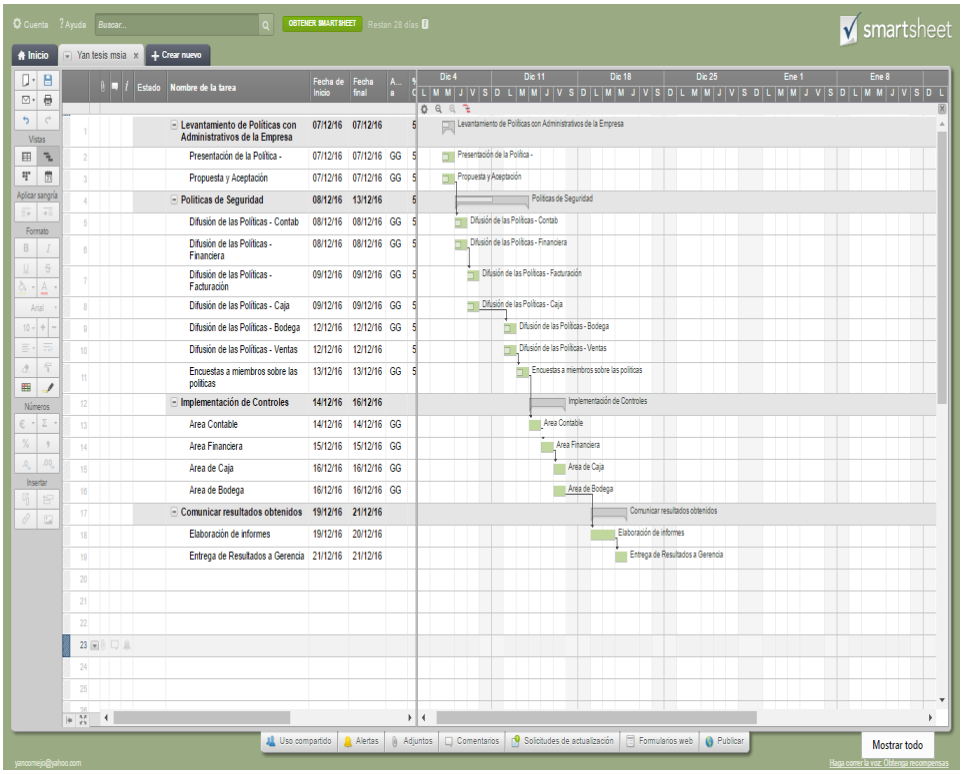


Figura 4. 4 Cronograma de actividades realizadas en la implementación

CAPÍTULO 5

IMPLEMENTACIÓN DE LA SEGURIDAD FÍSICA Y AMBIENTAL

5.1. Factores Físicos

Son todos aquellos factores ambientales que dependen de las propiedades físicas de los cuerpos tales como:

- Ruido
- Temperaturas Extremas
- Ventilación
- Iluminación
- Presión
- Radiación
- Vibración

Así como también:

- Incendios
- Inundaciones
- Sismos
- Humedad

Incendios. Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones inalámbricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

Inundaciones. Es la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en centros de cómputo.

Sismos. Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan, o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas.

Humedad. Se debe proveer de un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de computadoras y al área de máquinas en forma exclusiva**.**

Que actúan sobre el trabajador y que pueden producir efectos nocivos, de acuerdo con la intensidad y tiempo de exposición [37]

5.2. Factores Humanos.

Las personas representan el eslabón más débil dentro de la seguridad informática y la base fundamental en el proceso de seguridad, a diferencia de las computadoras, las personas pueden no seguir las instrucciones tal y como fueron dictadas, por lo que la seguridad informática debería ser el factor más importante.[38] .

El factor humano es la base fundamental los procesos de control de ingreso a instalaciones, es el resultado de la experiencia profesional donde intervienen: la capacitación, disciplina y compromiso de las personas e instituciones que brindan este servicio.

Estudios realizados por RSA en la División de Seguridad de la empresa EMC, entre trabajadores del sector público y privado en Boston, Washington D.C. y Buenos Aires indican los siguientes porcentajes

El 56% de empleados han ingresado a su trabajo sin presentar tarjeta de acceso en más de una oportunidad.

El 85% de trabajadores facilitó el acceso a alguien que no conocían a sus oficinas.

Lo que indica un cambio de cultura en actitudes y conductas de seguridad de acceso a sus empresas.

Los resultados de estas encuestas señalan el riesgo de manejo de datos de empleados, proveedores, socios externos, consultores y visitantes que tuvieron acceso físico y/o lógico a los datos de la empresa.

Además de que el 75% de problemas relacionados a la seguridad se debe a : fallos en la configuración de los equipos o un mal uso de parte del personal de la empresa.

La organización puede ser responsable solidario (dependiendo de la legislación) de los actos de sus empleados lo que les puede acarrear sanciones económicas.

Ejemplo:[39]

- Envíos de comunicaciones comerciales no solicitadas (spam).
- Cesiones no autorizadas de datos de carácter personal
- Delitos contra la propiedad intelectual
- Responsabilidad por la comisión de delitos informáticos ej. intrusiones
- Descarga de herramientas de hacking, acceso a pornografía o contenidos tipificados como ilegales en el país
- Envíos a terceros de información confidencial de la empresa o de sus posibles clientes y proveedores.

A continuación, se menciona los posibles actos que pueden ser cometidos por el factor Humano:

- Robos
- Actos vandálicos
- Fraude
- Sabotaje
- Terrorismo[40]

Por lo que se sugiere que, al implantar un sistema de gestión de la seguridad de la información, se debe considerar el factor humano como un elemento clave, donde se incluya una formación y sensibilización a los empleados, la aprobación de reglamentos internos, compromiso de la alta Dirección, para que exista un adecuado manejo de sus sistemas y servicios informáticos, así como asegurar la seguridad de la información.

Recomendaciones

✓ ¿Cómo implementar buenas prácticas?

- Diferencias entre el “qué se debe hacer” y el “cómo se hace”
- Establecer acuerdos

✓ El rol de las personas

- Actitudes
- Aptitudes

- ✓ Los ámbitos
    - Predisponen (para bien o para mal)
    - Relacionan y mezclan niveles
    - Que sean armónicos y no disonantes
- ✓ Los procesos
    - Procedimientos
- ✓ Las relaciones entre los procesos
- ✓ La implementación.

5.3. Definición De Políticas Y Procedimientos

Políticas De Seguridad:

Una política de Seguridad es una técnica referente a cómo se gestionan a los activos de información, acerca de cómo protegerlos adecuadamente informando que está permitido y que no, socializando la responsabilidad de protección de los recursos que deben asumir todos los que integran a la organización.

Con la difusión del Manual de Políticas de Seguridad de la información para la empresa FELMOVA S.A., se pretende lograr que los colaboradores se rijan bajo dichas normas para asegurar los bienes y recursos, para que sean utilizados de manera correcta, todo esto con el fin de que se proteja, prevenga y gestione los daños posibles a los

cuales pueda estar expuesta la empresa por vulnerabilidades que puedan existir.

Por lo que se sugiere que estas políticas sean diseñadas y elaboradas dentro de la organización en cualquier momento y que sean documentadas formalmente:

- Antes de que se produzcan ataques
- Luego de acontecido un ataque
- Para evitar problemas legales
- Antes de una auditoría
- Al iniciar una organización

Cuando Modificar Políticas De Seguridad

Las políticas de seguridad cumplen un ciclo de vida dentro de ella, por lo que son sujetas a cambios, mejoras o su eliminación.

Las causas por las que puedan ser modificadas las políticas son las siguientes:

- Cambios en la tecnología de la organización
- Implementación de nuevos proyectos de software
- Necesidades de regulación vigentes
- Requerimientos especiales de clientes o proveedores
- Cambios en la línea de negocios.

¿Qué Protección Ofrece Una Política De Seguridad?

A veces la seguridad se implementa en un momento a futuro y no se toman las debidas precauciones, debido a que se lo considera algo costoso de implementar.

Por lo que es de suma importancia reconocer la necesidad de implementar políticas de seguridad y que se cumplan dentro de la organización, lo que permitirá que se tenga un mejor control.

5.4. Clasificación General De Las Instalaciones

El primer paso consiste en establecer en términos generales si se trata de una instalación de riesgo alto, medio o bajo.[41]

Instalaciones de alto riesgo:

- Datos o programas que contienen información confidencial de interés nacional o que poseen un valor competitivo alto en el mercado.
- Pérdida financiera potencial considerable para la institución y en consecuencia una amenaza potencial alta para su subsistema.

Instalación de riesgo medio:

Son aquellas aplicaciones cuya interrupción prolongada casusa grandes inconvenientes y el posible incremento de costos, pero con muy poca pérdida material.

Instalación de bajo riesgo:

Son aquellas aplicaciones cuyo procesamiento retardado tiene poco impacto material en la organización, en término de costos o de reposición del servicio interrumpido.

