UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERÍAS

Trabajo de fin de carrera titulado:

"DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA SWEADEN COMPAÑÍA DE SEGUROS S.A, BASADO EN LA NORMA ISO/IEC 27002:2013"

Realizado por:

Ing. Jaime Andrés Almeida Bajaña

Director del proyecto:

Ing. Verónica Rodríguez, MBA.

Como requisito para la obtención del título de:

MÁSTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD EN REDES Y COMUNICACIÓN

DECLARATORIA

Este trabajo de investigación tiene por título:

"DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA SWEADEN COMPAÑÍA SEGUROS S.A BASADO EN LA NORMA ISO/IEC 27002:2013"

Realizado por:

JAIME ANDRÉS ALMEIDA BAJAÑA

Como requisito para la Obtención del Título de:

MÁSTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD EN REDES Y COMUNICACIÓN

Ha sido dirigido por el profesor

Ing. Verónica Elizabeth Rodríguez Arboleda, MBA.

Quien considera que constituye un trabajo original de su autor

_____

Ing. Verónica Elizabeth Rodríguez Arboleda, MBA.

DIRECTORA

DEDICATORIA

Dedico este proyecto de tesis a:

Mi madre Fanny Bajaña, por guiarme y por brindarme su apoyo incondicional siempre.

Mi padre Jaime Almeida, que siempre lo llevo presente y quien ha sido mi inspiración para cumplir todo lo que me he propuesto en lo personal y profesional y aunque ya no estás aquí con nosotros este logro también es tuyo.

Mi hermano, hermana y sobrinas, por estar conmigo y apoyarme cuando lo necesité, son mi motivación para seguir superándome.

Finalmente, a mis maestros, quienes me guiaron con su conocimiento y enseñanzas, y a mi tutora de tesis por haberme ayudado con el desarrollo de esta investigación.

AGRADECIMIENTO

Agradezco a:

Mi madre por su confianza y apoyo incondicional, a mis hermanos y sobrinas por ser mi inspiración.

A SWEADEN Seguros, por permitirme realizar la investigación para este proyecto de tesis.

A la Ing. Verónica Rodríguez, mi directora de Tesis por su valiosa guía y apoyo en el desarrollo de este proyecto de tesis.

DECLARACIÓN JURAMENTADA

Yo, Jaime Andrés Almeida Bajaña, con cédula de identidad 1600362774, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que ha consultado las referencias bibliográficas que se incluyen en este documento.

Mediante la presente declaración, cedo los derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

_____

Jaime Andrés Almeida Bajaña
C.C: 1600362774

LOS PROFESORES INFORMANTES

Los Profesores informantes:

Ing. Christian David Pazmiño Flores, MSC.

Ing. Edison Estrella Mogollón, MBA

Después de revisar el trabajo presentado lo han calificado

como apto para su defensa oral ante el tribunal examinador

_____	_____
Ing. Christian David Pazmiño Flores, MSC	Ing. Edison Estrella Mogollón, MBA

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

Jaime Andrés Almeida Bajaña

CC: 1600362774

RESUMEN

Este proyecto de tesis tiene como alcance Diseñar una Política de Seguridad de la Información, basada en la Norma ISO/IEC 27002:2013 para el área tecnológica de SWEADEN Compañía de Seguros, con la finalidad de controlar y mitigar las amenazas y vulnerabilidades que podrían afectar a la confidencialidad, integridad y disponibilidad de la información de la organización. Como punto inicial se genera una matriz de riesgos adoptando la metodología MAGERIT la misma que permite identificar los activos de información, sus amenazas y vulnerabilidades para posteriormente valorar las dimensiones de probabilidad e impacto que determinan el riesgo a los que se expone la información. Se realizan encuestas al personal de la aseguradora para diagnosticar el nivel de conciencia que tienen los usuarios con respecto a seguridades y protección de la información. Posteriormente se analiza la norma internacional ISO/IEC 27002:2013 que contiene buenas prácticas para la gestión de la seguridad de la información, esta norma es aplicable en todo tipo de organizaciones sin importar su tamaño, tipo o naturaleza. Con este análisis y en función de los riesgos identificados en la matriz generada se seleccionan los controles de la norma que permitirían mitigar los riesgos encontrados en la organización. Finalmente, con los controles seleccionados se procede a diseñar una política de seguridad de la información para SWEADEN Compañía de Seguros S.A, ya que esto le permitirá a la organización y al área de TICs contar con guía para el buen uso y gestión de sus activos de información.

Palabras Clave: ISO/IEC 27002, Metodología MAGERIT, Norma, Política de seguridad

ABSTRACT

This thesis project is designed to design an Information Security Policy, based on the ISO / IEC 27002: 2013 Standard for the technological area of SWEADEN Insurance Company, in order to control and mitigate threats and vulnerabilities that could affect to the confidentiality, integrity and availability of the organization's information. As a starting point, a risk matrix is generated by adopting the MAGERIT methodology, which allows the identification of information assets, their threats and vulnerabilities, to subsequently assess the probability and impact dimensions that determine the risk to which the information is exposed. Surveys are carried out to insurer's personnel to diagnose the level of awareness that users have regarding security and information protection. Subsequently, the international standard ISO / IEC 27002: 2013, which contains good practices for the management of information security, is analyzed, this standard is applicable in all types of organizations regardless of their size, type or nature. With this analysis and based on the risks identified in the generated matrix, the controls of the norm that would mitigate the risks found in the organization are selected. Finally, with the selected controls we proceed to design an information security policy for SWEADEN Insurance Company S.A., as this will allow the organization and the ICT area to have guidance for the proper use and management of its assets. information.

Key Words: ISO / IEC 27002, MAGERIT Methodology, Standard, Security Policy.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I

INTRODUCCIÓN

1.1 Problema de investigación

1.1.1 Planteamiento del problema

1.1.1.1 Diagnóstico

SWEADEN COMPAÑÍA DE SEGUROS S.A. es una empresa dedicada a la venta y gestión de pólizas de seguros, estos seguros pueden ser de vida como también de bienes materiales o patrimoniales, tiene presencia en 12 ciudades a nivel nacional y se conforma de 160 empleados, por lo que se consideraría una mediana empresa en proceso de crecimiento.

De la última auditoría realizada al área de tecnología en el 2018 por el Ing. CISA Eduardo Guacapiña, cuyo alcance fue evaluar la gestión del área tecnológica y sus procesos relacionados, se logró determinar que existen novedades que están relacionados con la gestión de la seguridad física y lógica de la información, por lo que se han considerado estas observaciones en el presente estudio.

Los resultados de la auditoría efectuada y la observación directa muestran que a pesar de que la organización cuenta con un manual de políticas de tecnologías, manual de procedimientos de tecnología y planes de contingencia, aún existen brechas en la seguridad tales como:

- La organización no cuenta con un sistema de Directorio Activo, que permita implementar controles óptimos para gestionar el acceso y el uso controlado de los recursos de la red de datos corporativa.
- A pesar de que la organización cuenta con un antivirus corporativo debidamente licenciado, existen equipos que no están protegidos con esta herramienta.
- El sistema web de consulta para asesores no posee certificado SSL.
- El portal de consulta para facturación electrónica no posee certificado SSL.
- Existen usuarios que no hacen uso del bloqueo de pantallas en los ordenadores asignados, esto permite que cualquier persona pueda acceder a ellos cuando el usuario se ausenta de su lugar de trabajo.
- Las credenciales de las cuentas de correos electrónicos de los usuarios son conocidas por los administradores de tecnología.
- No existe puerta metálica ni con panel biométrico en el acceso al centro de cómputo.
- Se evidencia que existe una deficiencia con el control de acceso a periféricos como USB, esto permitiría la infección del equipo por malware o la sustracción de información.
- No existen convenios de confidencialidad para las personas que ocupan cargos críticos en donde se establezcan cláusulas de no divulgación de información de la organización.
- El área de tecnología no posee una política de seguridad informática donde se detallen los lineamientos y responsabilidades para el tratamiento seguro de la información, poniendo en riesgo a la confidencialidad, integridad y disponibilidad de esta.

1.1.1.2 Pronóstico

SWEADEN Seguros, desde que inició sus actividades ha tenido un crecimiento institucional significativo hasta la actualidad, esto se puede notar en la Tabla número 1. Debido a este crecimiento es importante considerar como prioridad la seguridad de su información, que es uno de los activos valiosos para brindar continuidad y sostenibilidad a la organización. Si en el futuro no existe un proceso controlado o una política para la gestión de la información, la empresa puede exponerse a una serie de riesgos informáticos que afectarían a los datos, considérese (alteración, eliminación, suplantación, acceso no autorizado, fuga de información, etc.) los mismos que pueden detener las operaciones del negocio de manera temporal e incluso permanente.

Tabla 1 Crecimiento de la población Institucional

AÑO	CANT. INGRESOS DE USUARIOS POR AÑO	CRECIMIENTO DEL PERSONAL POR AÑO
2008	5	5
2009	7	12
2010	3	15
2011	8	23
2012	12	35
2013	11	46
2014	12	58
2015	5	63
2016	15	78
2017	28	106
2018	43	149
2019	14	163

Fuente: Área de Talento Humano SWEADEN

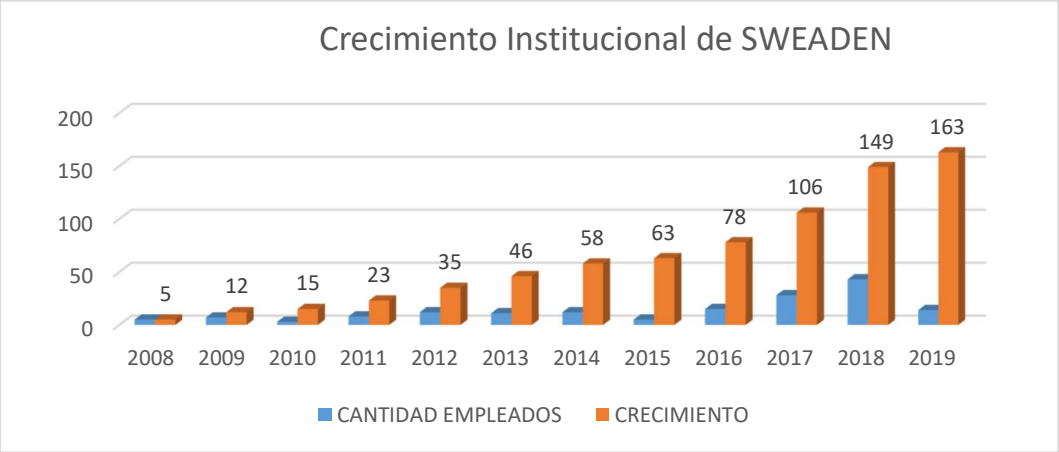


Figura 1 Crecimiento Institucional SWEADEN
Fuente: Elaborado por el investigador

Como se puede ver en la Figura 1, la cantidad de usuarios de SWEADEN Seguros desde sus inicios hasta la actualidad se ha venido incrementando, tanto así que el problema más importante de no tener una política de seguridad de la información radica en que los riesgos de los datos aumentan a medida de que el personal de la empresa crece, de tal manera que si dichos riesgos no se llegaran a controlar pueden ocasionar: daños a la reputación de la empresa, pérdidas económicas, afectación en la productividad e incluso penalizaciones que provoquen el cese de las funciones, inhabilitando las operaciones de la organización de manera temporal o indefinida, por consecuencia de una inadecuada gestión de los datos.

1.1.1.3 Control del Pronóstico

Para la mitigación y control de los riesgos de la información se tiene que considerar una normativa de seguridad de la información internacional como la ISO/IEC 27002:2013, ya que esta permite establecer controles y estrategias más adecuadas para eliminar o minimizar dichos riesgos, por lo tanto, establecer una normativa de seguridad permitirá que la organización y su área

tecnológica cuente con mecanismos para el aseguramiento de los activos de información de manera apropiada.

1.1.1.4 Formulación del problema.

Mediante la información recopilada y los procesos de auditoría realizados en el área tecnológica de SWEADEN Seguros, se han observado inconvenientes relacionados con la seguridad de la información, estos pueden afectar directamente a los procesos tecnológicos de la organización interrumpiendo sus operaciones de manera temporal o definitiva.

1.2 Objetivos

1.2.1 Objetivo General

Diseñar una política de seguridad de la información para SWEADEN COMPAÑÍA DE SEGUROS basada en la normativa ISO/IEC 27002:2013, con los lineamientos para que él área de tecnología de la organización gestione la información asegurando su confidencialidad, integridad y disponibilidad.

1.2.2 Objetivos específicos

- Identificar la situación actual de la información de SWEADEN Seguros, mediante una matriz de riesgos basada en la metodología MAGERIT que permita el análisis de las vulnerabilidades y amenazas a las que está expuesta.

- Analizar el nivel de concientización en el manejo de seguridad y protección de la información que tiene el personal de la organización, mediante una aplicación de encuestas que permita la identificación de los riesgos que pueden afectar a las operaciones del negocio a través de las prácticas de los usuarios.

- Determinar los controles de la norma ISO/IEC 27002:2013 en base a la matriz de riesgos elaborada, que satisfacen la necesidad del área de tecnológica de SWEADEN Seguros.

- Diseñar los controles de la política de seguridad para SWEADEN Seguros en base al análisis realizado a la norma ISO/IEC 27002:2013 que permita la mitigación de los riesgos asociados con las vulnerabilidades y amenazas de seguridad de la información existentes.

1.3 Justificación

La información es el activo más importante para una empresa luego de las personas, para ello la seguridad informática es un componente muy importante que considerar, la gestión y el tratamiento de este activo mediante la aplicación de procesos, políticas, procedimientos y controles logran mitigar los riesgos relacionados con el aseguramiento de los datos.

Actualmente el área de tecnología de SWEADEN Seguros cuenta con seis personas, cuatro de ellas se dedican a actividades específicas de desarrollo, y las operaciones de seguridad, infraestructura, soporte, y más son realizadas por el restante del personal, esto hace que la gestión de seguridades sea una tarea difícil de manejar.

De la información recolectada y analizada se puede notar que SWEADEN Seguros posee actualmente riesgos asociados con la seguridad de la información, esto se debe a la falta de políticas y controles de seguridad formales, como también a la falta de un responsable sobre la gestión de la seguridad, debilitando de esta manera la protección de un activo muy valioso como es la información.

Sin embargo, se verifica que la organización posee un manual de políticas de tecnologías, que si bien es cierto contiene un capítulo específico enfocado en la seguridad de la información, el mismo es básico por lo que se recomienda profundizar y especificar controles basados en una normativa internacional, además de protocolos que contribuyan a la gestión acertada para la protección real de información organizacional.

Para que SWEADEN Seguros garantice la confidencialidad, integridad y disponibilidad de su información, debería establecer mecanismos y controles seguros basados en normas y estándares internacionales que le permitan gestionar de manera segura el uso de la información y los recursos tecnológicos, considerando lo antes descrito se escoge el diseño de una política de seguridad de la información basado en la normativa ISO/IEC 27002:2013.