5.5. Enunciado De Aplicabilidad.

Luego de identificar los controles necesarios para todos los riegos con nivel No Aceptable para la empresa FELMOVA, se deben detallar cuáles se aplican o no al entorno de la empresa. El documento en el cual se especificarán los controles que aplican para este caso se lo denomina Declaración de Aplicabilidad o SOA ver documento Anexo 2.

5.6. Difusión De La Política.

A continuación, se expone un compendio de normas para uso de la empresa FELMOVA S.A. Estos comunicados surgen como una medida correctiva ante algún incidente de la seguridad de la información.

Definición De Políticas

Las políticas de seguridad las adoptan las empresas con la posibilidad de mitigar las amenazas que pueden aparecer en cualquier proceso y así proteger el activo más importante que es la información, cumpliendo con ciertos requisitos que son la integridad, disponibilidad y confidencialidad, considerados los pilares de la seguridad informática.

La definición de estas políticas requiere de una alta responsabilidad por parte de quienes forman la organización, en este caso quienes integran FELMOVA, por lo que las mismas deben ser lo más cercanas a la realidad de la empresa. Como la empresa es relativamente pequeña, el Gerente General mantendrá bajo su responsabilidad la implementación del Manual de Políticas de Seguridad, ya que entre sus funciones se identifican las siguientes:

- Gestionar los incidentes de seguridad de la información, reportados y encontrados.
- Garantizar que se cumplan los principios básicos de seguridad como son: integridad, confidencialidad y disponibilidad de la información.
- Evaluar los recursos tecnológicos, así como plataformas necesarias.

- Gestionar y/o Aprobar los recursos para soportar requerimientos de necesidades de la empresa.

Políticas Del Negocio.

Políticas De Despacho De Mercadería

- Investigar y seleccionar el segmento de mercado a donde realizar las entregas de mercadería.
- Controlar la entrega de mercadería con la guía de remisión
- Revisión de estado de entrega del producto a la salida de bodega hasta el momento de embarcar en el carro repartidor.

Políticas De Crédito A Clientes

- Analizar la capacidad de crédito del cliente.
- Establecer calendarios de pago conforme al monto facturado.
- Realizar auditorías programadas para los seguimientos de cobros a clientes.

Políticas Generales

- Los activos que se entregan a los empleados para que realicen sus labores son propiedad de la empresa. El uso de estas herramientas, sean de hardware o de software debe estar estrictamente relacionados con el trabajo asignado.
- Cada persona está autorizada para accesar a la información relacionada a las actividades que realiza, manteniendo una adecuada segregación de funciones.

- Los accesos que otorga el Gerente General, le permite a cada empleado única y exclusivamente trabajar en las actividades conectadas para el usuario creado.
- La información de los sistemas utilizados en la empresa, deberá estar disponible para asuntos referentes al negocio.
- Debe haber una separación real de autoridad y responsabilidad para asegurar que ningún individuo tiene control exclusivo de una parte de la información.
- Las medidas que se tomen en cuanto a la seguridad deben ser identificadas e implementadas teniendo en cuenta el tipo de riesgo, definiendo la probabilidad y su impacto.
- La seguridad debe estar presente en todo momento conforme los lineamientos indicados en este proyecto.

Políticas De Acceso

- La actualización y eliminación de permisos de acceso, se realizará mediante requerimientos formales con aprobación y controles previos.
- La eliminación de derechos se efectuará con un procedimiento que indique que el contrato se da por finiquitado.
- Los perfiles de usuarios deben indicar los permisos necesarios en determinadas opciones o servicios.

- Cada proceso o actividad tendrá un responsable para su correcto funcionamiento.
- Las políticas de acceso serán revisadas por el Gerente General, para su aprobación.
- El ingreso al centro de cómputo estará limitado al personal debidamente autorizado con el uso de huellas dactilares y llaves del mismo.
- Los cambios que se necesiten realizar y que estén relacionados con el negocio, serán tramitados por el Gerente General quién es el único que otorga dicha autorización.
- Las claves que se utilicen para acceder a cualquier servicio del negocio, deben contener al menos ocho caracteres de al menos seis letras con la siguiente combinación: Una letra mayúscula, una letra minúscula, un número y un carácter especial.
- Se sugiere que las claves que se utilicen para acceder a cualquier actividad del negocio, estén encriptadas y enmascaradas.
- Control de identificación de IDS (Sistema de detección de intrusos), IPS (Sistemas de prevención de intrusos), firewalls, entre otros, para monitorear el acceso.
- No se podrá instalar software no autorizado, salvo con la respectiva autorización.

- La información sensible al negocio podrá ser actualizada o modificada de acuerdo a la asignación de permisos que se haya realizado al personal encargado y se mantendrá un log de dichos cambios.
- Se realizarán monitoreos de forma periódica de los accesos a ciertas actividades privilegiadas o intentos de acceso no autorizados.
- Se controlará que los empleados no tengan acceso a borrar o desactivar rastros de sus propias actividades.
- Se deberá aplicar la política de escritorio limpio.
- El computador debe bloquearse inmediatamente después de un tiempo de 5 minutos de no usarse.
- Debe realizarse una copia de todos los accesos de usuarios en un servidor que se designe para ello.

Políticas De Ingreso A Nivel Físico

- Todo el personal portará su respectiva tarjeta o carnet de identificación, de forma visible. En estas tarjetas debe estar anotado la política de gestión.
- El personal externo deberá portar una tarjeta de visita. En dicha tarjeta debe estar indicada la política de seguridad de la información

y mecanismo para reportar incidentes de seguridad. El personal externo deberá estar acompañado por un empleado interno.

- Al ingresar o salir de la Oficina, cada empleado de la empresa deberá registrar en el lector biométrico su ingreso o salida.
- La clave es personal, secreta e intransferible, cada persona es responsable por dicha clave.
- Los empleados de la empresa utilizarán los programas o equipos conforme a los convenios de licencia, no se podrán utilizar programas sin licencia o copias de los mismos, así como tampoco se podrá utilizar ningún programa obtenido de Internet.
- Todos los programas o equipos que se necesiten para cumplir con sus labores deberán ser solicitados por requerimiento y aprobación.
- Todo equipo que desee conectarse a la red de la compañía deberá contar con el respectivo permiso.
- Queda prohibido fumar o encender cigarros o botar colillas de cigarrillos en cualquier área que llegue a afectar equipos o programas de la compañía.
- Se prohíbe ingerir bebidas alcohólicas.
- Se debe mantener los respectivos equipos de control de fuego en caso de incendios.

Políticas De Acceso A Nivel Lógico

- Todos los equipos deben tener bloqueo de puertos USB y la unidad de DVD y su reasignación se hará previa autorización.
- Todos los equipos deberán contar con software antivirus licenciado.
- Cada mes se deberá solicitar el cambio de la contraseña de acceso al computador.

Políticas De Respaldo Y Recuperación De Información

- Las copias de respaldo de la información se realizarán en forma diaria previa necesidad requerida por el gerente general.
- Los respaldos se realizarán mediante la herramienta correspondiente y serán almacenados en una unidad de almacenamiento externo.
- Se deben realizar pruebas de restauración, al menos una vez al año.
- La clave de acceso al correo electrónico será cambiada cada 3 meses. con el correspondiente permiso y autorización del gerente general,
- No se autoriza a abrir el case del equipo. Esta actividad está reservada solo al personal autorizado por el gerente general.
- Las claves que se utilicen para acceder a cualquier servicio del negocio, deben contener al menos ocho caracteres de al menos seis letras con la siguiente combinación: Una letra mayúscula, una letra minúscula, un número y un carácter especial.

Políticas De Mantenimiento De Equipos

- Establecer, analizar y recopilar un proceso de aprobación de las solicitudes de cambio.
- Realizar un inventario de equipos donde se identifique al responsable, su nivel de riesgo, su nivel de seguridad y mitigación.
- Garantizar las medidas de seguridad adecuadas en el transporte de datos en medios físicos fuera de la empresa.
- Aprobar los cambios de configuración y la revisión de logs del Firewall.
- Identificar los recursos críticos de servicios de TI.

Garantizar el monitoreo y planificación en la revisión de capacidades del equipo.

Políticas De Uso De Software

- Los usuarios no están autorizados a instalar o intentar instalar programas, utilitarios o complementos para navegadores de internet. Esta actividad está reservada solo al personal designado por el gerente general.
- Se prohíbe el uso de programas sin licencias no autorizadas por la empresa.

Todo equipo de computación de la empresa debe mantener en forma residente un antivirus instalado y las actualizaciones de las nuevas versiones, deben realizarse en línea de forma automática.

CAPÍTULO 6

PRUEBAS DE CONTROLES

6.1. Análisis De Resultados De Pruebas

A pesar de que en la actualidad es muy conocido en todos los medios los riesgos que corren las empresas al ser blanco de ataques cibernéticos, no toman en cuenta que la inversión costo- beneficio que les daría un Sistema de Gestión de Seguridad de la Información - SGSI implantado, no es porque aumentarían sus ingresos, sino el hecho de que evitaría un posible ataque que pueda causar pérdida de sus activos en mayor o menor escala.

En la evaluación de resultados de la encuesta realizada al gerente general de la empresa, denota puntos no favorables que afectan en lo relacionado al desempeño de la empresa.

- El área de sistemas es pequeña, debido a que sus necesidades son abastecidas por personal externo.
- La empresa no cuenta con normas ISO de seguridad.
- La empresa necesita mantener acuerdos de servicios con otras empresas
- La empresa requiere establecer de un servicio de internet de respaldo.

Se adjunta cuadros comparativos de la situación inicial de la empresa y de la situación final luego de aplicarse los controles necesarios.

Tabla 20 Situación Inicial de empresa FELMOVA

PROBLEMA	POSIBLES CONSECUENCIAS
Poca difusión del buen manejo de contraseñas entre el personal de oficina, lo que implica un posible abuso de privilegios, así como una posible alteración de la información, y de una probable destrucción de la información	• Pérdida de soportes de información. • Alteración intencional de la información • Abuso de derecho

No existe antivirus legalizado para amenorar las infecciones a través de unidades portables, o descargas de archivos realizadas desde internet	• Actos fraudulentos • Ingeniería Social • Intrusiones en el sistema • Suplantación de identidad
Poco control al momento de realizar una contratación personal en Bodega	• Posible robo sistemático de productos
La auditoría de cobros a clientes no se la realiza con regularidad.	• Actos de fraude de tipo contable
No existe un plan de contingencia en cuanto a mantenimiento de hardware, es decir no hay un plan de mantenimiento físico de repuestos e insumos, lo que implicaría una posible pérdida de datos por error de hardware.	• Mal funcionamiento de equipos • Degradación de los equipos de HW • Posible pérdida de datos
No existe un plan de contingencia en cuanto a actualización de software, lo que puede ocasionar error por parte de los usuarios y poca protección por licencias desactualizadas	• Posible pérdida de datos • Información poco confiable • Infestación por virus

Tabla 21 Situación de FELMOVA luego de aplicar Controles

	APLICANDO LA NORMA ISO/IEC 27002:2013
SALVAGUARDAS O CONTROLES	DATOS
	[A.9.1.1]Politica de Control de Acceso, A.7 , N.1.1
	[A.18.2.2] Cumplimiento de las politicas y normas de seguridad
	[A.5.1.1] Politicas para la seguridad de la información A.7, I9, A.18
	SERVICIOS
	[A.11.1.4] Protección contra amenazas externas e internas
	[A.1.8.2.2] Cumplimiento en las politicas y normas de seguridad
	[A.7.2.2] Toma de conciencia, educación y formación en la seguridad de la información
	[A.7.1.2] Terminos y condiciones del empleo
	SW – APLICACIONES
	[A.9.4.1] Restricción de acceso a la información
	[A.7.1.2] Terminos y condiciones del empleo
	[A.9.4.1]Restricción de acceso a la información
	HW
	[A.9.1.1] Politica de control de acceso
	[A.1.1.2.4] Mantenimiento de equipos
	[A.1.1.2.1] Instalación y protección de equipos
	[A.1.1.1.4] Protección contra amenazas externas e internas

Descripción De Casos

Los casos que se mencionarán a continuación se refieren a situaciones que acontecen en toda empresa comercial que maneja gran volumen de mercadería. Tabla 22.

El primer caso es el cobro de valores a clientes en donde no hay un soporte de la forma de pago al momento de realizar abonos o pagos parciales.

El segundo caso es la fuga de información al momento de transportar valores desde el interior de la empresa.

Tabla 22 Detalles de Casos

	DETALLES	INTERVINIENTES
CASO 1	Cobro de Valores a clientes	• Gerente General • Supervisor de Ventas • Auditor de Cobranzas Externo • Asesora de Crédito y Cobranzas • Vendedor - Cobrador
CASO 2	Fuga de Información	• Gerente General • Chofer

CASO 1. Cobro De Valores A Clientes

El cobro de valores generados por el despacho de mercadería y que generan una emisión de factura al cliente de la empresa FELMOVA, ha generado en algunas ocasiones que ciertos vendedores que también realizan la función de cobradores retengan esos valores y no los entreguen en la empresa.

- Puede darse el caso que el vendedor no entregue el respectivo recibo de pago debido a la confianza depositada del cliente en el cobrador de la empresa FELMOVA y solo le firma la copia de la factura del cliente como referente de pago.
- Otra situación es cuando se efectúan los cobros que son todos los lunes, aprovechan a realizar el tan conocido “jineteo” es decir que cubren el faltante de facturas antiguas ya pagadas, con recaudaciones de efectivo provenientes de facturas “frescas” ya

pagadas y no son detectados sino hasta que les hace el seguimiento por parte del auditor de cobranzas externo, o puede el cliente recibir la llamada telefónica para comprobar si ya está pagada un factura o está en mora, es así como se detectan los faltantes, desvío de dinero o “robos”.

Roles que intervienen en el caso

Entre las responsabilidades de cada uno de ellos se mencionan:

Gerente General

- Controlar y promover el cumplimiento de políticas de seguridad.
- -Promover otras formas de efectuar los cobros
- Promover cultura organizacional para manejo de posibles riesgos

Supervisor de Ventas

- Trabajar en conjunto con la Gerencia General en el plan estratégico de la empresa
- -Llevar un control y seguimiento de los cobros que realizan los vendedores en la ruta asignada.
- -Asesorar y atender a clientes importantes de la empresa.

Auditor de Cobranzas Externo

- Trabajar en conjunto con la Gerencia General en el plan estratégico de la empresa por los seguimientos en el control de pagos de clientes.
- -Comprobar que los pagos realizados sean los correctos
- -Realizar los seguimientos de las cobranzas a personal nuevo y a clientes que demoran en pagos en forma frecuente.

Asesora de Crédito y Cobranzas.

- Trabajar en conjunto con la Gerencia General en el plan estratégico de la empresa.
- Cumplir con las políticas de seguridad de la empresa
- Comprobar que los pagos realizados sean los correctos

Vendedor – Cobrador.

- Cumplir con las políticas de seguridad de la empresa
- Realizar las rutas de ventas y cobros ya programadas
- Cumplir con las metas ya establecidas para los cupos asignados.
- Comprobar que los pagos realizados sean los correctos

Controles Aplicados

Las amenazas encontradas se mitigan con los controles que se mencionan a continuación en la tabla 6.4:

Tabla 23 Caso No. 1 Amenazas, Vulnerabilidades y Controles

AMENAZA	VULNERABILIDAD	CONTROLES
[E.7] Deficiencias en la organización	• E.7.1 Acciones no coordinadas • E.7.2 Errores por omisión • E.7.3 Roles mal definidos • E.7.4 Desconocimiento de procedimientos	• A.18.2.2 Cumplimiento en las políticas y normas de seguridad • A.17.1.1 Planificación de la continuidad de la seguridad de la información • A.18.1.3 Protección de registros
[A.7] Uso no previsto	• A.7.1 Ausencia de procedimientos de manejo de información clasificada • A.7.3 Documentación con fallas estructurales no acordes a la organización	
[A.25] Robo	• A.25.1 Pérdida de soportes de Información	• **A.16.1.1** Responsabilidades y Procedimientos
[A.15] Modificación deliberada de la información	• A.15.1 alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.	• **A.7.1.1** Investigación de antecedentes • **A.7.3.1** Cese o cambio de puesto de trabajo.
[A.6] Abuso de privilegios de acceso	• A.6.1 Abuso de derecho	

CASO 2. Fuga De Información Del Proceso De Transporte De Valores

En la empresa FELMOVA se transporta los valores recaudados de los cobros para depositarlos en el banco, sin una compañía policial o guardia privada de custodia de valores.

Los depósitos se efectuaban con normalidad y salía en primera instancia el gerente general acompañado de una persona para realizar

el deposito en el banco, pero al querer evitar que los delincuentes piensen que solo el realizaba esa actividad, delega a otra persona para que vaya a realizar los depósitos de dichos valores en efectivo, y al salir por la puerta principal de las instalaciones de la empresa los estaba esperando un grupo armado de delincuentes que dispararon y asaltaron el vehículo, llevándose todo el dinero producto de lo recaudado por el cobro de valores.

Roles que intervienen en el caso

Entre las responsabilidades de cada uno de ellos se mencionan:

Gerente General

- ✓ Controlar y promover el cumplimiento de políticas de seguridad.
- ✓ -Buscar otras formas de efectuar los depósitos
- ✓ Promover cultura organizacional para manejo de posibles riesgos
- ✓ -Programar cronograma de depósitos para despistar a los delincuentes

Chofer

- ✓ -Cumplir con procedimientos de seguridad designados por el gerente general.
- ✓ **-**Cumplir con las normas de seguridad designadas por el gerente general.
- ✓ **-**Estar atento a cualquier situación anómala o comprometedora para evitar cualquier incidente.