1.4 Estado del arte

Actualmente la seguridad de la información es un factor muy importante para cualquier organización, por lo que debe ser administrada de tal manera que permita controlar sus tres pilares fundamentales: su confidencialidad, integridad y disponibilidad. La protección de este activo es una tarea que las empresas privadas o públicas del Ecuador y del mundo tienen que considerar de manera oportuna para mantener seguras sus infraestructuras tecnológicas y por ende dar continuidad a sus procesos.

En la implementación de la Norma ISO/IEC 27002:2013 sección Control de Acceso para las aplicaciones informáticas de la Aseguradora del Sur (2016) realizado por Huacanés se menciona que: la utilización del estándar ISO 27002 permite aplicar procedimientos adecuados para establecer un acceso seguro a las aplicaciones y sistemas de la organización garantizando la seguridad de la información (pág. 26).

Por otra parte Suarez (2015) en sus tesis “ANÁLISIS Y DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA EN LA EMPRESA ASEGURADORA SUÁREZ

PADILLA & CÍA.LTDA" refiere que la falta de políticas y controles de seguridad para la información pueden afectar considerablemente a las organizaciones en la consecución de sus objetivos, sin embargo, un factor muy importante para la implementación de estas políticas y controles, es contar con el apoyo de la Alta Dirección de otro modo difícilmente se podrá contar con un esquema formal para la gestión de la seguridad de la información.

Para Garzón (2016), en su escrito "DESARROLLO DE UN PLAN DE RIESGOS DE SEGURIDAD PARA EL PROCESO DE EMISIÓN DE PÓLIZAS PARA UNA EMPRESA DE SEGUROS DEL ECUADOR, SIGUIENDO LA NORMA ISO 27001:2013" concluye que la gestión de seguridad de información es un sistema en el que se deben considerar ciertos puntos como: la concienciación y educación del personal en temas de seguridad, la aplicación de controles preventivos sobre los riesgos de la información, el involucramiento de la Alta Dirección para apoyar en el desarrollo en implementación de políticas de seguridad, en términos generales los sistemas de Gestión de Seguridad la Información proveen controles y medidas preventivas para controlar los riesgos y proteger los activos de información en las organizaciones.

Según Avellaneda (2014) en su escrito "Ciberseguridad, minuto y resultado: Los malos 3, Los buenos 0", desde su perspectiva como consultor de seguridad de la información menciona en forma de analogía a un partido de futbol, que en temas de seguridad Los Malos llevan 3 goles arriba en el marcador, pues bien nos comenta que el primer gol se marca en los primeros minutos del partido y se debe a que los fabricantes de software o desarrolladores generan productos inseguros, de ahí la importancia de la seguridad en el diseño para gestionar oportunamente las fallas o vulnerabilidades.

El segundo gol es a medio partido y se puede considerar como un autogol, pues su origen es la falta de importancia que las organizaciones le dan a sus áreas tecnológicas por la omisión o carencia del recurso humano y herramientas para contrarrestar las cyberamenazas que pueden afectar a la información.

En el tercer gol que es a final del partido se puede decir considerar como único mérito propio de los Malos, ya que corresponde a su esfuerzo para desarrollar amenazas de software comúnmente llamadas *malware* y que los dispositivos como *firewalls* o antivirus no puede detectar fácilmente.

Haciendo un análisis sobre la seguridad de la información en las empresas de seguros, ya sea en el mercado asegurador ecuatoriano o del mundo, se debe tener en cuenta que para la protección y mitigación de los riesgos asociados con la información es muy importante contemplar la implementación de esquemas de seguridad que garanticen el funcionamiento continuo de sus procesos organizacionales. Considerar normativas y estándares internacionales de seguridad posibilita que las empresas de seguros y de cualquier tipo puedan establecer mecanismos y procedimientos que permiten proteger su información, brindando seguridad a sus infraestructuras tecnológicas, generando confianza en sus clientes e involucrados, además de fomentar una cultura de seguridad digital.

CAPÍTULO II

MARCO TEÓRICO

2.1 Política de seguridad

Según Excellence (2018) una política de seguridad de la información no necesariamente debe contener todo sobre seguridad, ya que para la norma ISO/EIC 27001 esto no es una exigencia, una política de seguridad de la información es un documento organizacional y de tecnología que debe contemplar los objetivos que la institución quiere lograr en temas de seguridad, para con ello establecer los controles que le permitan administrar el Sistema de Gestión de Seguridad de la Información.

La política de seguridad debe cumplir con ciertos propósitos fundamentales y estos son:

- Una política de seguridad deberá ser acorde a la necesidad de cada organización es decir debe ser **adaptada** a su realidad.
- El **alcance** definido en la política de seguridad establecerá la capacidad del Sistema de Gestión de Seguridad de la Información (SGSI).
- Se debe establecer claramente las **responsabilidades** de los gestores del Sistema de Gestión de Seguridad de la Información.
- Se debe definir un marco para establecer los objetivos de seguridad de la información.
- El **compromiso de la alta dirección** es un factor decisivo para la implementación y aplicación de la política de seguridad.

- La política debe ser **socializada** dentro de la organización y a todos los involucrados.
- De nada sirve implementar una política de seguridad de la información si la misma no es **revisada y mejorada de manera continua**.

2.2 Seguridad de la información

Como menciona Soriano (2014) la seguridad de la información no solamente implica establecer controles para protegerse contra las amenazas: virus, ataques a la red o el spam en el correo electrónico. La seguridad de la información contempla el establecimiento y ejecución de procedimientos seguros y la aplicación de buenas prácticas que garanticen la protección sobre los sistemas de información, el control de accesos a dichos sistemas, con la finalidad de mantener protegidos los datos de la organización frente a las amenazas informáticas actuales.

Dicho esto, la seguridad de la información tiene como objetivo primordial asegurar sus tres dimensiones fundamentales: la disponibilidad, confidencialidad e integridad de la información.

2.3 Sistema de Gestión de la Seguridad de la Información (SGSI)

Según la ISO 27001 (2005) el SGSI "es parte del sistema de gestión general, que basa su enfoque en el riesgo del negocio para establecer, implementar, operar, monitorear, revisar y mejorar la seguridad de la información"

Por otra parte, la ISO/IEC (2018) menciona que en un SGSI se deben establecer las políticas, procedimientos, lineamientos, recursos y actividades asociadas para garantizar el aseguramiento de los activos de información en una organización.

2.4 Familias ISO

Según Pereira (2013) en su documento Plan de implementación de la norma ISO/IEC 27001 menciona que "La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC), esta serie contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y gestionar las especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI)".

2.4.1 NORMA ISO/IEC 27000

La Organización Internación de Estandarización ISO/IEC (2018) indica que la ISO 27000:2018 contempla una visión general de los sistemas de gestión de seguridad de la información (SGSI). También proporciona términos y definiciones que se usan comúnmente en la familia de estándares de SGSI. Este modelo es aplicable a todos los tipos y tamaños de empresas (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro).

2.4.2 NORMA ISO/IEC 27001

En el documento oficial de la ISO/IEC 27000 (2018) se indica que esta norma proporciona los requisitos normativos para el desarrollo y operación de un Sistema Gestor de Seguridad de la información (SGSI), además incluye un conjunto de objetivos de control y la mitigación de los riesgos asociados con los activos de información que la organización busca asegurar y proteger.

La norma ISO 27001 describe fundamentalmente como desarrollar un SGSI, basa su metodología de procesos adoptando el ciclo de mejora continua de Deming como se indica en la Figura 1, la misma que demuestra el cumplimiento de acciones o fases: "Panificar-Hacer-Verificar-Actuar" comúnmente conocida como (PHVA) o (PDCA) bajo sus siglas en inglés "*Plan-Do-Check-Act*"

Como indica Carvajal (2013) la figura 2 muestra un SGSI donde se cumplen cuatro niveles repetitivos que nunca terminan, inician por Planificar y terminan en Actuar, reciclando en mejoras continuas:

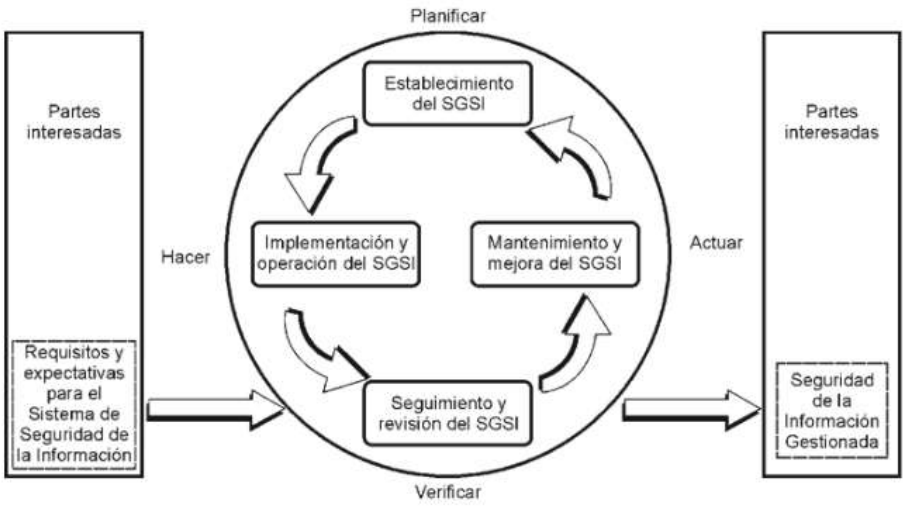


Figura 2 Ciclo de Deaming PDCA – PHVA
Fuente: Tomado de ISO 27002:2005

A continuación, en la Tabla 2 se describen los pasos a considerar en cada una de las fases del ciclo de mejora continua de Deaming para la implementación del SGSI.

Tabla 2 Fases ciclo de Deaming

Fase-Acción	Actividades
Planificar: Diseño del SGSI	- Definir alcance. - Identificar los riesgos de la información. - Analizar y evaluar los riesgos de la información. - Aceptación de riesgos. - Documentar la política (SGSI).
Hacer: Implementación y operación del SGSI	- Tratamiento de Riesgos. - Implementar procedimientos y controles para la gestión de la seguridad. - Manejo de Incidentes. - Planes de capacitación y concienciación a usuarios.
Verificar: Hacer Seguimiento y Revisar el SGSI	- Verificar el correcto funcionamiento de los controles de seguridad. - Medir la eficacia de los procedimientos controles de seguridad. - Ejecución de auditorías internas. - Actualización de los planes de contingencia y seguridad. - Comprobar el alcance del SGSI. - Auditorías de seguridad.
Actuar: Mantener y mejorar el SGSI	- Desarrollar las mejoras en el SGSI. - Implementar acciones correctivas y preventivas en el SGSI. - Socializar la política de seguridad con todos los involucrados.

Fuente: Tesis de Aliaga (2013)

2.4.3 NORMA ISO/IEC 27002:2013

Según (ISO/IEC, 2018) esta norma contiene un manual de buenas prácticas de seguridad en las que se describen los objetivos de control y las recomendaciones referentes a la seguridad de la información, con la particularidad de que no es certificable, su alcance y aplicación se adapta para todo tipo de empresas sean pequeñas como multinacionales.

La norma ISO/IEC 27002:2013 gestiona seguridad de la información mediante el cumplimiento a objetivos de control, los mismos que se clasifican en 14 dominios, 35 objetivos de control y 114 controles.

En la Tabla 3 se muestra los dominios de la norma ISO 27002:2013 con sus respectivos objetivos de control y cantidades de controles.

Tabla 3 Dominios y objetivos de control ISO 27002:2013

ÍTEMS	DOMINIOS	OBJETIVOS DE CONTROL	# CONTROLES
1	5. POLÍTICAS DE SEGURIDAD.	5.1 DIRECTRICES DE LA DIRECCIÓN EN SEGURIDAD DE LA INFORMACIÓN	2
2	6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.	6.1 ORGANIZACIÓN INTERNA	5
		6.2 DISPOSITIVOS PARA MOVILIDAD Y TELETRABAJO	2
3	7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	7.1 ANTES DE LA CONTRATACIÓN	2
		7.2 DURANTE LA CONTRATACIÓN	3
		7.3 CESE O CAMBIO DE PUESTO DE TRABAJO	1
4	8. GESTIÓN DE ACTIVOS.	8.1 RESPONSABILIDAD SOBRE LOS ACTIVOS	4
		8.2 CLASIFICACIÓN DE LA INFORMACIÓN	3
		8.3 MANEJO DE LOS SOPORTES DE ALMACENAMIENTO	3
5	9. CONTROL DE ACCESOS.	9.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS	2
		9.2 GESTIÓN DE ACCESO DE USUARIO	6

ÍTEMS	DOMINIOS	OBJETIVOS DE CONTROL	# CONTROLES
		9.3 RESPONSABILIDADES DEL USUARIO	1
		9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	5
6	10. CIFRADO.	10.1 CONTROLES CRIPTOGRÁFICOS	2
7	11. SEGURIDAD FÍSICA Y AMBIENTAL.	11.1 ÁREAS SEGURAS	6
		11.2 SEGURIDAD DE LOS EQUIPOS	9
8	12. SEGURIDAD EN LA OPERATIVA.	12.1 RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN	4
		12.2 PROTECCIÓN CONTRA CÓDIGO MALICIOSO	1
		12.3 COPIAS DE SEGURIDAD	1
		12.4 REGISTRO DE ACTIVIDAD Y SUPERVISIÓN	4
		12.5 CONTROL DEL SOFTWARE EN EXPLOTACIÓN	1
		12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA	2
		12.7 CONSIDERACIONES DE LAS AUDITORÍAS DE LOS SISTEMAS DE INFORMACIÓN	1
9	13. SEGURIDAD EN LAS TELECOMUNICACIONES.	13.1 GESTIÓN DE LA SEGURIDAD EN LAS REDES	3
		13.2 INTERCAMBIO DE INFORMACIÓN CON PARTES EXTERNAS	4
10	14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS	14.1 REQUISITOS DE SEGURIDAD DE LOS	3

ÍTEMS	DOMINIOS	OBJETIVOS DE CONTROL	# CONTROLES
	SISTEMAS DE INFORMACIÓN.	SISTEMAS DE INFORMACIÓN	
		14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE	9
		14.3 DATOS DE PRUEBA	1
11	15. RELACIONES CON SUMINISTRADORES.	15.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON SUMINISTRADORES	3
		15.2 GESTIÓN DE LA PRESTACIÓN DEL SERVICIO POR SUMINISTRADORES	2
12	16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	16.1 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS	7
13	17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	17.1 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	3
		17.2 REDUNDANCIAS	1
14	18. CUMPLIMIENTO.	18.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES	5
		18.2 REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN	3

Fuente: Enunciado adoptado de la Norma ISO 27002:2013 (Iso27000.es)

Tomando como referencia a Agustín López Neira y Javier Ruiz Spohr (2012) del portal www.iso27000.es, a continuación, se detalla de manera breve y general cada uno de los 14 dominios de la norma ISO/IEC 27002:2013.