Controles Aplicados

Las amenazas encontradas se mitigan con los controles que se mencionan a continuación en la tabla 24:

Tabla 24 Caso No. 2 Amenazas, Vulnerabilidades y Controles

AMENAZA	VULNERABILIDAD	CONTROLES
[E.7] Deficiencias en la organización	• E.7.1 Acciones no coordinadas • E.7.2 Errores por omisión • E.7.4 Desconocimiento de procedimientos	• A.18.2.2 Cumplimiento en las políticas y normas de seguridad • A.17.1.1 Planificación de la continuidad de la seguridad de la información. • A.11.11 Perímetro de Seguridad física • • A.11.1.2 Controles Físicos de entrada. • A.11.1.4 Protección contra las amenazas externas y ambientales. • A.11.1.6 Áreas de acceso público, carga y descarga •
[A.25] Robo	• A.25.1 Robo por personas ajenas a la organización	• **A.16.1.1** Responsabilidades y Procedimientos
[A.6] Abuso de privilegios de acceso	• A.6.1 Abuso de derecho	• **A.7.1.1** Investigación de antecedentes • **A.7.3.1** Cese o cambio de puesto de trabajo.

Los dos casos anteriormente mencionados sucedieron en la empresa, pero desde hace tiempo ya mantienen contratado un seguro para este

tipo de situaciones, por lo que se les aplicó controles por ser los de mayor criticidad, pero también se mencionan otros criterios que se deben tomar en cuenta para la mejor funcionalidad de la empresa

Por lo que se los mencionan a continuación:

Criterios de Valoración de información levantada.

Los criterios de valoración han sido aplicados en una escala de valores de 1-5, teniendo como valores críticos:

(5) **La empresa no cuenta con normas ISO de seguridad**.

Las normas ISO, ayudan a demostrar una gestión competente y eficaz de los recursos y datos que gestionan. Es decir que el no tenerlas resta garantías de las funcionalidades que hace activas las operaciones de cualquier organización.

El no tenerlo no implica un alto riesgo, pero que puede tener consecuencias críticas.

(4) **La empresa requiere establecer un servicio de internet de respaldo**.

El servicio de internet mantiene activo varias actividades que opera la empresa, el no contar con un servicio de respaldo puede retrasar las

tareas de empleados y no cumplir con obligaciones legales de la empresa.

(5) **La empresa necesita mantener acuerdos de servicios con otras empresas.**

Los acuerdos de servicio están relacionados directamente con los proveedores de la empresa, en donde debe estar estipulado en un documento que especifique la calidad del servicio contratado.

El no tener este tipo de compromisos, no implica un riesgo alto al momento para la empresa, pero sí es menester que se establezcan estos acuerdos que ayudarán a evitar que por los riesgos que puedan aparecer ocasione deterioro en los bienes de la empresa.

Cuadro de Afectaciones encontradas [29]

N	Riesgos	Afectaciones
5	La empresa no cuenta con normas ISO de seguridad	1. Puede causar un daño serio a la organización. 2. Puede afectar las relaciones comerciales. 3. Puede tener impacto con los clientes actuales y futuros. 4. Puede causar un daño que afecte la seguridad de la empresa.
4	La empresa requiere establecer de un servicio de internet de respaldo.	5. Puede afectar el interés comercial y económico de la empresa

5	La empresa necesita mantener acuerdos de servicios con otras empresas	6.	Puede causar un menor impacto que puede ser solucionado.

La dimensión de activos hace referencia al cuadro de afectaciones con escala de valoración del modelo MAGERIT, en donde estima el riesgo que pueden tener los activos, y que muestra como resultado las afectaciones relevantes para la organización.

En la gráfica 61 se detalla los porcentajes de amenazas de mayor riesgo en las organizaciones, realizado por Kapersky.

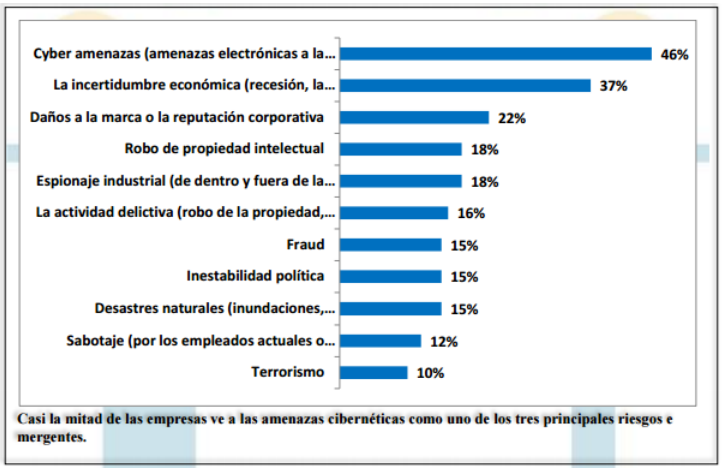


Figura 6. 1 Futuros Riesgos Fuente Kapersky Riesgos Globales de Seguridad de TI

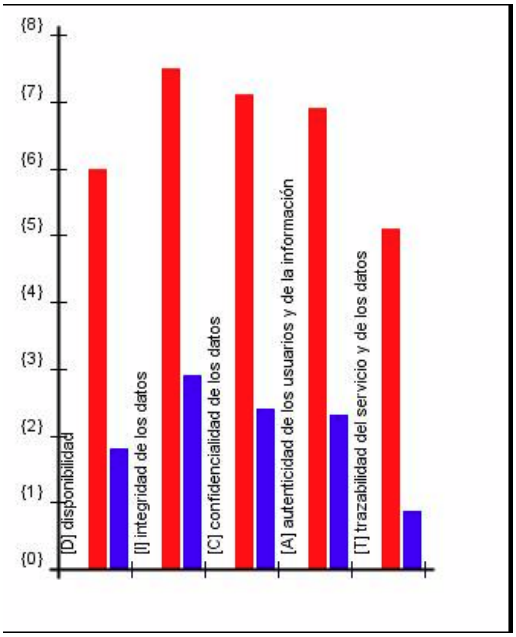


Figura 6. 2 Riesgo acumulado vs aplicando Pilar-salvaguardas

6.2. Entrega De Informes.

Lo más importante al realizar la evaluación de seguridad, es tener una comunicación clara y eficaz de los resultados, y así interpretar de la mejor manera la situación de la empresa y que protecciones son las más adecuadas para mitigar riesgos.

Se entrega un documento adicional donde se encuentran todos los anexos indicados en este estudio y que forman parte de los análisis realizados a la empresa FELMOVA S.A.

CONCLUSIONES Y RECOMENDACIONES

1. Con los datos recopilados se concluye que es muy importante tener un SGSI Sistema de Gestión de Seguridad de la Información, en donde este trabajo ha descrito la importancia de los términos utilizados en el análisis y gestión de riesgos y que debe ser manejada por equipos, servicios y personal idóneo del área de TI, además de que se mencionan estándares, metodologías y herramientas que permiten su estudio.
2. Como ya se lo ha mencionado, MAGERIT es la metodología que se empleó para conocer las amenazas a las que puede estar expuesta cualquier organización, en este caso específico a los activos de información y posteriormente desglosar los activos críticos.
3. La herramienta PILAR (licencia temporal), permitió el ingreso de valoraciones, en donde se les realizó evaluaciones de los activos, amenazas y salvaguardas, y así obtener niveles de riesgo e impacto mostrados en las gráficas, que dieron la pauta y la dirección para

implementar procedimientos y normas, con el propósito de proteger los recursos e información.

4. Al final se desarrolló una propuesta de un Plan de Seguridad, que tiene una política de seguridad y un cronograma de ejecución, con la finalidad de que la persona que se contrate pueda llevar a cabo esta actividad.
5. Las salvaguardas sugeridas (controles), permitirán minimizar los riesgos, pero tienen cada una un costo, por lo que es primordial evaluar cada caso en particular sobre la información a proteger y qué costos implicaría si sufriera la pérdida o un ataque, así como planificar las acciones necesarias para proteger la información.
6. Al proponer los controles de la Norma ISO 27002 aplicando la metodología MAGERIT con la herramienta (software)- PILAR-, se demostró una mejora para la Seguridad Física y del Entorno de la empresa FELMOVA en base a los resultados obtenidos para que, al implementar los controles necesarios, se aplique las salvaguardas, normas y procedimientos necesarios para la seguridad informática, sin olvidar los pilares de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
7. Si bien los resultados muestran una mejora a nivel de seguridad informática y reducción del riesgo de la situación actual de **64.8%** a **23.8%** ver figura 62**,** estos números pueden mejorar a medida que se tome en cuenta la planificación propuesta y los correctivos necesarios

planteados por la herramienta PILAR y de esta manera llegar al objetivo propuesto de **20.5%,** mitigando en gran porcentaje a las amenazas y vulnerabilidades encontradas en la investigación.

8. Según cita la revista GMV SOLUCIONES GLOBALES INTERNET S.A, en un artículo publicado “Risk Management Pilot forSMEs and Micro Enterprises in Spain”, indica que no existe ninguna herramienta disponible de gestión de riesgos para las pequeñas y medianas empresas. [42]
9. Se recomienda a las organizaciones, en general que realicen una evaluación de riesgos usando modelos simples, como el utilizado en este estudio, que permitirá resultados prácticos en menor tiempo y costos reducidos.
10. Se les sugiere a las empresas que realicen el análisis y gestión de riesgos de los sistemas de información, al menos una vez al año, con la finalidad de conocer sus fortalezas o debilidades e implementar salvaguardas necesarias y reducir las debilidades encontradas.