Política de seguridad

Este dominio busca que exista un documento denominado política de seguridad en la organización, el mismo que proporciona una guía para que la dirección gestione la seguridad de la información en función a lo que la organización requiere.

Organización de la seguridad de la información

El objetivo de este dominio es establecer cómo se debe gestionar la seguridad de la información definiendo un esquema de asignación de funciones y responsabilidades en la organización.

Seguridad ligada a los Recursos Humanos

Es necesario establecer los procedimientos seguridad de la información antes, durante y después de la contratación del personal, este dominio permite definir los mecanismos para que los usuarios sepan de manera clara cuáles son sus responsabilidades y funciones que desarrollar.

Gestión de Activos

Se busca definir con precisión todos los activos (físicos, información, bases de datos, servicios y recursos informáticos) que posee la organización, para la adecuada administración de los riesgos de estos.

Control de acceso

Este dominio tiene como objetivo controlar el acceso a la información o sistemas mediante la implementación de mecanismos y procedimientos formales.

Cifrado

Se necesitan definir las técnicas y sistemas criptográficos para proteger la información garantizando las dimensiones de confidencialidad e integridad.

Seguridad física y ambiental

Este dominio de seguridad busca controlar el acceso no autorizado a las instalaciones físicas, prevenir daños o afectaciones a las instalaciones y a la información de la organización, mediante la implementación de perímetros de seguridad, control de factores ambientales, asegurando el correcto funcionamiento de los recursos para el procesamiento de la información.

Seguridad en la operativa

Se busca controlar la existencia de procedimientos de operación y responsabilidades debidamente aprobados por la dirección, para garantizar la seguridad en los recursos de procesamiento de información de la organización.

Seguridad en las telecomunicaciones

Gestionar adecuadamente el uso de los recursos de telemática que realizan el tratamiento de la información.

Adquisición, desarrollo y mantenimiento de los sistemas de información

A través de la implementación de controles de seguridad además de la definición de normas y procedimientos se debe asegurar que los sistemas de información cumplan con los estándares de seguridad deseados, esto aplica para la gestión del desarrollo propio y adquisición de software de terceros.

Relación con los suministradores

El objetivo es garantizar que los servicios entregados por terceros cumplan con los niveles de acuerdo y satisfagan los requerimientos que se contrataron.

Gestión de incidentes en la Seguridad de la información

Se busca asegurar que los sistemas de información cuenten con la debida protección ante los posibles eventos de seguridad y vulnerabilidades a los que están expuestos, el tratamiento y mitigación de estos riesgos se logra mediante una oportuna y proactiva gestión de la seguridad.

Gestión de la Continuidad del negocio

Es la capacidad para reaccionar ante los posibles eventos o fallas de seguridad que afectan a los sistemas y recursos críticos de información, mitigando las interrupciones por eventos naturales o amenazas del entorno.

Cumplimiento

El objetivo es asegurar que los procesos y sistemas que gestionan la información estén alineados a los reglamentos internos y las regulaciones de los organismos de controles estatales e internacionales, según sea el caso.

Dimensiones de la seguridad de la información

Las dimensiones de la seguridad de la información son:

- Disponibilidad
- Integridad
- Confidencialidad

Disponibilidad

Se entiende por disponibilidad de información a que los usuarios autorizados puedan hacer uso de los servicios o información con total normalidad en el horario que se requiera (INTECO, 2010).

La disponibilidad de la información lo que se busca es garantizar que los datos, las aplicaciones y los servicios tecnológicos estén disponibles para su consumo en los horarios que han sido establecidos.

Integridad

Buendía (2013) afirma que la integridad hace referencia a que los datos permanezcan almacenados tal y como el usuario espera además de esto la integridad asegura que los datos no sean alterados sin el consentimiento del propietario (pág. 15).

Confidencialidad

Buendía (2013) refiere que la confidencialidad intenta que la información sea utilizada únicamente por las personas autorizadas. Para que se garantice la confidencialidad es necesario tomar en cuenta las siguientes tres características o mecanismos:

Autenticación. Es validar que una máquina o una persona es quien dice ser, en otras palabras, garantiza que no se trate de un impostor o simulador.

Autorización. La autorización se da luego del proceso de autenticación y significa que un usuario pueda utilizar la información en función de los privilegios que se le han otorgado ni más ni menos, básicamente dos: solo lectura, o lectura y modificación.

Cifrado. Es el medio que permite blindar la información, supongamos la fase de autenticación es superada con el cifrado la información será inútil para un intruso.

Seguridad pasiva

Como lo indica Buendía (2013) en su libro Seguridad Informática la seguridad pasiva son los mecanismos que permiten una recuperación ante los ataques de una manera relativamente aceptable.

Seguridad activa

Así mismo Buendía (2013) indica que la seguridad activa busca adoptar medidas que protejan los activos empresariales como la información de los posibles ataques, dichas medidas pueden ser: cortafuegos, antivirus corporativos.

2.5 Metodología MAGERIT

Como menciona Rodríguez y Peralta (2013) MAGERIT es el acrónimo de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, fue elaborada por el Consejo Superior de Administración Electrónica de España, su estudio se basa en los riesgos que pueden afectar a los sistemas de información permitiendo la identificación de los riesgos y amenazas que acechan a los sistemas de información, para generar estrategias de prevención con la finalidad de garantizar la protección adecuada de la información.

Para resumir lo anteriormente mencionado se puede decir que es una metodología para conocer el riesgo al que está sometido la información y como esta es segura o insegura. MAGERIT es un método formal para identificar los riesgos que pueden soportar los sistemas de información, permitiendo adoptar las medidas apropiadas para la gestión y el control de riesgos.

2.5.1 Objetivos de MAGERIT

El Consejo Superior de Administración Electrónica (2012) menciona que MAGERIT contempla los siguientes objetivos:

Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos,
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

El análisis de riesgos es una aproximación metódica para determinar el riesgo tomando en cuenta las siguientes pautas:

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos.
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

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

2.5.1.1 Determinar los activos relevantes para la organización

El primer paso, es determinar los activos relevantes para la organización, por lo que existen dos cosas esenciales en un sistema de información:

- La **información** que maneja
- Los **servicios** que presta

La clasificación de los activos relevantes de la organización se detalla a continuación:

- **Datos** que materializan la información.
- **Servicios** auxiliares que se necesitan para poder organizar el sistema.
- **Las aplicaciones informáticas** (software) que permiten manejar los datos.
- **Los equipos informáticos** (hardware) y que permiten hospedar datos, aplicaciones y servicios.
- **Los soportes de información** que son dispositivos de almacenamiento de datos.
- **El equipamiento auxiliar** que complementa el material informático.
- **Las redes de comunicaciones** que permiten intercambiar datos.
- **Las instalaciones** que acogen equipos informáticos y de comunicaciones.
- **Las personas** que explotan u operan todos los elementos anteriormente citados.

Dependencias

Los activos esenciales son la información y los servicios prestados; pero estos activos dependen de otros activos más prosaicos como pueden ser los equipos, las comunicaciones, las instalaciones y las frecuentemente olvidadas personas que trabajan con aquellos.

Aunque en cada caso hay que adaptarse a la Organización objeto del análisis, con frecuencia se puede estructurar el conjunto de activos en capas, donde las capas superiores dependen de las inferiores:

- Activos esenciales
    - Información que se maneja
    - Servicios prestados
- Servicios internos
    - Que estructuran ordenadamente el sistema de información
- El equipamiento informático
    - Aplicaciones (software)
    - Equipos informáticos (hardware)
    - Comunicaciones
    - Soportes de información: discos, cintas, etc.
- El entorno: activos que se precisan para garantizar las siguientes capas
    - Equipamiento y suministros: energía, climatización, etc.
    - Mobiliario
- Los servicios subcontratados a terceros

- Las instalaciones físicas
- El personal
    - Usuarios
    - Operadores y administradores
    - Desarrolladores

Dimensiones

Se reconocen habitualmente como dimensiones de la seguridad de la información a la confidencialidad, integridad y disponibilidad no obstante en esta metodología se han añadido las características como: la autenticidad y el concepto de trazabilidad:

- Su **confidencialidad**: ¿Qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.
- Su **integridad**: ¿Qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o incluso faltar datos.
- Su **disponibilidad**: ¿Qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios.
- La **autenticidad**: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

  Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente consultar)
- La **trazabilidad del uso del servicio**: ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?

- La **trazabilidad del acceso a los datos**: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

Valoración de los activos

La valoración puede ser cuantitativa (con una cantidad numérica) o cualitativa (en alguna escala de niveles). Los criterios más importantes para considerar son:

- La **homogeneidad**: es importante poder comparar valores, aunque sean de diferentes dimensiones a fin de poder combinar valores propios y valores acumulados, así como poder determinar si es más grave el daño en una dimensión o en otra.
- La **relatividad**: es importante poder relativizar el valor de un activo en comparación con otros activos.

2.5.1.2 Determinar las amenazas a las que están expuestos los activos

En este siguiente paso, se necesita determinar las amenazas que puede afectar a los activos de la información.

Identificación de las amenazas

Las amenazas pueden ser de diferentes tipos:

a) **De origen natural:** Son los referentes a las catástrofes naturales como inundaciones o terremotos.
b) **Del entorno (de origen industrial)** Pueden ser desastres industriales como contaminación o fallos eléctricos.
c) **Defecto de las aplicaciones** Se pueden denominar como vulnerabilidades técnicas generadas en el diseño o implementación de los sistemas.

d) **Causadas por las personas de forma accidental** son amenazas ocasionadas en los sistemas de manera accidental por las personas típicamente por error u omisión.

e) **Causadas por las personas de forma deliberada** son amenazas ocasionadas en los sistemas de manera intencional por las personas, también pueden denominarse ataques; con ánimo de beneficiarse indebidamente o de causar daños.

Valoración de amenazas

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

a) **Degradación**: cuán perjudicado resultaría el valor del activo.

Tabla 4 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 raro	Muy raro	Extremadamente difícil

Fuente: Consejo Superior de Administración Electrónica, 2012, p.28 MAGERIT Libro I Versión 3

b) **Probabilidad**: cuán probable o improbable es que se materialice la amenaza.

Tabla 5 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

Fuente: Consejo Superior de Administración Electrónica, 2012, p.28 MAGERIT Libro I Versión 3

2.5.1.3 Determinar las salvaguardas

Se denominan salvaguardas a los procedimientos o mecanismos que reducen o mitigan el riesgo.

Para este paso, se seleccionan las salvaguardas adecuadas que se tienen que considerar:

a) Tipos de activos a proteger, ya que cada tipo se debe proteger específicamente.
b) Dimensión o dimensiones de seguridad que requieren protección.
c) Amenazas de las que necesitamos protegernos.
d) Si existen salvaguardas alternativas.

Además, es prudente establecer un principio de proporcionalidad y tener en cuenta:

a) El mayor o menor valor propio o acumulado sobre un activo, centrándonos en lo más valioso y obviando lo irrelevante.
b) La mayor o menor probabilidad de que una amenaza ocurra, centrándonos en los riesgos más importantes.
c) La cobertura del riesgo que proporcionan salvaguardas alternativas.

Esto lleva a dos tipos de declaraciones para excluir una cierta salvaguarda del conjunto de las que conviene analizar:

No aplica: se dictamina cuando una salvaguarda no es de aplicación porque técnicamente no es adecuada al tipo de activos a proteger, no protege la dimensión necesaria o no protege frente a la amenaza en consideración

No se justifica: se dice cuando la salvaguarda aplica, pero es desproporcionada al riesgo que tenemos que proteger.

2.5.1.4 Estimar el impacto

Se define como el daño sobre el activo derivado de la materialización de la amenaza

Sea la escala siguiente útil para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo:

- **MB:** muy bajo
- **B:** bajo
- **M:** medio
- **A:** alto
- **MA:** muy alto

Se puede calcular el impacto en base a tablas sencillas de doble entrada tal como se muestra a continuación:

Tabla 6 Estimación del Impacto

impacto		*degradación*		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Fuente: Consejo Superior de Administración Electrónica, 2012, p.6 Libro MAGERIT III Versión 3

Como se puede ver en la Tabla 6 los activos con una calificación de impacto MA es decir Muy Alto serán objetos de atención inmediata.

2.5.1.5 Estimar el riesgo

La estimación del riesgo se define como el impacto ponderado con la tasa de ocurrencia de la amenaza.

Para la estimación del riesgo se modelan impacto, probabilidad y riesgo por medio de escalas cualitativas de tal modo como se muestra en la Figura 3:

escalas		
impacto	probabilidad	riesgo
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB:** muy raro	**MB:** despreciable

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 Escala cualitativa - Estimación del Riesgo
Fuente: Consejo Superior de Administración Electrónica, 2012, p.7 Libro MAGERIT III Versión 3

CAPÍTULO III

ANÁLISIS SITUACIONAL

SWEADEN Seguros S.A.

SWEADEN Seguros es una sociedad anónima ecuatoriana con domicilio principal en el Distrito Metropolitano de Quito, está sometida al control y vigilancia de La Superintendencia de Compañías, Valores y Seguros del Ecuador, su objeto social está relacionado con la comercialización de seguros en los ramos vida y patrimoniales, fue constituida el 04 de septiembre de 2007 y fue aprobada mediante Resolución No. 774 el 13 de septiembre de 2007 por la Superintendente de Bancos y Seguros en ese momento, fue inscrita en el Registro Mercantil con fecha 1 de octubre de 2007 (SWEADEN, s.f.).

Misión

"Asumir riesgos con profesionalismo para que la sociedad y nuestros colaboradores se sientan seguros" (SWEADEN, s.f.).

Visión

"Líderes en Sudamérica en el mercado asegurador, con la mejor rentabilidad, imagen, ética y servicio. Queremos hacer de SWEADEN la Compañía donde todos quieran pertenecer" (SWEADEN, s.f.).