BIBLIOGRAFÍA

[1] Seguridad de la Información, https://www.gms.com.ec/

[2] El magazine para los profesionales de la seguridad de TI, http://magazcitum.com.mx/?p=2193#.V2SOX_nhDIU, fecha de consulta agosto 2016

[3] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I – Método

[4] Noticias, opiniones y análisis de la comunidad de seguridad de ESET, Metodología de Implantación de un SGSI en un grupo empresarial jerárquico ,http://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/, fecha de consulta agosto 2016

[5] Gustavo Pallas Mega, Tesis de Maestría, Metodología de Implantación de un SGSI en un grupo empresarial jerárquico www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf, fecha de consulta agosto 2016

[6] 27001 Academy, https://advisera.com/27001academy/es/

[7] El magazine para los profesionales de la seguridad de TI, http://www.magazcitum.com.mx/?p=2397#.V5Krm7jhCUk

[8] ISO 27002–Controles de Seguridad, http://www.iso27000.es/iso27002.html

[9] Noticias, opiniones y análisis de la comunidad de seguridad de ESET,ISO/IEC 27002:2013 Y Los Cambios En Los Dominios De Control http://www.welivesecurity.com/la-es/2013/12/12/iso-iec-27002-2013-cambios-dominios-control/

[10] Ormella Meyer y ASoc,"Las Nuevas Versiones de las Normas ISO 27001 e ISO 27002", http://www.criptored.upm.es/descarga/NuevasVersionesISO27001eISO27002.pdf

[11] https://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf

[12] Seguridad Física y Lógica en los Data Center, http://es.slideshare.net/Eve_And/seguridad-fsica-y-lgica

[13] The Electoral Knowledge Project, http://aceproject.org/main/espanol/et/ete01a.htm

[14] López Tello, Director de Alienvault , La seguridad física y lógica: conceptos convergentes,http://www.redseguridad.com/opinion/articulos/la-seguridad-fisica-y-logica-conceptos-convergentes

[15] http://www.gitsinformatica.com/seguridad%20logica%20fisica.html

[16] Lanche Capa, Tesis: "Diseño De Un Sistema De Seguridad De La Información Para La Compañía Acotecnic Cía. Ltda. Basado En La Norma Nte Inen ISO/IEC 27002", fecha de consulta agosto 2016

[17] Talens-Oliag, Seguridad Física, http://www.uv.es/~sto/cursos/icssu/html/ar01s04.html

[18]Torres Rodrigo , Metodología de Análisis de Riesgo de la Empresa La casa de las Baterías S.A. de C.V.,https://upload.wikimedia.org/wikipedia/commons/8/87/Riesgoinformatico.pdf

[19] Tovar Edgar,Teoria de Seguridad y Protección, http://www.monografias.com/trabajos82/teoria-seguridad-y-proteccion/teoria-seguridad-y-proteccion2.shtml

[20] Ramírez Riestra, “Sabotaje Interno: Una De Las Principales Causas De Pérdida De Información”, http://topmanagement.com.mx/sabotaje-interno-una-de-las-principales-causas-de-perdida-de-informacion/

[21] Castillo Tatiana, “Riesgo y Control Informático”,http://riesgosycontrolinf.blogspot.com/2014/03/evaluacion-de-riesgos-informaticos.html

[22] Portal Administración Electrónica, MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

[23] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información,Libro II - Catálogo de Elementos

[24] Tovar Edgar, Guía de seguridad física de instalaciones (Venezuela), http://www.monografias.com/trabajos94/seguridad-fisica-instalaciones-ii-venezuela/seguridad-fisica-instalaciones-ii-venezuela.shtml#ixzz4AZ7Va6gC

[25] Nieto Muñoz, Plan de Implementación de la ISO/IEC 27001, http://openaccess.uoc.edu/webapps/o2/bitstream/10609/23054/1/Nieto_WP2013_PlanImplementacionISO2007.pdf

[26] Estándares y Buenas Prácticas, MAGERIT página 50 medidas activas, http://estandares-y-buenas-practicas.wikispaces.com/MAGERITPagina 50 medidas activas

[27] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas

[28] Gorriti Aranguren , Máster MISTIC - Plan de Implementación de la ISO/IEC27001:2013, http://openaccess.uoc.edu/webapps/o2/bitstream/10609/43106/6/igorritiTFM0615memoria.pdf

[29] Moncayo Racines, Tesis: “Modelo de Evaluación de Riesgo en Activos de TIC’s para pequeñas y medianas Empreas del Sector Automotriz”, http://bibdigital.epn.edu.ec/bitstream/15000/8499/3/CD-5741.pdf, fecha de consulta agosto 2016

[30] Menéndez-Barzanallana Asensio, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información http://dis.um.es/~barzana/Curso03_04/MAGERIT.pdf, fecha de consulta agosto 2016

[31]Sánchez Esteban, “Análisis y Gestión de Riesgos en la UPCT con PILAR”, http://www.rediris.es/difusion/eventos/foros-seguridad/fs2012/archivo/analisis_riesgos_upct.pdf

[32] Universidad Nacional de Luján Departamento de Seguridad Informática , “Riesgo vs. Seguridad de la Información”,http://www.seguridadinformatica.unlu.edu.ar/sites/www.se

guridadinformatica.unlu.edu.ar/files/site/material_taller_gestion_de_riesgo.pdf

[33] Forero William, “Las Salvaguardas de Magerit”, http://www.seguriesgos.com/index.php/blog/79-las-salvaguardas-de-magerit

[34] Gaona Karina, Tesis: ”Aplicación de la Metodología MAGERIT, para el Análisis y gestión de Riesgos de la Seguridad de la Información aplicado a la empresa Pesquera e Industrial Bravito S.A en la ciudad de Machala” http://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdfhttp://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf

[35] Espinel y Martínez, “Copy of ISO 27002”, https://prezi.com/swg1cudlrmrx/copy-of-iso-27002/

[36] Eugeno y Parrales, “Implantación de un sistema de /gestión de Seguridad de la Información aplicada al Dominio Gestión de Activos para la Empresa Plásticos Internacionales Plasinca S.A.”, https://www.dspace.espol.edu.ec/bitstream/123456789/21624/1/Manual%20SGSI%20Aplicada%20a%20la%20Gestion%20de%20Activos.pdf

[37] Wutorres, Prevención Seguridad y Salud Laboral, http://prevencionseguridadysaludlaboral.blogspot.com/2012/05/factores-de-riesgos-fisicos.html

[38] Bedoya Jorge, “La Importancia Del Factor Humano En Los Procesos De Control De Acceso En Instalaciones”, http://repository.unimilitar.edu.co/bitstream/10654/12225/1/LA%20IMPORTANCIA%20DEL%20FACTOR%20HUMANO%20EN%20LOS%20PROCESOS%20DE%20CONTROL%20DE%20ACCESO%20EN%20INSTALACIONES.pdf

[39] Omar Reyes, “El factor humano, el mayor riesgo para la seguridad informática”, http://www.actiweb.es/reyes_278/archivo5.pdf

[40] Chan Aida, “Problemas de Seguridad Física (Factores ambientales y humanos)”, http://normasdeseguridad.blogspot.com/2012/09/seguridad-fisica-y-contra-cortos.html

[41] Administración de Centros de Cómputo , http://www.fcca.umich.mx/descargas/apuntes/Academia%20de%20Informatica/Adm%C3%B3n%20de%20Centros%20de%20Computo%20%20R.C.M/UNIDAD%20III.pdf

[42] GMV Soluciones Globales Internet, (2009), “Risk Management pilot forSMEs and Micro Enterprises in Spain”, En: http://www.enisa.europa.eu/act/rm/cr/infosec-smes/files/cs_GMV.pdf

[43] OWASP Secure Coding Practices Quick Reference Guide, https://www.owasp.org/index.php?title=File:OWASP_SCP_Quick_Reference_Guide_SPA.pdf&setlang=es, fecha de consulta 23 de enero de 2017.

[44] Universidad Nacional Autónoma de México, Facultad de Ingeniería, Laboratorio de redes y seguridad. http://redyseguridad.fip.unam.mx /proyectos/seguridad/ServDisponibilidad.php, fecha de consulta 23 de enero de 2017.

[45] Organización Internacional de Normalización ISO, ISO/DIS 22313:2012 Protección y Seguridad de los Ciudadanos – Sistema de Gestión de la Continuidad del Negocio – Directrices, 2012.