Estructura organizacional

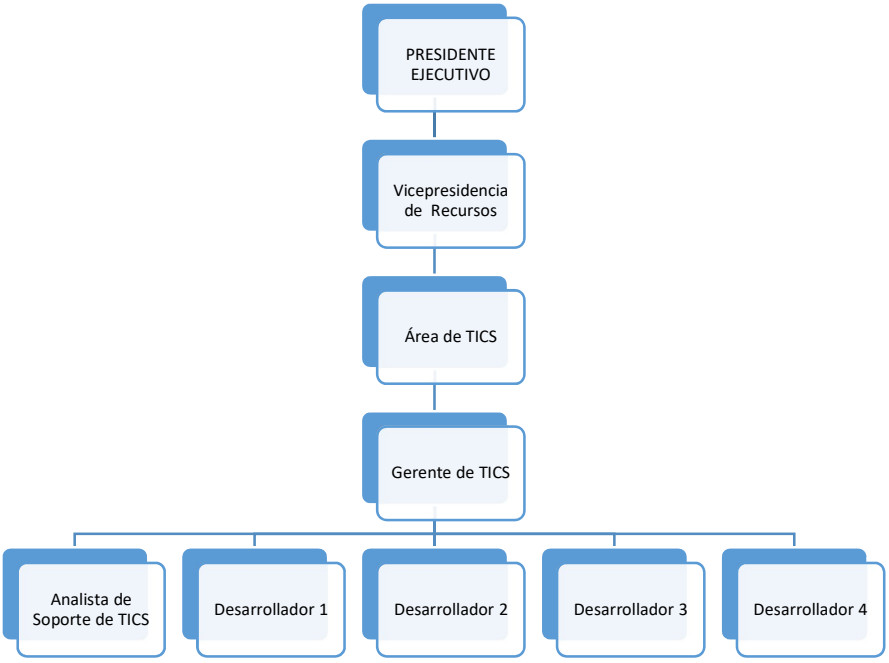


Figura 4 Organigrama institucional
Fuente: Organigrama SWEADEN Seguros

Como se puede observar en el organigrama de la organización el área de TICs está bajo la responsabilidad del coordinador de TICs quien a su vez reporta a la Vicepresidencia de recursos, por lo que las operaciones de tecnología recaen sobre seis personas: cuatro de estas se encargan del desarrollo y mantenimiento de los sistemas para la organización, una persona realiza operaciones de soporte y el restante ejecuta operaciones gerenciales, de infraestructura y seguridades, esto demuestra que la gestión de la seguridad es una falencia en la organización ya que se carece de un esquema adecuado que permita la segregación de funciones para el tratamiento y gestión de la seguridad de manera independiente.

Análisis y valoración de riesgos

Si bien es cierto se puede evidenciar que actualmente la organización y específicamente el área de TICs posee documentación referente a la gestión de la información (plan estratégico de tecnologías, manual de políticas de tecnologías y plan de contingencias) todos debidamente aprobados por la Dirección, no obstante consideran que es necesario desarrollar una política de seguridad de la información basado en la norma ISO/IEC 27002:2013, con el objetivo asegurar la confidencialidad, integridad y disponibilidad de la misma.

Para esto es necesario analizar, identificar amenazas y vulnerabilidades a la que está expuesta la información mediante una matriz de riesgos por lo que se recomienda considerar al menos una las metodologías existentes.

En la actualidad existen varias metodologías que permiten analizar y valorar riesgos informáticos (OCATVE, MAGERIT, MEHARI, EBIOS, CRAMM, CORAS) cada una tiene ventajas y desventajas; no obstante, se debe optar por la que más se adapte a las necesidades de la organización.

Para este proyecto se ha escogido la metodología MAGERIT ya que proporciona un método sistemático y ordenado para el análisis de riesgos relacionados con el uso de tecnologías, el objetivo es mitigar las amenazas y vulnerabilidades mediante la implementación de medidas preventivas y controles.

3.1 Empleando la metodología MAGERIT

MAGERIT (2012) indica que para el análisis y valoración de riesgos se deben seguir los siguientes pasos:

a) Identificación de activos de información
b) Identificación de amenazas y vulnerabilidades
c) Identificación de las salvaguardas existentes
d) Estimación de impacto
e) Estimación del riesgo

Sin embargo, para el análisis y valoración de riesgos SWEADEN Seguros procede a contemplar los pasos en el siguiente orden:

a) Identificación de activos de información
b) Identificación de amenazas y vulnerabilidades
c) Estimación de impacto
d) Estimación del riesgo
e) Identificación de las salvaguardas existentes

3.1.1 Identificación de los activos de información

Tal como indica la metodología de análisis de riesgos MAGERIT, la selección clara de los activos de información a protegerse es fundamental para la correcta implementación de un SGSI ya que estos constituyen un factor muy importante para garantizar las operaciones del negocio y su continuidad, para llevar a cabo esta actividad es necesario apoyarse de los involucrados o

responsables, en este caso la Dirección de SWEADEN Seguros ha designado como responsable de esta tarea al coordinador del área de TICs.

Una vez definido el responsable se procede con la entrevista al coordinador del área de TICs de la organización para recopilar información que ayude con la identificación de los activos a protegerse, para esta selección es muy importante considerar las actividades que realiza y gestiona el área de TICs de SWEADEN, las mismas que se clasifican en propias y compartidas con terceros o proveedores como se muestra a continuación en la Tabla 7.

Tabla 7 Actividades de TI y Terceros SWEADEN

Actividad	**Ejecuta**
Desarrollo In House - Desarrollo del sistema SIA (Core Principal) sólo de uso interno	TICs SWEADEN
Desarrollo In House - Desarrollo del sistema SisWeb (Sistema Web) sistema para asesores, de uso externo	TICs SWEADEN
Desarrollo In House - Desarrollo del sistema Diamante (Cliente-Servidor) Sólo de uso interno)	TICs SWEADEN
Mantenimiento Correctivo y preventivo de equipos	TICs SWEADEN
Comunicaciones	PROVEEDOR
Seguridad perimetral	PROVEEDOR
Seguridad local – *EndPoint*	TICs SWEADEN
Administración y mantenimiento de Servidores	TICs SWEADEN
Documentación de políticas y planes de contingencias	TICs SWEADEN
Respaldos críticos: Se realizan en nube privada, no hay redundancia.	TICs SWEADEN

Fuente: SWEADEN - Entrevista al coordinador de TI

Adicionalmente el coordinador del área de TICs de SWEADEN manifiesta que existen observaciones de auditorías realizadas en la organización, de esta información se considera los puntos que directamente se relacionan con la seguridad de la información y que a continuación se detallan en la siguiente tabla:

Tabla 8 Observaciones Auditoría Externa

Observación	Riesgo
El acceso al Data Center debe contar con una puerta de metal blindado con un panel digital, para permitir el ingreso al personal autorizado.	Alto
La organización deberá controlar el acceso a la red, para lo cual será necesario implementar un Controlador de Dominio (Directorio Activo)	Alto

Fuente: Auditoría SWEADEN 2018, entrevista al coordinador de TICs

A más de la entrevista con el coordinador de TICs de SWEADEN Seguros, se realizaron encuestas online a todo el personal de la organización con la finalidad de recopilar información que permita conocer el nivel de conciencia en temas de seguridad y protección.

Las preguntas que se contemplaron en la encuesta se muestran en la tabla 9 con sus respectivos resultados:

Tabla 9 Encuesta de seguridad y protección de la información

#	PREGUNTA	SI	NO	RESPUESTA
P1	¿Conoces qué es una contraseña fuerte?	85.71%	14.29%	
P2	¿Conoces qué es un sistema de autenticación de doble factor?	15.87%	84.13%	
P3	¿Existe un departamento o encargado de seguridad informática en la organización?	73.02%	26.98%	
P4	¿Realizas copias de seguridad de tu información?	49.21%	50.79%	
P5	¿Crees que es mejor tener una misma contraseña	25.40%	74.60%	

#	PREGUNTA	SI	NO	RESPUESTA
	para todas tus cuentas?			
P6	¿A qué considerarías Phishing?	80.95%	19.05%	A una técnica de hackeo que busca robar las contraseñas de los usuarios
P7	Tienes una cuenta de ahorros en **MiBanco** y te llega un correo de info@mibancos.ec donde te avisan de que hay una nueva web donde cambiar las claves:	N/A	N/A	Nunca el banco no pide cambios de claves.
P8	¿Qué navegador web utilizas normalmente?	N/A	N/A	Chrome
P9	¿Tienes software antivirus instalado en tu computador?	77.78%	22.22%	
P10	¿Crees que es necesario una inducción sobre seguridad informática en la organización?	100%	0%	

Fuente: Elaborado por el investigador

De la información obtenida con la encuesta realizada se puede evidenciar que el personal de la organización tiene un conocimiento básico relacionado con temas de seguridad informática además de que considera necesario una inducción sobre el tema.

Luego de recopilar la información y con el apoyo del coordinador del área de TICs de SWEADEN Seguros se identifican los activos de información más relevantes, para ello se toma como referencia la metodología de análisis de riesgos indicada en el Libro II MAGERIT Versión 3 Catálogo de Elementos, estos activos se clasifican de la siguiente manera:

Tabla 10 Activos de información SWEADEN Seguros

Tipo de Activo	Descripción	Código
[D] Datos / Información	Código fuente Sistema SIA DIAMANTE SISWEB	*[source]*
	Base Datos Sistemas: SIA, DIAMANTE, SISWEB	*[files]*
	NAS	*[backup]*
[S] Servicios	Correo electrónico corporativo	*[email]*
[SW] Software - Aplicaciones informáticas	Aplicaciones De desarrollo In House SIA, DIAMANTE, SISWEB	*[exe]*
	Ofimática	*[office]*
	Gestor de máquinas virtuales	*[hypervisor]*
[HW] Equipamiento informático (hardware)	Servidores de Virtualización	*[host]*
	Switchs	*[switch]*
[L] Instalaciones.	Datacenter	*[site]*
[PERSONAL] Personal	Administrador de sistema SIA	*[adm]*
	Desarrolladores / programadores	*[des]*

Fuente: (Consejo Superior de Administración Electrónica, 2012) Libro II MAGERIT versión 3

Según el Consejo Superior de Administración Electrónica (2012) para la valoración de un activo debe considerarse la perspectiva que responda a la 'necesidad de proteger' es decir si un activo es significativamente valioso para la organización, el nivel de protección deberá ser mayor.

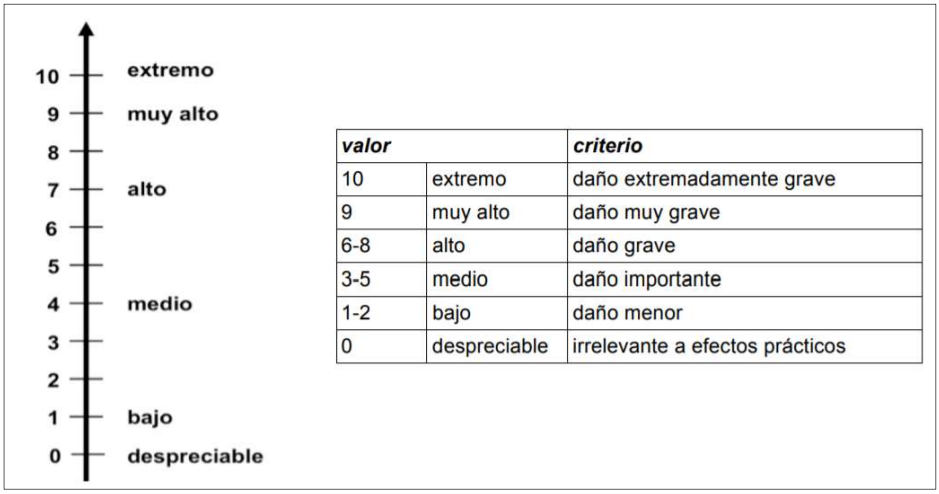
La valoración de un activo de información se debe calibrar en las siguientes dimensiones:

Confidencialidad: Busca garantizar que la información no se exponga a personas o procesos no autorizados.

Integridad: Garantiza que los datos permanezcan intactos, las modificaciones deben ser realizadas únicamente por personas o procesos autorizados.

Disponibilidad: Garantiza que los servicios y la información estén siempre disponibles cuando se los requiere.

Como menciona el Consejo Superior de Administración Electrónica (2012) para la valoración de los activos se maneja una escala de diez valores dejando la escala cero como un valor despreciable en cuanto a efectos de riesgo se refiere, sin embargo, la escala se puede simplificar si el análisis de riesgo es de manera menos detallada. Estas escalas se ven representadas en la siguiente figura:



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 5 Escala para análisis de riesgo
Fuente: Consejo Superior de Administración Electrónica, 2012, p.19 Libro MAGERIT II Versión 3

Como lo indica el Consejo Superior de Administración Electrónica (2012) las características que hacen valioso a un activo son la confidencialidad, integridad y disponibilidad, para ello SWEADEN Seguros ha establecido una escala cualitativa y una cuantitativa de manera simplificada la misma que contiene 5 niveles en donde el nivel cero representa pérdidas nulas o despreciables para el área de TICs:

Tabla 11 Criterios de seguridad para la valoración de los activos

Criterio	Valor	Confidencialidad	Integridad	Disponibilidad
Extremo	5	¿Qué daño causaría si se divulgara quien no debe?	¿Qué daño causaría si estuviera dañado o corrupto?	¿Qué perjuicio causaría si no estuviera disponible?
Muy Alto	4			
Alto	3			
Medio	2			
Bajo	1			
Despreciable	0			

Fuente: Consejo Superior de Administración Electrónica, 2012, p.19 Libro MAGERIT II Versión 3

En la Tabla 12 se puede visualizar la valoración de los activos de información más relevantes para SWEADEN Seguros considerando las dimensiones de Confidencialidad, Integridad y Disponibilidad.

Tabla 12 Activos de información de SWEADEN Seguros

Tipo de Activo	Descripción	Código	Confidencialidad	Integridad	Disponibilidad	Promedio	Valor
[D] Datos / Información	Código fuente Sistemas SIA, DIAMANTE, SISWEB	[*source*]	5	5	5	5	**Extremo**
	Base Datos Sistemas: SIA, DIAMANTE, SISWEB	[*files*]	5	5	5	5	**Extremo**
	NAS	[*backup*]	3	3	3	3	**Alto**
[S] Servicios	Correo electrónico corporativo	[*email*]	3	3	3	3	**Alto**
[SW] Software - Aplicaciones informáticas	SIA, DIAMANTE, SISWEB	[*exe*]	5	5	5	5	**Extremo**
	Ofimática	[*office*]	1	1	2	1	**Bajo**
	Gestor de máquinas virtuales	[*hypervisor*]	3	3	3	3	**Alto**
[HW] Equipamiento informático (hardware)	Servidores de Virtualización	[*host*]	5	5	5	5	**Extremo**
	Equipos de escritorio	[*host*]	3	2	3	3	**Medio**
	Equipos portátiles	[*mobile*]	3	2	2	2	**Medio**
	Switchs	[*switch*]	1	1	1	1	**Bajo**
[L] Instalaciones.	Datacenter	[*site*]	4	4	5	4	**Muy Alto**
[PERSONAL] Personal	Administradores de sistemas SIA, DIAMANTE, SISWEB	[*adm*]	5	5	5	5	**Extremo**
	Desarrolladores / programadores	[*des*]	4	4	4	4	**Muy Alto**

Fuente: Elaborado por el investigador, basándose en metodología MAGERIT Versión 3

Para la valoración de los activos antes descritos se toma en consideración el apoyo del coordinador de TICs de SWEADEN.

3.1.2 Identificación de las amenazas

MAGERIT sugiere la división de las amenazas sobre cada uno de los activos de la siguiente manera:

Tabla 13 Clasificación de las amenazas según MAGERIT

Amenaza	Origen	Descripción
[N] Desastres naturales	Natural	Causas por desastres naturales (Inundaciones, Terremotos), no necesariamente por sin intervención del ser humano.
[I] De origen industrial	Entorno Humano	Causas de tipo industrial, provocadas por el ser humano o de manera accidental (Interrupciones Eléctricas, Explosiones).
[E] Errores y fallos no intencionados	Humano	Sucesos ocasionados por el ser humano de manera no intencional (Errores de programación de sistemas, omisión de procesos).
[A] Ataques intencionados	Humano	Sucesos provocados por el ser humano de manera intencional (Ataques de hackers)

Fuente: Consejo Superior de Administración Electrónica, 2012, Libro MAGERIT II Versión 3 Pág. 25-47

Considerando la clasificación anterior, se procede con la identificación de las amenazas y sus vulnerabilidades para cada uno de los activos ya seleccionados.

[D] Datos / Información

Tabla 14 Amenazas y vulnerabilidades de código fuente de los sistemas

Secuencia	Activo	Código	Amenaza	Vulnerabilidad	Dimensión de seguridad afectada
1	[D] Código fuente de los Sistemas SIA, DIAMANTE, SISWEB	E.2	Errores del administrador	Falta de manuales, instructivos y capacitación en manejo de los sistemas	[C] Confidencialidad [I] Integridad [D] Disponibilidad
2		E.15	Alteración accidental de la información	Falta de control en la gestión del cambio	[I] Integridad
3		E.18	Destrucción de información	Falencia en la gestión de respaldos de código fuente	[D] Disponibilidad
4		E.19	Fugas de información	Falta de control en el acceso al código fuente y al término de la relación laboral	[C] confidencialidad
5		A.6	Abuso de privilegios de acceso	Fallas de controles en el acceso	[C] Confidencialidad [I] Integridad [D] Disponibilidad
6		A.11	Acceso no autorizado	Fallas en el control de acceso	[C] Confidencialidad [I] Integridad
7		A.18	Destrucción de información	Falta de controles en la gestión de respaldos	[D] Disponibilidad
8		A.19	Divulgación de información	Falta de control al término de la relación laboral.	[C] confidencialidad
1	[D] Base Datos Sistemas: SIA, DIAMANTE, SISWEB	E.1	Errores de los usuarios	Falta de manuales, instructivos y capacitación en manejo de los sistemas	[C] Confidencialidad [I] Integridad [D] Disponibilidad
2		E.2	Errores del administrador	Falta de segregación de funciones.	[C] Confidencialidad [I] Integridad [D] Disponibilidad
3		E.15	Alteración accidental de la información	Falta de controles y privilegios en la DB	[I] Integridad
4		E.18	Destrucción de información	Falta de controles en la gestión de respaldos	[D] Disponibilidad
5		E.19	Fugas de información	Falta de contratos de confidencialidad	[C] Confidencialidad
6		A.6	Abuso de privilegios de acceso	Fallas en el control de acceso	[C] Confidencialidad [I] Integridad

Secuencia	Activo	Código	Amenaza	Vulnerabilidad	Dimensión de seguridad afectada
7		A.11	Acceso no autorizado	Fallas en el control de acceso	[D] Disponibilidad [C] Confidencialidad [I] Integridad
8		A.15	Modificación deliberada de la información	Fallas en el control de acceso	[I] Integridad
9		A.18	Destrucción de información	Falta de controles en la gestión de respaldos	[D] Disponibilidad
10		A.19	Divulgación de información	Falta de contratos de confidencialidad	[C] Confidencialidad
1	[D] NAS	E.1	Errores de los usuarios	Falta de manuales, instructivos y capacitación en manejo de los sistemas	[I] Integridad [C] Confidencialidad [D] Disponibilidad
2		E.2	Errores del administrador	Falta de capacitación en el manejo del sistema	[I] Integridad [C] Confidencialidad [D] Disponibilidad
3		E.15	Alteración accidental de la información	Falta de control en la segregación de privilegios	[I] Integridad
4		E.18	Destrucción de información	Falta de control en la segregación de privilegios	[D] Disponibilidad
5		E.19	Fugas de información	Falta de controles en la desvinculación o cese del cargo	[C] Confidencialidad
6		A.6	Abuso de privilegios de acceso	Falta de control en la asignación de privilegios	[I] Integridad [C] Confidencialidad [D] Disponibilidad
7		A.11	Acceso no autorizado	Fallas en el control de acceso	[I] Integridad [C] Confidencialidad
8		A.15	Modificación deliberada de la información	Fallas en el control de acceso	[I] Integridad
9		A.18	Destrucción de información	Falta de controles en la gestión de respaldos	[D] Disponibilidad
10		A.19	Divulgación de información	Falta de contratos de confidencialidad.	[C] Confidencialidad

Fuente: Elaborado por el investigador, basándose en metodología MAGERIT Versión 3

[S] Servicios

Tabla 15 Amenazas y vulnerabilidades de los servicios

Secuencia	Activo	Código	Amenaza	Vulnerabilidad	Dimensión de seguridad afectada
1	[S] Correo Electrónico corporativo	E.1	Errores de los usuarios	Falta de manuales, instructivos y capacitación en manejo de los sistemas	[C] Confidencialidad [I] Integridad [D] Disponibilidad
2		E.2	Errores del administrador	Falta de manuales, instructivos y capacitación en manejo de los sistemas	[C] Confidencialidad [I] Integridad [D] Disponibilidad
3		E.9	Errores de [re-]encaminamiento	Falta de contratos de confidencialidad	[C] Confidencialidad
4		E.15	Alteración accidental de la información	Falta de manuales, instructivos y capacitación en manejo de los sistemas	[I] Integridad
5		E.18	Destrucción de información	Falta de contratos de confidencialidad	[D] Disponibilidad
6		E.19	Fugas de información	Falta de contratos de confidencialidad	[C] confidencialidad
7		E.24	Caída del sistema por agotamiento de recursos	Falta de controles de Denegación de servicio	[D] Disponibilidad
8		A.5	Suplantación de la identidad del usuario	Falta de controles Antispam	[C] Confidencialidad [A] Autenticidad [I] Integridad
9		A.6	Abuso de privilegios de acceso	Falta de control en la segregación de privilegios	[C] Confidencialidad [I] Integridad [D] Disponibilidad
10		A.7	Uso no previsto	Falta de controles en el manejo del correo electrónico	[C] Confidencialidad [I] Integridad [D] Disponibilidad
11		A.11	Acceso no autorizado	Fallas en el control de acceso	[I] Integridad [C] Confidencialidad
12		A.13	Repudio	Falta de controles de auditoría	[I] Integridad
13		A.14	Destrucción de información	Falta de controles en la vinculación, desvinculación o cambio de cargo.	[D] Disponibilidad

Secuencia	Activo	Código	Amenaza	Vulnerabilidad	Dimensión de seguridad afectada
14		A.19	Divulgación de información	Falta de controles en la vinculación, desvinculación o cambio de cargo.	[C] confidencialidad
15		A.24	Denegación de servicio	Falta de controles de Denegación de servicio	[D] disponibilidad

Fuente: Elaborado por el investigador, basándose en metodología MAGERIT Versión 3

[SW] Software - Aplicaciones informáticas

Tabla 16 Amenazas y vulnerabilidades de las aplicaciones

Secuencia	Activo	Código	Amenaza	Vulnerabilidad	Dimensión de seguridad afectada
1	[SW] De desarrollo In House: SIA, DIAMANTE, SISWEB	I.5	Avería de origen físico o lógico	Falta de controles en las pruebas del Software resultante	[D] disponibilidad
2		E.1	Errores de los usuarios	Falta de manuales, instructivos y capacitación en manejo de los sistemas	[I] Integridad [D] Disponibilidad [C] Confidencialidad
3		E.20	Vulnerabilidades de los programas (software)	Falta de controles en las pruebas del Software resultante	[C] Confidencialidad [I] Integridad [D] Disponibilidad
4		E.21	Errores de mantenimiento / actualización de programas (software)	Falta de controles en la gestión del cambio	[I] Integridad [D] Disponibilidad
5		A.5	Suplantación de la identidad del usuario	Fallas en el control de acceso	[C] Confidencialidad [A] autenticidad [I] Integridad
6		A.6	Abuso de privilegios de acceso	Falta de control en la segregación de privilegios	[I] Integridad [D] Disponibilidad [C] Confidencialidad
7		A.11	Acceso no autorizado	Falta de control de acceso en los ambientes de producción	[I] Integridad [C] Confidencialidad
8		A.22	Manipulación de programas	Falta de controles en la gestión del cambio	[I] Integridad [D] Disponibilidad [C] Confidencialidad

Fuente: Elaborado por el investigador, basándose en metodología MAGERIT Versión 3

[HW] Equipamiento informático (hardware)

Tabla 17 Amenazas y vulnerabilidades de servidores de virtualización

Secuencia	Activo	Código	Amenaza	Vulnerabilidad	Dimensión de seguridad afectada
1	[HW] Servidores de Virtualización	N.1	Fuego	Falta de controles de seguridad contra incendio automatizados.	[D] Disponibilidad
2		N.2	Daños por agua	Falta de controles de seguridad ambiental	[D] Disponibilidad
3		N.*	Desastres naturales	Falta de planes de contingencia, *Disaster Recovery Plan*	[D] Disponibilidad
4		I.6	Corte del suministro eléctrico	Falta de contingente eléctrico.	[D] Disponibilidad
5		I.7	Condiciones inadecuadas de temperatura o humedad	Falta de controles de seguridad ambiental	[D] Disponibilidad [I] Integridad
6		E.24	Caída del sistema por agotamiento de recursos	Falta de controles de Denegación de servicios	[D] Disponibilidad [C] Confidencialidad
7		E.25	Pérdida de equipos	Falta de planes de contingencia, *Disaster Recovery Plan*	[D] Disponibilidad [C] Confidencialidad
8		A.11	Acceso no autorizado	Falta de controles de seguridad física	[I] Integridad [C] Confidencialidad
9		A.23	Manipulación de los equipos	Falta de controles de seguridad física	[D] Disponibilidad [C] Confidencialidad
10		A.25	Robo	Falta de controles de seguridad física	[D] Disponibilidad [C] Confidencialidad
11		A.26	Ataque destructivo	Falta de planes de contingencia, *Disaster Recovery Plan*	[D] Disponibilidad
1	[HW] Equipos de escritorio	I.5	Avería de origen físico o lógico	Fallas en el funcionamiento del hardware	[D] Disponibilidad
2		I.6	Corte del suministro eléctrico	Falta de suministro de energía de respaldo	[D] Disponibilidad
3		E.2	Errores del administrador	Falta de antivirus	[I] Integridad [D] Disponibilidad [C] Confidencialidad
4		E.2	Errores del administrador	Falta de mantenimiento de equipos	[I] Integridad [D] Disponibilidad [C] Confidencialidad
5		E.2	Errores del administrador	Falta de Control en unidades extraíbles (USB)	[I] Integridad [D] Disponibilidad [C] Confidencialidad

Secuencia	Activo	Código	Amenaza	Vulnerabilidad	Dimensión de seguridad afectada
6		A.7	Uso no previsto	Falta de controles en el manejo de los equipos	[I] Integridad [D] Disponibilidad [C] Confidencialidad
7		A.11	Acceso no autorizado	Fallas en el control de acceso	[I] Integridad [C] Confidencialidad
1	[HW] Equipos Portátiles	I.5	Avería de origen físico o lógico	Fallas en el hardware	[D] Disponibilidad
2		E.2	Errores del administrador	Falta de antivirus	[I] Integridad [D] Disponibilidad [C] Confidencialidad
3		E.2	Errores del administrador	Falta de mantenimiento en los equipos	[I] Integridad [D] Disponibilidad [C] Confidencialidad
4		E.2	Errores del administrador	Falta de Control en unidades extraíbles (USB)	[I] Integridad [D] Disponibilidad [C] Confidencialidad
5		E.25	Pérdida de equipos	Robo de equipo	[D] Disponibilidad [C] Confidencialidad
6		A.7	Uso no previsto	Falta de controles en el manejo de los equipos	[I] Integridad [D] Disponibilidad [C] Confidencialidad
7		A.11	Acceso no autorizado	Fallas en el control de acceso	[I] Integridad [C] Confidencialidad
8		A.25	Robo	Robo de equipo	[D] Disponibilidad [C] Confidencialidad

Fuente: Elaborado por el investigador, basándose en metodología MAGERIT Versión 3

[L] Instalaciones

Tabla 18 Amenazas y vulnerabilidades de las Instalaciones

Secuencia	Activo	Código	Amenaza	Vulnerabilidad	Dimensión de seguridad afectada
1	[L] Datacenter	N.1	Fuego	Falta de controles de seguridad contra incendio automatizados.	[D] Disponibilidad
2		N.2	Daños por agua	Falta de controles de seguridad ambiental	[D] Disponibilidad
3		N.*	Desastres naturales	Falta de planes de contingencia, *Disaster Recovery Plan*	[D] Disponibilidad
4		I.6	Corte del suministro eléctrico	Falta de contingente eléctrico.	[D] Disponibilidad
5		I.7	Condiciones inadecuadas de temperatura o humedad	Falta de controles de seguridad ambiental	[D] Disponibilidad [I] Integridad
6		A.11	Acceso no autorizado	Falta de controles de seguridad física	[I] Integridad [C] Confidencialidad
7		A.23	Manipulación de los equipos	Falta de controles de seguridad física	[D] Disponibilidad [C] Confidencialidad
8		A.25	Robo	Falta de controles de seguridad física	[D] Disponibilidad [C] Confidencialidad
9		A.26	Ataque destructivo	Falta de planes de contingencia, *Disaster Recovery Plan*	[D] Disponibilidad

Fuente: Elaborado por el investigador, basándose en metodología MAGERIT Versión 3

[PERSONAL] Personal

Tabla 19 Amenazas y vulnerabilidades del Personal

Secuencia	Activo	Código	Amenaza	Vulnerabilidad	Dimensión de seguridad afectada
1	[PERSONAL] Administradores de sistemas SIA, DIAMANTE, SISWEB	E.7	Deficiencias en la organización	Falta de segregación de funciones	[D] Disponibilidad
2		E.19	Fugas de información	Falta de contratos de confidencialidad en la desvinculación	[C] Confidencialidad
3		E.30	Ingeniería social	Falta de capacitación en seguridades	[C] Confidencialidad [I] Integridad [D] Disponibilidad
1	[PERSONAL] Desarrolladores / programadores y DBA	E.7	Deficiencias en la organización	Falta de segregación de funciones	[D] Disponibilidad
2		E.19	Fugas de información	Falta de contratos de confidencialidad en la desvinculación	[C] Confidencialidad
3		E.30	Ingeniería social	Falta de capacitación en seguridades	[C] Confidencialidad [I] Integridad [D] Disponibilidad

Fuente: Elaborado por el investigador, basándose en metodología MAGERIT V3

3.1.3 Estimación del impacto

En esta instancia se tiene que valorar la influencia y afectación de cada amenaza sobre el activo, para ello se basa en lo que dice MAGERIT y se establecen dos escalas una para representar la degradación y otra para la probabilidad.

Degradación: Su estimación se basa en que tanto ha sido perjudicado o afectado el activo.