[46] Manual De Políticas De Seguridad De La Información, Instituto Colombiano De Crédito Educativo Y Estudios Técnicos En El Exterior, https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manualseguridadinformacion.pdf , fecha de consulta 23 de enero de 2017

ANEXOS

ANEXO 2 SoA

ISO 27001 SOA				
No	**Titulo del Control**	**Descripción del control**	**Implementación**	**Porque no se implementa**
A.5	POLITICA DE SEGURIDAD			
A5.1	Políticas de seguridad de la información			
A.5.1.1	Documento de las políticas de seguridad de la información	Control La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.	SI	
A.5.1.2	Revisión de las políticas de seguridad de la información	Control La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.	SI	
A.6	OGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
A.6.1	Organización interna			
A.6.1.1	Compromiso de la gerencia con la seguridad de la información	Control La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.	SI	
A.6.1.2	Coordinación de la seguridad de información	Control Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.	NO	Porque en el punto anterior ya está establecido con el gerente general
A.6.1.3	Asignación de responsabilidades de la seguridad de la información	Control Se deben definir claramente las responsabilidades de la seguridad de la información.	SI	

A.6.1.4	Proceso de autorización para los servicios de procesamiento de información	Control Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información	NO	No aplica porque la empresa está en proceso de expansión y ya se absorben ciertos procesos
A.6.1.5	Acuerdos de confidencialidad	Control Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información.	SI	
A.6.1.6	Contacto con autoridades	Control Se debe mantener los contactos apropiados con las autoridades relevantes.	SI	
A.6.1.7	Contacto con grupos de interés especial	Control Se deben mantener contactos apropiados con los grupos de interés especial u otros foros de seguridad especializada y asociaciones profesionales.	NO	Porque no es la línea de especialidad de la empresa
A.6.1.8	Revisión independiente de la seguridad de la información	Control El enfoque de la organización para manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se debe revisar independientemente a intervalos planeados, o cuando ocurran cambios significativos para la implementación de la seguridad.	SI	
A6.2	Entidades externas			
A.6.2.1	Identificación de riesgos relacionados con entidades externas	Control Se deben identificar los riesgos que corren la información y los medios de procesamiento de información de la organización y se deben implementar los controles apropiados antes de otorgar acceso.	SI	

A.6.2.2	Tratamiento de la seguridad cuando se trata con clientes	Control Se deben tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización.	NO	No hay extranet para clientes
A.6.2.3	Tratamiento de la seguridad en contratos con terceras personas	Control Los acuerdos que involucran acceso, procesamiento, comunicación o manejo por parte de terceras personas a la información o los medios de procesamiento de información de la organización; agregar productos o servicios a los medios de procesamiento de la información deben abarcar los requerimientos de seguridad necesarios relevantes.	SI	
A.7	Gestión de activos			
A.7.1	Responsabilidad por los activos			
A.7.1.1	Inventarios de activos	Control Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes	SI	
A.7.1.2	Propiedad de los activos	Control Toda la información y los activos asociados con los medios de procesamiento de la información deben ser 'propiedad' de una parte designada de a organización.	SI	
A.7.1.3	Uso aceptable de los activos	Control Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.	SI	
A.7.2	Clasificación de la información			
A.7.2.1	Lineamientos de clasificación	Control La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.	SI	

A.7.2.2	Etiquetado y manejo de la información	Control Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.	SI	
A.8	Durante el empleo			
A.8.1	Antes del empleo			
A.8.1.1	Roles y responsabilidades	Control Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización.	SI	
A.8.1.2	Selección	Control Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y	SI	
A.8.1.3	Términos y condiciones de empleo	Control Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información.	SI	
A.8.2	Durante el empleo			
A.8.2.1	Gestión de responsabilidades	Control La gerencia debe requerir que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.	SI	

A.8.2.2	Capacitación y educación en seguridad de la información	Control Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.	SI	
A.8.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.	SI	
A.8.3	Terminación o cambio del empleo			
A.8.3.1	Responsabilidades de terminación	Control Se deben definir y asignar claramente las responsabilidades para realizar la terminación o cambio del empleo.	SI	
A.8.3.2	Devolución de activos	Control Todos los empleados, contratistas y terceros deben devolver todos los activos de la organización que estén en su posesión a la terminación de su empleo, contrato o acuerdo.	SI	
A.8.3.3	Eliminación de derechos de acceso	Control Los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de la información deben ser eliminados a la terminación de su empleo, contrato o acuerdo, o se deben ajustar al cambio.	SI	
A.9	Seguridad física y ambiental			
A9.1	Áreas seguras			
A9.1.1	Perímetro de seguridad física	Control Se debe utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.	SI	

A9.1.2	Controles de entrada físicos	Control Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.	SI	
A9.1.3	Seguridad de oficinas, habitaciones y medios	Control Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.	SI	
A9.1.4	Protección contra amenazas externas y ambientales	Control Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.	SI	
A9.1.5	Trabajo en áreas seguras	Control Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras.	Parcial	
A9.1.6	Áreas de acceso público, entrega y carga	Control Se deben controlar los puntos de acceso como las áreas de entrega y descarga y otros puntos donde personas no-autorizadas pueden ingresar a los locales, y cuando fuese posible, se deben aislar de los medios de procesamiento de la información para evitar un acceso no autorizado.	SI	.
A9.2				
A9.2.1	Ubicación y protección de equipos	Control los equipo de deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno y las oportunidades de acceso no autorizado.	SI	
A9.2.2	Servicio de suministros	Control los equipo de deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas en los servicios de suministro	SI	

A9.2.3	Seguridad del cableado	Control el cableado de energía eléctrica y telecomunicaciones que trasporta datos o presta soporte a los servicios de información deben estar protegidos contra interrupciones o daños	SI	
A9.2.4	Mantenimiento de los equipos	Control El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad	SI	
A9.2.5	Seguridad de los equipos fuera de las instalaciones	Control Se debe aplicar seguridad al equipo fuera-del- local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.	SI	
A9.2.6	Seguridad de la reutilización o eliminación de los equipos	Control Todos los ítems de equipo que contengan medios de almacenaje deben ser chequeados para asegurar que se haya removido o sobre-escrito de manera segura cualquier data confidencial y software con licencia antes de su eliminación.	SI	
A9.2.7	Retiro de activos	Control Equipos, información o software no deben ser sacados fuera de la propiedad sin previa autorización.	SI	
A10	GESTIÓN DE COMUNICACIONES Y OPERACIONES			
A10.1	Procedimientos operacionales y responsabilidades.			
A10.1.1	Documentación de los procedimientos de operación.	Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.	SI	
A10.1.2	Gestión del cambio.	Se debe controlar los cambios en los servicios y los sistemas de procesamiento de información.	SI	
A10.1.3	Distribución de funciones.	Las funciones y las áreas de responsabilidad se deben distribuir para reducir las oportunidades de modificación no autorizada o no	SI	

		intencional, o el uso inadecuado de los activos de la organización.		
A10.1.4	Separación de las instalaciones de desarrollo, ensayo y operación.	Las instalaciones de desarrollo, ensayo y operación deben estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo.	NO	No aplica por el tipo de actividad de la empresa que es comercial
A10.2	Gestión de la prestación de los servicios por terceras partes.			
A10.2.1	Prestación del servicio.	Se debe garantizar que los controles de seguridad, las definiciones del servicio y los niveles de prestación del servicio incluidos en el acuerdo, sean implementados, mantenidos y operados por las terceras partes.	SI	
A10.2.2	Monitoreo y revisión de los servicios por terceras partes.	Los servicios, reportes y registros suministrados por terceras partes se deben controlar y revisar con regularidad y las auditorias se deben llevar a cabo a intervalos regulares.	SI	
A10.2.3	Gestión de los cambios en los servicios por terceras partes.	Los cambios de la prestación de los servicios, incluyendo mantenimiento y mejora de las políticas existentes de seguridad de la información, en los procedimientos y controles se deben gestionar teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados, así como la revaluación de los riesgos.	SI	
A10.3	Protección contra códigos maliciosos y móviles.			
A10.3.1	Gestión de la capacidad.	Se debe hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.	SI	