Tabla 20 Degradación del valor

5	100%	MA	Muy Alta	Casi seguro	Fácil
4	90%	A	Alta	Muy alta	Medio
3	50%	M	Media	Posible	Difícil
2	10%	B	Baja	Poco probable	Muy difícil
1	1%	MB	Muy Baja	Muy raro	Extremadamente difícil

Fuente: Consejo Superior de Administración Electrónica, 2012, p.28 Libro MAGERIT I Versión 3

Probabilidad: Su estimación se basa en cada cuanto se puede materializar una amenaza sobre el activo.

Tabla 21 Probabilidad de ocurrencia

5	100%	MA	Muy frecuente	A diario
4	90%	A	Frecuente	Mensualmente
3	50%	M	Normal	Una vez al año
2	10%	B	Poco frecuente	Cada varios años
1	1%	MB	Muy poco frecuente	Siglos

Fuente: Consejo Superior de Administración Electrónica, 2012, p.28 Libro MAGERIT I Versión 3

Para calcular el impacto en los activos se utilizan las dos variables: degradación y probabilidad tal como se puede apreciar en la siguiente tabla:

Tabla 22 Matriz de calor para la estimación del impacto

IMPACTO		***Degradación***				
		1%	10%	50%	90%	100%
		MB	**B**	**M**	**A**	**MA**
Probabilidad	**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

Fuente: Elaborado por el investigador, basado en la metodología MAGERIT Libro III Versión 3, Pág. 6

A continuación, se detalla la valoración del impacto de las amenazas y vulnerabilidades identificadas, considerando las dimensiones de degradación y probabilidad:

Tabla 23 Estimación del impacto

IMPACTO						
ACTIVO	**CÓDIGO**	**AMENAZA**	**VULNERABILIDAD**	**DEGRADACIÓN**	**PROBABILIDAD**	**ESTIMACIÓN DEL IMPACTO**
[D] Código fuente de los Sistemas SIA, DIAMANTE, SISWEB	E.2	Errores del administrador	Falta de manuales, instructivos y capacitación en manejo de los sistemas	B	B	**B**
	E.15	Alteración accidental de la información	Falta de control en la gestión del cambio	A	M	**A**
	E.18	Destrucción de información	Falencia en la gestión de respaldos de código fuente	M	MB	**B**
	E.19	Fugas de información	Falta de control en el acceso al código fuente y al término de la relación laboral	B	B	**B**
	A.6	Abuso de privilegios de acceso	Fallas de controles en el acceso	M	B	**B**
	A.11	Acceso no autorizado	Fallas en el control de acceso	MB	B	**B**
	A.18	Destrucción de información	Falta de controles en la gestión de respaldos	B	B	**B**
	A.19	Divulgación de información	Falta de control al término de la relación laboral.	M	MB	**MB**
[D] Base Datos Sistemas: SIA, DIAMANTE, SISWEB	E.1	Errores de los usuarios	Falta de manuales, instructivos y capacitación en manejo de los sistemas	A	B	**M**
	E.2	Errores del administrador	Falta de segregación de funciones.	A	M	**A**
	E.15	Alteración accidental de la información	Falta de controles y privilegios en la DB	A	M	**A**
	E.18	Destrucción de información	Falta de controles en la gestión de respaldos	M	B	**B**
	E.19	Fugas de información	Falta de contratos de	M	B	**B**

IMPACTO						
ACTIVO	**CÓDIGO**	**AMENAZA**	**VULNERABILIDAD**	**DEGRADACIÓN**	**PROBABILIDAD**	**ESTIMACIÓN DEL IMPACTO**
			confidencialidad			
	A.6	Abuso de privilegios de acceso	Fallas en el control de acceso	B	B	**B**
	A.11	Acceso no autorizado	Fallas en el control de acceso	A	B	**M**
	A.15	Modificación deliberada de la información	Fallas en el control de acceso	M	MB	**MB**
	A.18	Destrucción de información	Falta de controles en la gestión de respaldos	MA	A	**MA**
	A.19	Divulgación de información	Falta de contratos de confidencialidad	M	B	**B**
[D] NAS	E.1	Errores de los usuarios	Falta de manuales, instructivos y capacitación en manejo de los sistemas	B	M	**B**
	E.2	Errores del administrador	Falta de capacitación en el manejo del sistema	MB	MB	**MB**
	E.15	Alteración accidental de la información	Falta de control en la segregación de privilegios	B	MB	**B**
	E.18	Destrucción de información	Falta de control en la segregación de privilegios	MA	MA	**MA**
	E.19	Fugas de información	Falta de controles en la desvinculación o cese del cargo	B	MB	**B**
	A.6	Abuso de privilegios de acceso	Falta de control en la asignación de privilegios	B	MB	**B**
	A.11	Acceso no autorizado	Fallas en el control de acceso	M	B	**B**
	A.15	Modificación deliberada de la información	Fallas en el control de acceso	B	B	**B**
	A.18	Destrucción de información	Falta de controles en la gestión de respaldos	MA	MA	**MA**
	A.19	Divulgación de información	Falta de contratos de confidencialidad.	B	B	**B**
[S] Correo Electrónico corporativo	E.1	Errores de los usuarios	Falta de manuales, instructivos y capacitación en manejo de los sistemas	B	B	**B**
	E.2	Errores del administrador	Falta de manuales, instructivos y	B	B	**B**

IMPACTO						
ACTIVO	**CÓDIGO**	**AMENAZA**	**VULNERABILIDAD**	**DEGRADACIÓN**	**PROBABILIDAD**	**ESTIMACIÓN DEL IMPACTO**
			capacitación en manejo de los sistemas			
	E.9	Errores de [re-]encaminamiento	Falta de contratos de confidencialidad	B	B	**B**
	E.15	Alteración accidental de la información	Falta de manuales, instructivos y capacitación en manejo de los sistemas	B	B	**B**
	E.18	Destrucción de información	Falta de contratos de confidencialidad	MB	M	**MB**
	E.19	Fugas de información	Falta de contratos de confidencialidad	M	M	**M**
	E.24	Caída del sistema por agotamiento de recursos	Falta de controles de Denegación de servicio	A	MB	**B**
	A.5	Suplantación de la identidad del usuario	Falta de controles Antispam	M	M	**M**
	A.6	Abuso de privilegios de acceso	Falta de control en la segregación de privilegios	M	B	**B**
	A.7	Uso no previsto	Falta de controles en el manejo del correo electrónico	B	B	**B**
	A.11	Acceso no autorizado	Fallas en el control de acceso	B	B	**B**
	A.13	Repudio	Falta de controles de auditoría	B	B	**B**
	A.14	Destrucción de información	Falta de controles en la vinculación, desvinculación o cambio de cargo.	B	B	**B**
	A.19	Divulgación de información	Falta de controles en la vinculación, desvinculación o cambio de cargo.	B	B	**B**
	A.24	Denegación de servicio	Falta de controles de Denegación de servicios	B	B	**B**
[SW] De desarrollo In House: SIA, DIAMANTE, SISWEB	I.5	Avería de origen físico o lógico	Falta de controles en las pruebas del Software resultante	MA	M	**A**
	E.1	Errores de los usuarios	Falta de manuales, instructivos y capacitación en manejo de los sistemas	M	M	**M**

IMPACTO						
ACTIVO	**CÓDIGO**	**AMENAZA**	**VULNERABILIDAD**	**DEGRADACIÓN**	**PROBABILIDAD**	**ESTIMACIÓN DEL IMPACTO**
	E.20	Vulnerabilidades de los programas (software)	Falta de controles en las pruebas del Software resultante	M	M	**M**
	E.21	Errores de mantenimiento / actualización de programas (software)	Falta de controles en la gestión del cambio	MA	A	**MA**
	A.5	Suplantación de la identidad del usuario	Fallas en el control de acceso	M	M	**M**
	A.6	Abuso de privilegios de acceso	Falta de control en la segregación de privilegios	B	B	**B**
	A.11	Acceso no autorizado	Falta de control de acceso en los ambientes de producción	M	B	**B**
	A.22	Manipulación de programas	Falta de controles en la gestión del cambio	B	B	**B**
[HW] Servidores de Virtualización	N.1	Fuego	Falta de controles de seguridad contra incendio automatizados.	A	B	**M**
	N.2	Daños por agua	Falta de controles de seguridad ambiental	A	B	**M**
	N.*	Desastres naturales	Falta de planes de contingencia, *Disaster Recovery Plan*	A	M	**M**
	I.6	Corte del suministro eléctrico	Falta de contingente eléctrico.	A	M	**M**
	I.7	Condiciones inadecuadas de temperatura o humedad	Falta de controles de seguridad ambiental	A	B	**M**
	E.24	Caída del sistema por agotamiento de recursos	Falta de controles de Denegación de servicios	MA	B	**M**
	E.25	Pérdida de equipos	Falta de planes de contingencia, *Disaster Recovery Plan*	M	M	**M**
	A.11	Acceso no autorizado	Falta de controles de seguridad física	M	B	**B**
	A.23	Manipulación de los equipos	Falta de controles de seguridad física	M	B	**B**
	A.25	Robo	Falta de controles de seguridad física	M	M	**M**
	A.26	Ataque destructivo	Falta de planes de contingencia,	M	M	**M**

IMPACTO						
ACTIVO	**CÓDIGO**	**AMENAZA**	**VULNERABILIDAD**	**DEGRADACIÓN**	**PROBABILIDAD**	**ESTIMACIÓN DEL IMPACTO**
			Disaster Recovery Plan			
[HW] Equipos de escritorio	I.5	Avería de origen físico o lógico	Fallas en el funcionamiento del hardware	B	B	**B**
	I.6	Corte del suministro eléctrico	Falta de suministro de energía de respaldo	B	B	**B**
	E.2	Errores del administrador	Falta de antivirus	B	M	**M**
	E.2	Errores del administrador	Falta de mantenimiento de equipos	B	M	**M**
	E.2	Errores del administrador	Falta de Control en unidades extraíbles (USB)	B	M	**M**
	A.7	Uso no previsto	Falta de controles en el uso de los equipos	B	B	**B**
	A.11	Acceso no autorizado	Fallas en el control de acceso	B	M	**M**
[HW] Equipos Portátiles	I.5	Avería de origen físico o lógico	Fallas en el hardware	B	B	**B**
	E.2	Errores del administrador	Falta de antivirus	B	M	**M**
	E.2	Errores del administrador	Falta de mantenimiento en los equipos	B	M	**M**
	E.2	Errores del administrador	Falta de Control en unidades extraíbles (USB)	B	M	**M**
	E.25	Pérdida de equipos	Robo de equipo	M	M	**M**
	A.7	Uso no previsto	Falta de controles en el uso de los equipos	B	B	**B**
	A.11	Acceso no autorizado	Fallas en el control de acceso	B	M	**M**
	A.25	Robo	Robo de equipo	M	M	**M**
[L] Datacenter	N.1	Fuego	Falta de controles de seguridad contra incendio automatizados.	A	B	**M**
	N.2	Daños por agua	Falta de controles de seguridad ambiental	A	B	**M**
	N.*	Desastres naturales	Falta de planes de contingencia, *Disaster Recovery Plan*	A	M	**M**
	I.6	Corte del suministro eléctrico	Falta de contin1gente eléctrico.	A	M	**M**

IMPACTO						
ACTIVO	**CÓDIGO**	**AMENAZA**	**VULNERABILIDAD**	**DEGRADACIÓN**	**PROBABILIDAD**	**ESTIMACIÓN DEL IMPACTO**
	I.7	Condiciones inadecuadas de temperatura o humedad	Falta de controles de seguridad ambiental	A	B	**M**
	A.11	Acceso no autorizado	Falta de controles de seguridad física	A	M	**A**
	A.23	Manipulación de los equipos	Falta de controles de seguridad física	A	M	**A**
	A.25	Robo	Falta de controles de seguridad física	M	M	**M**
	A.26	Ataque destructivo	Falta de planes de contingencia, *Disaster Recovery Plan*	M	M	**M**
[PERSONAL] Administradores de sistemas SIA, DIAMANTE, SISWEB	E.7	Deficiencias en la organización	Falta de segregación de funciones	M	M	**M**
	E.19	Fugas de información	Falta de contratos de confidencialidad en la desvinculación	B	B	**B**
	E.30	Ingeniería social	Falta de capacitación en seguridades	M	B	**B**
[PESRONAL] Desarrolladores / programadores y DBA	E.7	Deficiencias en la organización	Falta de segregación de funciones	M	M	**M**
	E.19	Fugas de información	Falta de contratos de confidencialidad en la desvinculación	B	B	**B**
	E.30	Ingeniería social	Falta de capacitación en seguridades	M	B	**B**

Fuente: Elaborado por el investigador basándose en la metodología MAGERIT Libro III Versión 3

3.1.4 Estimación del riesgo

Consejo Superior de Administración Electrónica (2012) indica que el crecimiento del riesgo va en función de la probabilidad y el impacto, por consiguiente, para su tratamiento el riesgo se define mediante escalas o zonas detalladas a continuación:

Zona 1: Es representado en la zona de color roja: Riesgos de muy alto impacto y que son muy probables.

Zona 2: Se representa en la zona de color amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables, pero de impacto bajo o muy bajo.

Zona 3: Es representado en la zona de color verde: Son riesgos improbables y de bajo impacto, dicho de otra manera, son riesgos que se puede asumir.

Zona 4: Es representado en la zona de color verde: Se consideran riesgos improbables, pero de muy alto impacto.

En la siguiente figura se representa el mapa de calor de las zonas de riesgo considerando el impacto y la probabilidad.

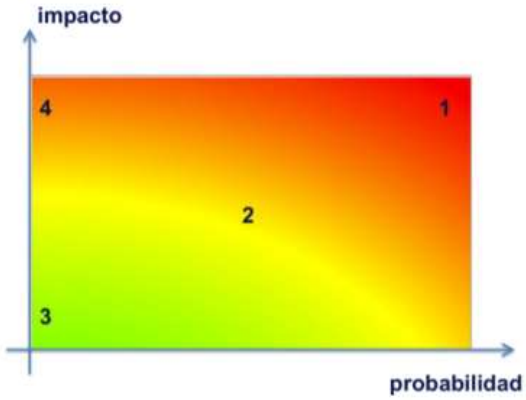


Figura 6 Mapa de calor del riesgo
Fuente: (Consejo Superior de Administración Electrónica, 2012, pág. 30) Libro I MAGERIT versión 3

Tabla 24 Escala estimación del riesgo

IMPACTO	PROBABILIDAD	RIESGO
MA = Muy Alto	MA = Prácticamente seguro	MA = Crítico
A = Alto	A = Probable	A = Importante
M = Medio	M = Posible	M = Apreciable
B = Bajo	B = Poco Probable	B = Bajo
MB = Muy Bajo	MB = Muy Improbable	MB = Insignificante

Mediante la definición de rangos para valorar el riesgo y su representación mediante matrices se logra que la organización pueda tomar decisiones acertadas que le ayuden con el tratamiento de los riesgos para su control y mitigación.

Las valoraciones de impacto y probabilidad de ocurrencia fueron ponderadas conjuntamente con el coordinador del área de TICs de SWEADEN Seguros y se muestran en la siguiente tabla:

Tabla 25 Estimación del riesgo

RIESGO								
Activo	**Riesgo**	**Código**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Estimación del Riesgo**	**Control ISO/IEC 27002:2013**
[D] Código fuente de los Sistemas SIA, DIAMANTE, SISWEB	**RI1**	E.2	Errores del administrador	Falta de manuales, instructivos y capacitación en manejo de los sistemas	B	A	**M**	12.1.1 Documentación de procedimientos de operación 9.4.5 Control de acceso al código fuente de los programas. 12.1.4 Separación de entornos de desarrollo, prueba y producción.
	RI2	E.15	Alteración accidental de la información	Falta de control en la gestión del cambio	A	B	**A**	12.1.1 Documentación de procedimientos de operación
	RI3	E.18	Destrucción de información	Falencia en la gestión de respaldos de código fuente	B	M	**B**	9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.4.5 Control de acceso al código fuente de los programas 12.3.1 Copias de seguridad de la información.

RIESGO								
Activo	**Riesgo**	**Código**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Estimación del Riesgo**	**Control ISO/IEC 27002:2013**
	RI4	E.19	Fugas de información	Falta de control en el acceso al código fuente y falta de control al término de la relación laboral	B	B	**B**	7.3.1 Cese o cambio de puesto de trabajo.
	RI5	A.6	Abuso de privilegios de acceso	Fallas de controles en el acceso	B	B	**B**	9.4.5 Control de acceso al código fuente de los programas
	RI6	A.11	Acceso no autorizado	Fallas en el control de acceso	B	B	**B**	9.2.2 Gestión de los derechos de acceso asignados a usuarios 9.4.5 Control de acceso al código fuente de los programas 10.1.2 Gestión de claves.
	RI7	A.18	Destrucción de información	Falta de controles en la gestión de respaldos	B	M	**B**	12.3.1 Copias de seguridad de la información.
	RI8	A.19	Divulgación de información	Falta de control al término de la relación laboral.	MB	MB	**MB**	7.3.1 Cese o cambio de puesto de trabajo. 9.4.5 Control de acceso al código fuente de los programas.
[D] Base Datos Sistemas: SIA, DIAMANTE, SISWEB	**RI9**	E.1	Errores de los usuarios	Falta de manuales, instructivos y capacitación en manejo de los sistemas	M	M	**M**	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 12.1.1 Documentación

RIESGO								
Activo	**Riesgo**	**Código**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Estimación del Riesgo**	**Control ISO/IEC 27002:2013**
								de procedimientos de operación
	RI10	E.2	Errores del administrador	Falta de segregación de funciones.	A	M	**A**	12.1.1 Documentación de procedimientos de operación 6.1.2 Segregación de tareas
	RI11	E.15	Alteración accidental de la información	Falta de controles y privilegios en la DB	A	B	**A**	9.1.1 Política de control de accesos. 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
	RI12	E.18	Destrucción de información	Falta de controles en la gestión de respaldos	B	M	**B**	12.3.1 Copias de 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 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

RIESGO								
Activo	**Riesgo**	**Código**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Estimación del Riesgo**	**Control ISO/IEC 27002:2013**
								(Redundancias)
	RI13	E.19	Fugas de información	Falta de contratos de confidencialidad	B	M	**B**	7.3.1 Cese o cambio de puesto de trabajo.
	RI14	A.6	Abuso de privilegios de acceso	Fallas en el control de acceso	B	B	**B**	9.2.2 Gestión de los derechos de acceso asignados a usuarios
	RI15	A.11	Acceso no autorizado	Fallas en el control de acceso	M	B	**M**	9.1.1 Política de control de accesos. 9.2.2 Gestión de los derechos de acceso asignados a usuarios
	RI16	A.15	Modificación deliberada de la información	Fallas en el control de acceso	MB	MB	**MB**	9.2.3 Gestión de los derechos de acceso con privilegios especiales.
	RI17	A.18	Destrucción de información	Falta de controles en la gestión de respaldos	MA	M	**MA**	12.3.1 Copias de 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 17.2.1 Disponibilidad de instalaciones para el procesamiento de la

RIESGO								
Activo	**Riesgo**	**Código**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Estimación del Riesgo**	**Control ISO/IEC 27002:2013**
								información. (Redundancias)
	RI18	A.19	Divulgación de información	Falta de contratos de confidencialidad	B	B	**B**	7.3.1 Cese o cambio de puesto de trabajo.
[D] NAS	**RI19**	E.1	Errores de los usuarios	Falta de manuales, instructivos y capacitación en manejo de los sistemas	B	M	**B**	12.1.1 Documentación de procedimientos de operación.
	RI20	E.2	Errores del administrador	Falta de capacitación en el manejo del sistema	MB	B	**MB**	12.1.1 Documentación de procedimientos de operación.
	RI21	E.15	Alteración accidental de la información	Falta de control en la segregación de privilegios	B	MB	**MB**	12.1.1 Documentación de procedimientos de operación.
	RI22	E.18	Destrucción de información	Falta de control en la segregación de privilegios	MA	M	**MA**	12.3.1 Copias de seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información. (Redundancias)
	RI23	E.19	Fugas de información	Falta de controles en la desvinculación o cese del cargo	B	MB	**MB**	7.3.1 Cese o cambio de puesto de trabajo.

RIESGO								
Activo	**Riesgo**	**Código**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Estimación del Riesgo**	**Control ISO/IEC 27002:2013**
	RI24	A.6	Abuso de privilegios de acceso	Falta de control en la asignación de privilegios	B	MB	**MB**	9.2.3 Gestión de los derechos de acceso con privilegios especiales.
	RI25	A.11	Acceso no autorizado	Fallas en el control de acceso	B	B	**B**	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 10.1.2 Gestión de claves.
	RI26	A.15	Modificación deliberada de la información	Fallas en el control de acceso	B	B	**B**	9.2.3 Gestión de los derechos de acceso con privilegios especiales.
	RI27	A.18	Destrucción de información	Falta de controles en la gestión de respaldos	MA	A	**MA**	12.3.1 Copias de seguridad de la información.
	RI28	A.19	Divulgación de información	Falta de contratos de confidencialidad.	B	B	**B**	7.3.1 Cese o cambio de puesto de trabajo.
[S] Correo Electrónico corporativo	**RI29**	E.1	Errores de los usuarios	Falta de manuales, instructivos y capacitación en manejo de los sistemas	B	M	**B**	12.1.1 Documentación de procedimientos de operación.
	RI30	E.2	Errores del administrador	Falta de manuales, instructivos y capacitación en manejo de los sistemas	B	B	**B**	12.1.1 Documentación de procedimientos de operación.
	RI31	E.9	Errores de [re-]encaminamiento	Falta de contratos de confidencialidad	B	B	**B**	7.2.1Responsabilidades de gestión.
	RI32	E.15	Alteración accidental de la información	Falta de manuales, instructivos y capacitación en	B	B	**B**	12.1.1 Documentación de procedimientos de operación.

RIESGO								
Activo	**Riesgo**	**Código**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Estimación del Riesgo**	**Control ISO/IEC 27002:2013**
				manejo de los sistemas				
	RI33	E.18	Destrucción de información	Falta de contratos de confidencialidad	MB	M	**MB**	9.2.6 Retirada o adaptación de los derechos de acceso
	RI34	E.19	Fugas de información	Falta de contratos de confidencialidad	M	M	**M**	9.2.2 Gestión de los derechos de acceso asignados a usuarios
	RI35	E.24	Caída del sistema por agotamiento de recursos	Falta de controles de Denegación de servicio	B	MB	**MB**	17.1.1 Planificación de la continuidad de la seguridad de la información.
	RI36	A.5	Suplantación de la identidad del usuario	Falta de controles Antispam	M	M	**M**	12.6.1 Gestión de las vulnerabilidades técnicas.
	RI37	A.6	Abuso de privilegios de acceso	Falta de control en la segregación de privilegios	B	B	**B**	9.2.2 Gestión de los derechos de acceso asignados a usuarios.
	RI38	A.7	Uso no previsto	Falta de controles en el manejo del correo electrónico	B	B	**B**	12.1.1 Documentación de procedimientos de operación. 5.1.1 Conjunto de políticas para la seguridad de la información.
	RI39	A.11	Acceso no autorizado	Fallas en el control de acceso	B	B	**B**	9.1.1 Política de control de accesos. 9.4.2 Procedimientos seguros de inicio de sesión.

RIESGO								
Activo	**Riesgo**	**Código**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Estimación del Riesgo**	**Control ISO/IEC 27002:2013**
	RI40	A.13	Repudio	Falta de controles de auditoría	B	B	**B**	
	RI41	A.14	Destrucción de información	Falta de controles en la vinculación, desvinculación o cambio de cargo.	B	B	**B**	9.2.6 Retirada o adaptación de los derechos de acceso.
	RI42	A.19	Divulgación de información	Falta de controles en la vinculación, desvinculación o cambio de cargo.	B	B	**B**	9.2.6 Retirada o adaptación de los derechos de acceso.
	RI43	A.24	Denegación de servicio	Falta de controles de Denegación de servicios	B	B	**B**	17.1.1 Planificación de la continuidad de la seguridad de la información.
[SW] De desarrollo In House: SIA, DIAMANTE, SISWEB	**RI44**	I.5	Avería de origen físico o lógico	Falta de controles en las pruebas del Software resultante	A	B	**A**	14.2.2 Procedimientos de control de cambios en los sistemas. 14.2.9 Pruebas de aceptación.
	RI45	E.1	Errores de los usuarios	Falta de manuales, instructivos y capacitación en manejo de los sistemas	M	M	**M**	12.1.1 Documentación de procedimientos de operación.
	RI46	E.20	Vulnerabilidades de los programas (software)	Falta de controles en las pruebas del Software resultante	M	B	**M**	12.6.1 Gestión de las vulnerabilidades técnicas. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los

RIESGO								
Activo	**Riesgo**	**Código**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Estimación del Riesgo**	**Control ISO/IEC 27002:2013**
								sistemas
	RI47	E.21	Errores de mantenimiento / actualización de programas (software)	Falta de controles en la gestión del cambio	MA	M	**MA**	14.2.2 Procedimientos de control de cambios en los sistemas. 12.1.4 Separación de entornos de desarrollo, prueba y producción.
	RI48	A.5	Suplantación de la identidad del usuario	Fallas en el control de acceso	M	B	**M**	9.1.1 Política de control de accesos. 9.4.2 Procedimientos seguros de inicio de sesión
	RI49	A.6	Abuso de privilegios de acceso	Falta de control en la segregación de privilegios	B	B	**B**	9.2.3 Gestión de los derechos de acceso con privilegios especiales.
	RI50	A.11	Acceso no autorizado	Falta de control de acceso en los ambientes de producción	B	B	**B**	9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.4.2 Procedimientos seguros de inicio de sesión
	RI51	A.22	Manipulación de programas	Falta de controles en la gestión del cambio	B	B	**B**	14.2.1 Política de desarrollo seguro de software.
	RI52	N.1	Fuego	Falta de controles de seguridad contra	M	M	**M**	11.1.4 Protección contra las amenazas

RIESGO								
Activo	**Riesgo**	**Código**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Estimación del Riesgo**	**Control ISO/IEC 27002:2013**
[HW] Servidores de Virtualización				incendio automatizados.				externas y ambientales
	RI53	N.2	Daños por agua	Falta de controles de seguridad ambiental	M	B	**M**	11.1.4 Protección contra las amenazas externas y ambientales
	RI54	N.*	Desastres naturales	Falta de planes de contingencia, *Disaster Recovery Plan*	M	M	**M**	11.1.4 Protección contra las amenazas externas y ambientales. 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 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información. (Redundancias)
	RI55	I.6	Corte del suministro eléctrico	Falta de contingente eléctrico.	M	M	**M**	11.2.2 Instalaciones de suministro.
	RI56	I.7	Condiciones inadecuadas de temperatura o humedad	Falta de controles de seguridad ambiental	M	B	**M**	11.1.4 Protección contra las amenazas externas y ambientales
	RI57	E.24	Caída del sistema por agotamiento de recursos	Falta de controles de Denegación de servicios	M	B	**M**	16.1.5 Respuesta a los incidentes de seguridad.

RIESGO								
Activo	**Riesgo**	**Código**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Estimación del Riesgo**	**Control ISO/IEC 27002:2013**
								17.1.1 Planificación de la continuidad de la seguridad de la información.
	RI58	E.25	Pérdida de equipos	Falta de planes de contingencia, *Disaster Recovery Plan*	M	M	**M**	16.1.5 Respuesta a los incidentes de seguridad. 17.1.1 Planificación de la continuidad de la seguridad de la información.
	RI59	A.11	Acceso no autorizado	Falta de controles de seguridad física	B	B	**B**	9.1.1 Política de control de accesos. 12.6.1 Gestión de las vulnerabilidades técnicas.
	RI60	A.23	Manipulación de los equipos	Falta de controles de seguridad física	B	M	**B**	11.1.1 Perímetro de seguridad física.
	RI61	A.25	Robo	Falta de controles de seguridad física	M	M	**M**	11.1.1 Perímetro de seguridad física.
	RI62	A.26	Ataque destructivo	Falta de planes de contingencia, *Disaster Recovery Plan*	M	M	**M**	11.1.1 Perímetro de seguridad física. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.2.1 Disponibilidad

RIESGO								
Activo	**Riesgo**	**Código**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Estimación del Riesgo**	**Control ISO/IEC 27002:2013**
								de instalaciones para el procesamiento de la información. (Redundancias)
[HW] Equipos de escritorio	**RI63**	I.5	Avería de origen físico o lógico	Fallas en el funcionamiento del hardware	B	B	**B**	11.2.4 Mantenimiento de los equipos
	RI64	I.6	Corte del suministro eléctrico	Falta de suministro de energía de respaldo	B	B	**B**	11.2.2 Instalaciones de suministro.
	RI65	E.2	Errores del administrador	Falta de antivirus	M	M	**M**	12.6.1 Gestión de las vulnerabilidades técnicas.
	RI66	E.2	Errores del administrador	Falta de mantenimiento de equipos	M	M	**M**	11.2.4 Mantenimiento de los equipos
	RI67	E.2	Errores del administrador	Falta de Control en unidades extraíbles (USB)	M	M	**M**	8.3.1 Gestión de soportes extraíbles
	RI68	A.7	Uso no previsto	Falta de controles en el uso de los equipos	B	B	**B**	5.1.1 Conjunto de políticas para la seguridad de la información 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla
	RI69	A.11	Acceso no autorizado	Fallas en el control de acceso	M	M	**M**	9.1.1 Política de control de accesos. 9.1.2 Control de acceso