A10.3.2	Aceptación del sistema.	Se deben establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.	SI	
A10.4	Protección contra códigos maliciosos y móviles.			
A10.4.1	Controles contra códigos maliciosos.	Se debe implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos adecuados de concientización de los usuarios.	SI	
A10.4.2	Controles contra códigos móviles.	Cuando se autoriza la utilización de códigos móviles, la configuración debe asegurar que dichos códigos operan de acuerdo con la política de seguridad claramente definida, y se debe evitar la ejecución de los códigos móviles no autorizados.	NO	No contamos con códigos móviles.
A10.5	Respaldo			
A10.5.1	Respaldo de la información.	Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.	SI	
A10.6	Gestión de la seguridad de las redes			
A10.6.1	Controles de la redes.	Las redes se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.	SI	
A10.6.2	Seguridad de los servicios de la red.	En cualquier acuerdo sobre los servicios de la red se deben identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan	SI	

		en la organización o se contratan externamente.		
A10.7	Manejo de los Medios.			
A10.7.1	Gestión de los medios removibles.	Se deben establecer procedimientos para la gestión de medios removibles.	SI	
A10.7.2	Eliminación de los medios.	Cuando ya no se requieran estos medios, su eliminación se debe hacer en forma segura y sin riesgo, utilizando los procedimientos formales.	SI	
A10.7.3	Procedimientos para el manejo de la información.	Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.	SI	
A10.7.4	Seguridad de la documentación del sistema.	La documentación del sistema debe estar protegida contra acceso no autorizado.	SI	
A10.8	Intercambio de la información.			
A10.8.1	Políticas y procedimientos para el intercambio de información.	Se deben establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación.	SI	
A10.8.2	Acuerdos para el intercambio.	Se deben establecer acuerdos para el intercambio de la información y el software entre la organización y partes externas.	SI	
A10.8.3	Medios físicos en tránsito.	Los medios que contienen información se deben proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la organización.	SI	
A10.8.4	Mensajería electrónica.	La información contenida en la mensajería electrónica debe tener la protección adecuada.	SI	
A10.8.5	Sistemas de información del negocio.	Se deben establecer, desarrollar e implementar políticas y procedimientos	SI	

		para proteger la información asociada con la interconexión de los sistemas de información del negocio.		
A10.9	Servicios de comercio electrónico.			
A10.9.1	Comercio electrónico.	La información involucrada en el comercio electrónico que se transmite por las redes públicas debe estar protegida contra actividades fraudulentas, disputas de contratos y divulgación o modificación no autorizada.	NO	No se cuenta con servicio comercio electrónico
A10.9.2	Transacciones en línea.	La información involucrada en las transacciones en línea debe estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración, divulgación, duplicación o repetición no autorizada del mensaje.	NO	No se dispone de este servicio
A10.9.3	Información disponible al público.	La integridad de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no autorizada.	No	No se dispone de este servicio
A10.10	Monitoreo			
A10.10.1	Registro de auditorías.	Se debe elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoria de las actividades de los usuarios, la excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso.	SI	
A10.10.2	Monitoreo del uso del sistema.	Se deben establecer procedimientos para el monitoreo de uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deben revisar con regularidad.	SI	
A10.10.3	Protección de la información del registro.	Los servicios y la información de la actividad de registro se deben proteger	SI	

		contra el acceso o la manipulación no autorizados.		
A10.10.4	Registros del administrador y del operador.	Se deben registrar las actividades tanto del operador como del administrador del sistema.	SI	
A10.10.5	Registros de falla.	Las fallas se deben registrar y analizar, y se deben tomar las acciones adecuadas.	SI	
A10.10.6	Sincronización de relojes.	Los relojes de todos los sistemas de procesamiento de información pertinente dentro de la organización o del dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta y acordada.	NO	No se dispone de este tipo de procesos
A11	CONTROL DE ACCESO			
A11.1	Requisitos del negocio para el control de acceso.			
A11.1.1	Política de control de acceso.	Se debe establecer, documentar y revisar la política de control de acceso con base a los requisitos del negocio y de la seguridad para el acceso.	SI	
A11.2	Gestión del acceso de usuarios.			
A11.2.1	Registro de usuarios.	Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.	SI	
A11.2.2	Gestión de privilegios.	Se debe restringir y controlar la asignación y uso de privilegios.	SI	
A11.2.3	Gestión de contraseñas para usuarios.	La asignación de contraseñas se debe controlar a través de un proceso formal de gestión.	SI	
A11.2.4	Revisión de los derechos de acceso de los usuarios.	La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.	SI	

A11.3	Responsabilidades de los usuarios			
A11.3.1	Uso de contraseñas.	Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas.	SI	
A11.3.2	Equipo de usuario desatendido.	Los usuarios deben asegurarse de que los equipos desatendidos se las da la protección adecuada.	SI	
A11.3.3	Política de escritorio despeja y pantalla despejada.	Se debe adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.	SI	
A11.4	Control de acceso a las redes			
A11.4.1	Política de uso de servicios de red.	Los usuarios solo deben tener acceso a los servicios para cuyo uso están específicamente autorizados.	SI	
A11.4.2	Autenticación de usuarios para conexiones externas.	Se deben emplear métodos adecuados de autenticación para controlar el acceso de usuarios remotos.	SI	
A11.4.3	Identificación de los equipos en las redes.	La identificación automática de los equipos se debe considerar un medio para autenticar conexiones de equipos y ubicaciones específicas.	SI	
A11.4.4	Protección de los puestos de configuración y diagóstico remoto.	El acceso lógico y físico a los puertos de configuración y de diagnóstico debe estar controlado.	SI	
A11.4.5	Separación de las redes.	En las redes se deben separar los grupos de servicios de información, usuarios y sistemas de información.	SI	
A11.4.6	Control de conexión a las redes.	Para redes compartidas, especialmente para aquellas que se extiendes más allá de las fronteras de la organización, se debe restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control de	SI	

		acceso y los requisitos de aplicación del negocio (véase el numeral 11.1)		
A11.4.7	Control de enrutamiento en la red.	Se deben implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control del acceso a de las aplicaciones.	SI	
A11.5	Control de acceso al sistema operativo.			
A11.5.1	Procedimientos de ingreso seguro.	El acceso a los sistemas operativos se debe controlar mediante un procedimiento de registro de inicio seguro.	SI	
A11.5.2	Identificación y autenticación de usuarios.	Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.	SI	
A11.5.3	Sistema de gestión de contraseñas.	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	SI	
A11.5.4	Uso de las utilidades del sistema.	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.	SI	
A11.5.5	Tiempo de inactividad de la sesión.	Las sesiones inactivas se deben suspender después de un periodo de inactividad.	SI	
A11.5.6	Limitación del tiempo de conexión.	Se deben utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo.	SI	
A11.6	Control de acceso a las aplicaciones y a la información.			
A11.6.1	Restricciones de acceso a la información.	Se debe restringir el acceso a la información y las funciones del sistema de aplicación por parte de los usuarios y	SI	

		del personal de soporte, de acuerdo con la política definida en el control de acceso.		
A11.6.2	Aislamiento de sistemas sensibles.	Los sistemas sensibles deben tener un entorno informático dedicado (aislados).	SI	
A11.7	Computación móvil y trabajo remoto.			
A11.7.1	Computación y comunicaciones móviles.	Se debe establecer una política formal y se deben adoptar las medidas de seguridad apropiadas para la protección contra riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.	SI	
A11.7.2	Trabajo remoto.	Se deben desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.	NO	No se dispone de este servicio
A12	ADQUISICION, MANTENIMIENTO Y DESARROLLO DE MANTENIMIENTOS DE INFORMACION.			
A12.1	Requisitos de seguridad de los sistemas de información.			
A12.1.1	Análisis y especificación de los requisitos de seguridad.	Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras de los sistemas existentes deben especificar los requisitos para los controles de seguridad.	SI	
A12.2	Procesamiento correcto de las aplicaciones.			
12.2.1	Validación de los datos de entrada.	Se deben validar los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados.	SI	
12.2.2	Control de procesamiento interno.	Se deben incorporar verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados.	SI	

12.2.3	Integridad del mensaje.	Se deben identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.	NO	No se requiere integridad de los mensajes
12.2.4	Validación de los datos de salida.	Se deben validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias.	SI	
A12.3	Controles Criptográficos.			
12.3.1	Política sobre el uso de controles criptográficos.	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	NO	No se utilizan estos controles
12.3.2	Gestión de llaves.	Se debe implementar un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas por parte de la organización.	NO	No se utilizan estos controles
A12.4	Seguridad de los archivos del sistema.			
12.4.1	Control del software operativo.	Se deben implementar procedimientos para controlar la instalación de software en los sistemas operativos.	SI	
12.4.2	Protección de los datos de prueba del sistema.	Los datos de prueba deben seleccionarse cuidadosamente, así como protegerse y controlarse.	SI	
12.4.3	Control de acceso al código fuente de los programas.	Se debe restringir el acceso al código fuente de los programas.	SI	
A12.5	Seguridad en los procesos de desarrollo y soporte			
12.5.1	Procedimientos de control de cambios.	Se debe controlar la implementación de cambios utilizando procedimientos formales de control de cambios.	SI	
12.5.2	Revisión técnica de las aplicaciones después de	Cuando se cambias los sistemas operativos, las aplicaciones críticas para el negocio se deben revisar y someter a prueba para asegurar que no hay	SI	

	los cambios en el sistema operativo.	impacto adverso en las operaciones ni en la seguridad de la organización.		
12.5.3	Restricciones en los cambios a los paquetes del software.	Se debe desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	SI	
12.5.4	Fuga de información.	Se debe evitar las oportunidades para que se produzca fuga de información.	SI	
12.5.5	Desarrollo de software contratado externamente.	La organización debe supervisar y monitorear el desarrollo de software contratado externamente.	SI	
A12.6	Gestión de la vulnerabilidad técnica.			
12.6.1	Control de vulnerabilidades técnicas.	Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.	SI	
A13	GESTION DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACION.			
A13.1	Reporte sobre los eventos y las debilidades de la seguridad de la información.			
13.1.1	Reporte sobre los eventos de seguridad de la información.	Los eventos de seguridad de la información se deben informar atreves de los canales de gestión apropiados tan pronto como sea posible.	SI	
13.1.2	Reporte sobre las debilidades de la seguridad.	Se debe exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.	SI	

13.2	Gestión de los incidentes y las mejoras en la seguridad de la información.			
13.2.1	Responsabilidades y procedimientos.	Se deben establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	SI	
13.2.2	Aprendizaje debido a los incidentes de seguridad de la información.	Deben existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.	SI	
13.2.3	Recolección de evidencia.	Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.	SI	
A14	GESTION DE LA CONTINUIDAD DEL NEGOCIO			
A14.1	Aspectos de seguridad de la información, de la gestión de la continuidad del negocio.			
14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.	Se debe desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.	SI	
14.1.2	Continuidad del negocio y evaluación de riesgos.	Se debe identificar los eventos que puedan ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus	SI	

		consecuencias para la seguridad de la información.		
14.1.3	Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información.	Se deben desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos críticos para el negocio.	SI	
14.1.4	Estructura para la planificación de la continuidad del negocio.	Se debe mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento.	SI	
14.1.5	Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio.	Los planes de continuidad del negocio se deben someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.	SI	
A15	CUMPLIMIENTO			
A15.1	Cumplimiento de los requisitos legales.			
15.1.1	Identificación de la legislación aplicable.	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la organización.	SI	
15.1.2	Derechos de la propiedad intelectual (DPI).	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad	SI	

		intelectual y sobre el uso de productos de software patentados.		
15.1.3	Protección de los registros de la organización.	Los registros importantes se deben proteger contra perdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio.	SI	
15.1.4	Protección de los datos y privacidad de la información personal.	Se debe garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes, si se aplica, con las clausulas del contrato.	SI	
15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información.	Se debe disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados.	SI	
15.1.6	Reglamentación de los controles criptográficos.	Se deben utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.	NO	No se utilizan estos controles
A15.2	Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico.			
15.2.1	Cumplimiento con las políticas y normas de seguridad.	Los directores deben garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr los cumplimientos con las políticas y las normas de seguridad.	SI	
15.2.2	Verificación del cumplimiento técnico.	Los sistemas de información se deben verificar periódicamente para verificar el cumplimiento con las normas de implementación de la seguridad.	SI	
A15.3	Consideraciones de la auditoria de los sistemas de información.			

15.3.1	Controles de auditoria de Los sistemas de información.	Los requisitos y las actividades de auditoria que implican verificaciones de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.	SI	
15.3.2	Protección de las herramientas de auditoria de los sistemas de información.	Se debe proteger el acceso a las herramientas de auditoria de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro	SI	

i

ANEXO 3 CATALOGO DE SALVAGUARDAS

1. Protecciones generales u horizontales
    - Identificación y autenticación
    - Control de acceso lógico
    - Segregación de tareas
    - Gestión de incidencias
    - Establecer herramientas de seguridad
    - Establecer herramienta contra código dañino
    - Establecer herramienta de detección/ prevención de intrusión
    - Establecer herramienta de chequeo de configuración
    - Establecer herramienta de análisis de vulnerabilidades
    - Establecer herramienta de monitorización de trafico
    - Establecer herramienta de monitorización de contenidos
    - Establecer herramienta de para análisis de logs
    - Gestión de vulnerabilidades de registro y auditoria

2. Protección de los datos / información
    - Protección de la información física y lógica
    - Copias de seguridad de los datos (backup)
    - Aseguramiento de la integridad de acceso a información
    - Cifrado de la información, claves de acceso
    - Uso de discos duros o dispositivos físicos para almacenamiento de información
    - Mecanismos de control para respaldo automático de información
    - Plan de alquiler de un casillero de seguridad para alojamiento de respaldos de información
    - Plan de adquisición o programación de reglas o normas para protección de activos

3. Protección de los servicios
    - Protección de los servicios
    - Aseguramiento de la disponibilidad
    - Aceptación y puesta en operación
    - Aplicar perfiles de seguridad
    - Gestión de cambios (mejoras y sustituciones)

- Protección de servicios y aplicaciones web
- Protección de correo electrónico
- Protección del directorio
- Protección del servidor de nombre de dominio

4. Protección de las aplicaciones (Software)
    - Protección de las aplicaciones informáticas
    - Copias de seguridad (backup)
    - Procedimientos para correr aplicaciones
    - Aplicar perfiles de seguridad sobre los datos
    - Cambios (actualizaciones y mantenimiento)
    - Plan instalación consola de antivirus para protección de ataques
    - Cotización y regulación de licencias de software
    - Plan de adquisición de equipos con su respectiva licencia y garantía

5. Protección de los equipos(hardware)
    - Protección de los equipos informáticos por medio de ups
    - Realizar un plan de apagado de equipos cuando no exista electricidad
    - Entrenar a los usuarios el apagado inmediato de equipos
    - Realizar un plan de operación manual de procesos
    - Gestión de cambio (mejoras y sustituciones)
    - Evaluaciones tecnológicas de los equipos
    - Programación de mantenimientos periódicos físico y lógico de los equipos

6. Protección de las comunicaciones
    - Protección de las comunicaciones a través de un plan de internet de respaldo
    - Aseguramiento de la disponibilidad
    - Plan de transparencia para el cambio de plan de datos
    - Protección, seguridades para plan B de respaldo
    - Registro de incidencias por perdidas de plan de datos

- Acuerdos con proveedores para mantener servicios de calidad

7. Protección en los puntos de interconexión con otros sistemas
    - Revisión de puntos de interconexión: conexiones entre zonas de confianza
    - Instalar un sistema de protección perimetral
    - Revisar tableros de control asociados a tierra
    - Realizar mediciones periódicas de voltaje para zonas que se requiere mayor protección
    - Instalar o mejorar protecciones actuales de UPS

8. Protección de los soportes de información
    - ¿Protección de soportes de información
    - Aseguramiento de la disponibilidad
    - Protección criptográfica del contenido
    - Limpieza de contenidos
    - Destrucción de soportes

9. Protección de elementos auxiliares
    - Mantener protección para elementos auxiliares
    - Plan de apagado de equipos auxiliares
    - Soportes de información para posibles desastres

10. Seguridad física – Protección de las instalaciones
    - Revisar protección de las instalaciones
    - Tener planos del diseño de instalaciones y conexiones
    - Tener control a mantenimientos de conexiones a tierra
    - Mantener seguridad en protecciones externas
    - Instalar sistemas de control de acceso a áreas restringidas

11. Salvaguardas relativas al personal
    - Formación y concientización al personal
    - Aseguramiento de la disponibilidad

12. Salvaguardas de tipo organizativo
    - Reunión alta gerencia de la Organización
    - Implementar gestión de riesgos
    - Planificación de la seguridad
    - Inspecciones de seguridad

13. Continuidad de operaciones
    - Elaborar un plan de prevención y reacción frente a desastres
    - Mantener continuidad del negocio
    - Análisis de impacto (BIA)
    - Plan de recuperación de Desastres (DRP)

14. Externalización
    - Identificación y calificación de proveedores
    - Procedimientos de escalado y resolución de incidencias
    - Procedimiento de terminación (duración en el tiempo de las responsabilidades asumidas)
    - Asunción de responsabilidades y penalizaciones por incumplimiento

15. Adquisición y desarrollo
    - Establecer buenas prácticas en instalaciones, calidad de servicios
    - Establecer normativas y controles que rige la ley
    - Buscar plan de capacitación sobre el manejo de nuevas normas a implementar
    - Establecer planes de mantenimiento de activos
    - Establecer acuerdos formales sobre la adquisición de servicios o equipos

16. Seguridad, protección de bienes
    - Plan de cotizaciones de seguros de equipos
    - Posibilidad de aplicar garantías de compras en equipos
    - Concientizar a la alta gerencia la importancia de mantener asegurados los activos

- Instalar cámaras de vigilancia para proteger a los equipos

Finalmente, los procedimientos y salvaguardas son medidas de protección desplegadas para aquellas amenazas cuyo valor es de riesgo alto.

GLOSARIO

Autenticación: Conjunto de Controles utilizados para verificar la identidad de un usuario o entidad que interactúa con el software [45]

Confidencialidad: Propiedad de la información por la que se garantiza que está accesible únicamente a entidades autorizadas [43].

Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye policías, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal. [46]

Disponibilidad: Es un servicio que garantiza que los usuarios autorizados tengan acceso a la información y a otros activos de información en el lugar, momento y forma en que son requeridos [43].

Ingeniería social: Técnica que consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían. Se refiere a formas de violación que se sustentan en las debilidades de las personas más que en el software. El objetivo es engañar a la gente para que revele contraseñas u otra información que comprometa la seguridad del sistema objetivo [44].

Integridad: La seguridad de que la información es precisa, completa y válida, y no ha sido alterada por una acción no autorizada [43].

Mitigar: Pasos tomados para reducir la severidad de una vulnerabilidad. Estos pueden incluir remover una vulnerabilidad, hacer una vulnerabilidad más difícil de explotar, o reducir el impacto negativo de una explotación exitosa [43].

Vulnerabilidad: Debilidad en un sistema que lo hace susceptible a ataque o daño. [43].