RIESGO								
Activo	**Riesgo**	**Código**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Estimación del Riesgo**	**Control ISO/IEC 27002:2013**
								a las redes y servicios asociados 9.4.2 Procedimientos seguros de inicio de sesión
[HW] Equipos portátiles	**RI70**	I.5	Avería de origen físico o lógico	Fallas en el hardware	B	B	**B**	11.2.4 Mantenimiento de los equipos
	RI71	E.2	Errores del administrador	Falta de antivirus	M	M	**M**	12.6.1 Gestión de las vulnerabilidades técnicas.
	RI72	E.2	Errores del administrador	Falta de mantenimiento en los equipos	M	M	**M**	11.2.4 Mantenimiento de los equipos
	RI73	E.2	Errores del administrador	Falta de Control en unidades extraíbles (USB)	M	M	**M**	8.3.1 Gestión de soportes extraíbles
	RI74	E.25	Pérdida de equipos	Robo de equipo	M	B	**M**	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
	RI75	A.7	Uso no previsto	Falta de controles en el uso de los equipos	B	B	**B**	6.2.1 Política de uso de dispositivos para movilidad. 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla
	RI76	A.11	Acceso no autorizado	Fallas en el control de acceso	M	M	**M**	9.1.1 Política de control de accesos. 9.1.2 Control de acceso

RIESGO								
Activo	**Riesgo**	**Código**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Estimación del Riesgo**	**Control ISO/IEC 27002:2013**
								a las redes y servicios asociados. 9.4.2 Procedimientos seguros de inicio de sesión
	RI77	A.25	Robo	Robo de equipo	M	M	**M**	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
[L] Datacenter	**RI78**	N.1	Fuego	Falta de controles de seguridad contra incendio automatizados.	M	B	**M**	11.1.4 Protección contra las amenazas externas y ambientales.
	RI79	N.2	Daños por agua	Falta de controles de seguridad ambiental	M	B	**M**	11.1.4 Protección contra las amenazas externas y ambientales.
	RI80	N.*	Desastres naturales	Falta de planes de contingencia, *Disaster Recovery Plan*	M	M	**M**	11.1.4 Protección contra las amenazas externas y ambientales. 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 17.2.1 Disponibilidad de instalaciones para el procesamiento de la

RIESGO								
Activo	**Riesgo**	**Código**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Estimación del Riesgo**	**Control ISO/IEC 27002:2013**
								información. (Redundancias)
	RI81	I.6	Corte del suministro eléctrico	Falta de contingente eléctrico.	M	M	**M**	11.2.2 Instalaciones de suministro.
	RI82	I.7	Condiciones inadecuadas de temperatura o humedad	Falta de controles de seguridad ambiental	M	B	**M**	11.1.4 Protección contra las amenazas externas y ambientales
	RI83	A.11	Acceso no autorizado	Falta de controles de seguridad física	A	M	**A**	11.1.2 Controles físicos de entrada.
	RI84	A.23	Manipulación de los equipos	Falta de controles de seguridad física	A	M	**A**	11.1.1 Perímetro de seguridad física.
	RI85	A.25	Robo	Falta de controles de seguridad física	M	M	**M**	11.1.1 Perímetro de seguridad física.
	RI86	A.26	Ataque destructivo	Falta de planes de contingencia, *Disaster Recovery Plan*	M	M	**M**	17.1.1 Planificación de la continuidad de la seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información. (Redundancias)
[PERSONAL] Administradores de sistemas SIA, DIAMANTE, SISWEB	**RI87**	E.7	Deficiencias en la organización	Falta de segregación de funciones	M	B	**M**	6.1.2 Segregación de tareas
	RI88	E.19	Fugas de información	Falta de contratos de confidencialidad en la desvinculación	B	B	**B**	7.2.2 Concienciación, educación y capacitación en seguridad de la información.

RIESGO								
Activo	**Riesgo**	**Código**	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad de ocurrencia**	**Estimación del Riesgo**	**Control ISO/IEC 27002:2013**
								7.3.1 Cese o cambio de puesto de trabajo.
	RI89	E.30	Ingeniería social	Falta de capacitación en seguridades	B	B	**B**	7.2.2 Concienciación, educación y capacitación en seguridad de la información.
[PESRONAL] Desarrolladores / programadores y DBA	**RI90**	E.7	Deficiencias en la organización	Falta de segregación de funciones	M	B	**M**	6.1.2 Segregación de tareas
	RI91	E.19	Fugas de información	Falta de contratos de confidencialidad en la desvinculación	B	B	**B**	7.2.2 Concienciación, educación y capacitación en seguridad de la información. 7.3.1 Cese o cambio de puesto de trabajo
	RI92	E.30	Ingeniería social	Falta de capacitación en seguridades	B	B	**B**	7.2.2 Concienciación, educación y capacitación en seguridad de la información.

Fuente: Elaborado por el investigador, basándose en la metodología MAGERIT Libro III Versión 3

De acuerdo a las a las dimensiones de probabilidad e impacto se representa en el siguiente mapa de calor la valoración de cada riesgo identificado para SWEADEN Seguros.

Tabla 26 Mapa de Riesgos SWEADEN Seguros

RIESGO		***Probabilidad***				
		MB	**B**	**M**	**A**	**MA**
Impacto	**MA**			**RI17, RI22, RI47**	**RI27**	
	A		RI2, RI11, RI44	RI10, RI83, RI84		
	M		RI15, RI46, RI48, R53, R56, R57, R74, R78, R79, R82, R87, R90	R9, R34, R36, R45 R52, R54, R55, R58 R61, R62, R65, R66 R67, R69, R71, R72 R73, R76, R77, R80 R81, R85, R86		
	B	RI21, RI23, RI24, RI35	RI4, RI5, RI6, RI14, RI18, RI25, RI26, RI28, RI30, RI31, RI32, RI37, RI38, RI39, RI40, RI41, RI42, RI43 RI49, RI50, RI51, RI59, RI63, RI64, RI68, RI70, RI75, RI88, RI89, RI91, RI92	RI3, RI7, RI12, RI13, RI19, RI29, RI60	RI1	
	MB	RI8, RI16	RI20	RI33		

Fuente: Elaborado por el investigador

Para la interpretación del mapa anterior y la aceptación del riesgo se debe considerar lo que se indica en la siguiente tabla:

Tabla 27 Aceptación del riesgo

Zona de riesgo	**Valor**	**Aceptación del riesgo**
Extrema	**MA**	Riesgos muy probables, requieren atención inmediata.
Alta	**A**	Riesgos improbables, pero de alto impacto, requieren la atención adecuada.
Moderada	**M**	Riesgos aceptables, sin embargo, se tiene que evaluar si los controles aplicados son lo suficientemente funcionales para tratar el riesgo.
Baja	**B**	Riesgos de bajo impacto e improbables, se requiere supervisión según sea necesario.
Muy Baja	**MB**	Riesgos improbables, se puede asumir.

Fuente: Elaborado por el investigador basado en la Metodología MAGERIT Libro I Versión 3

De acuerdo a la matriz de riesgos elaborada en la siguiente tabla se pueden apreciar los riesgos sobre los activos de la información más críticos para SWEADEN Seguros, por lo tanto, se deben implementar los controles y estrategias de seguridad para mitigarlos de manera inmediata.

Tabla 28 Riesgos de información críticos

Activo de Información	Riesgo	Código	Amenaza	Vulnerabilidad	Estimación del Riesgo	Control ISO/IEC 27002:2013
[D] Código fuente de los Sistemas SIA, DIAMANTE, SISWEB	**RI2**	E.15	Alteración accidental de la información	Falta de control en la gestión del cambio	**A**	12.1.1 Documentación de procedimientos de operación.
[D] Base Datos Sistemas: SIA, DIAMANTE, SISWEB	**RI10**	E.2	Errores del administrador	Falta de segregación de funciones.	**A**	12.1.1 Documentación de procedimientos de operación. 6.1.2 Segregación de tareas
	RI11	E.15	Alteración accidental de la información	Falta de controles y privilegios en la DB	**A**	9.1.1 Política de control de accesos. 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
	RI17	A.18	Destrucción de información	Falta de controles en la gestión de respaldos	**MA**	12.3.1 Copias de 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 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información. (Redundancias)

[D] NAS	**RI22**	E.18	Destrucción de información	Falta de control en la segregación de privilegios	**MA**	12.3.1 Copias de seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información. (Redundancias)
	RI27	A.18	Destrucción de información	Falta de controles en la gestión de respaldos	**MA**	12.3.1 Copias de seguridad de la información.
[SW] De desarrollo In House: SIA, DIAMANTE, SISWEB	**RI44**	I.5	Avería de origen físico o lógico	Falta de controles en las pruebas del Software resultante	**A**	14.2.2 Procedimientos de control de cambios en los sistemas. 14.2.9 Pruebas de aceptación.
	RI47	E.21	Errores de mantenimiento / actualización de programas (software)	Falta de controles en la gestión del cambio	**MA**	14.2.2 Procedimientos de control de cambios en los sistemas. 12.1.4 Separación de entornos de desarrollo, prueba y producción.
[L] Datacenter	**RI83**	A.11	Acceso no autorizado	Falta de controles de seguridad física	**A**	11.1.2 Controles físicos de entrada.
	RI84	A.23	Manipulación de los equipos	Falta de controles de seguridad física	**A**	11.1.1 Perímetro de seguridad física.

Fuente: Elaborado por el investigador

3.1.5 Determinando las salvaguardas para controlar o mitigar el riesgo

Las salvaguardas permiten contrarrestar las amenazas y de esta manera controlar o mitigar el riesgo.

Tomando como referencia el anexo 2 de la norma ISO/IEC 27002:2013, a continuación, se detallan los controles seleccionados para SWEADEN Seguros para la mitigación de los riesgos de cada uno de sus activos, en función de sus amenazas, vulnerabilidades y valoración riesgo obtenido.

Tabla 29 Controles de la norma ISO 27002 para el control de los riesgos

Dominio	Objetivo de control	Control	Riesgos
5. POLÍTICAS 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.	RI38, RI68
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.	6.1 Organización interna.	6.1.2 Segregación de tareas.	RI10, RI87, RI90
	6.2 Dispositivos para movilidad y teletrabajo	6.2.1 Política de uso de dispositivos para movilidad.	RI75
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	7.2 Durante la contratación.	7.2.1Responsabilidades de gestión.	RI31
		7.2.2 Concienciación, educación y capacitación en seguridad de la información.	RI88, RI89, RI91, RI91
	7.3 Cese o cambio de puesto de trabajo.	7.3.1 Cese o cambio de puesto de trabajo	RI4, RI8, RI13, RI18, RI23, RI28, RI88, RI91
8. GESTIÓN DE ACTIVOS.	8.2 Clasificación de la información.	8.2.1 Directrices de clasificación.	
		8.2.2 Etiquetado y manipulado de la información.	
	8.3 Manejo de los soportes de almacenamiento	8.3.1 Gestión de soportes extraíbles.	RI67, RI73
9. CONTROL DE ACCESOS.	9.1 Requisitos de negocio para el control de accesos.	9.1.1 Política de control de accesos.	RI11, RI15, RI39, RI48, RI50, RI59, RI69, RI76
		9.1.2 Control de acceso a las redes y servicios asociados.	RI50, RI69, RI76
	9.2 Gestión de acceso de usuario.	9.2.2 Gestión de los derechos de acceso asignados a usuarios	RI6, RI9, RI11, RI14, RI15, RI25, RI34, RI37
		9.2.3 Gestión de los derechos de acceso con privilegios especiales.	RI3, RI16, RI24, RI26, RI49
		9.2.6 Retirada o adaptación de los derechos de acceso	RI33, RI41, RI42
	9.3 Responsabilidades del usuario.	9.3.1 Uso de información confidencial para la autenticación	
	9.4 Control de acceso a sistemas y aplicaciones.	9.4.2 Procedimientos seguros de inicio de sesión	RI39, RI48, RI50, RI69, RI76
		9.4.5 Control de acceso al código fuente de los programas	RI1, RI3, RI5, RI6, RI8
10. CIFRADO.	10.1 Controles criptográficos.	10.1.2 Gestión de claves.	RI6, RI25

Dominio	Objetivo de control	Control	Riesgos
11. SEGURIDAD FÍSICA Y AMBIENTAL.	11.1 Áreas seguras.	11.1.1 Perímetro de seguridad física.	RI60, RI61, RI62, RI84, RI85
		11.1.2 Controles físicos de entrada.	RI83
		11.1.4 Protección contra las amenazas externas y ambientales.	RI52, RI53, RI54, RI56, RI78, RI79, RI80, RI82
	11.2 Seguridad de los equipos.	11.2.2 Instalaciones de suministro.	RI55, RI64, RI81
		11.2.4 Mantenimiento de los equipos	RI63, RI66, RI70, RI72
		11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	RI74, RI77
		11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla	RI68, RI75
12. SEGURIDAD EN LA OPERATIVA.	12.1 Responsabilidades y procedimientos de operación.	12.1.1 Documentación de procedimientos de operación	RI1, RI2, RI9, RI10, RI19, RI20, RI21, RI29, RI30, RI32, RI38, RI45
		12.1.4 Separación de entornos de desarrollo, prueba y producción.	RI1, RI47
	12.3 Copias de seguridad.	12.3.1 Copias de seguridad de la información.	RI3, RI7, RI12, RI17, RI22, RI27
	12.6 Gestión de la vulnerabilidad técnica.	12.6.1 Gestión de las vulnerabilidades técnicas.	RI36, RI46, RI59, RI65, RI71
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	14.2 Seguridad en los procesos de desarrollo y soporte.	14.2.1 Política de desarrollo seguro de software.	RI51
		14.2.2 Procedimientos de control de cambios en los sistemas.	RI44, RI47
		14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas	RI46
		14.2.9 Pruebas de aceptación.	RI44
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	16.1 Gestión de incidentes de seguridad de la información y mejoras.	16.1.5 Respuesta a los incidentes de seguridad.	RI57, RI58
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	17.1Continuidad de la seguridad de la información.	17.1.1 Planificación de la continuidad de la seguridad de la información.	RI12, RI17, RI35, RI43, RI54, RI57, RI58, RI62, RI80, RI86
		17.1.2 Implantación de la continuidad de la seguridad de la información	RI12, RI17, RI22, RI54, RI62, RI80
	17.2Redundancias.	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	RI12, RI17, RI22, RI54, RI62, RI80, RI86

Fuente: Norma ISO 27002:2013

CAPÍTULO IV

PROPUESTA

Una vez evaluados los riesgos del área de TICs de SWEADEN Seguros mediante la utilización de la metodología MAGERIT y considerando los lineamientos de la normativa ISO/IEC 27002:2013 se propone diseñar la política de seguridad en función de las actividades que realiza el área de TICs de SWEADEN, con el objetivo de fortalecer y garantizar un adecuado tratamiento de la información.

4.1 Introducción

El área de TICs de SWEADEN Seguros en conjunto con la dirección de la organización consideran que la información es un componente indispensable para la continuidad de las operaciones del negocio y la consecución de sus objetivos estratégicos, por esta razón es importante establecer un esquema para el aseguramiento de la información y sus activos involucrados; para dar cumplimiento a este objetivo es necesario diseñar mecanismos y controles que permitan la recolección, transporte, procesamiento y almacenamiento de la información de manera adecuada.

La seguridad de la información es una prioridad para SWEADEN Seguros, por lo tanto, existe la necesidad de contar con una metodología, mecanismos y controles que garanticen la calidad y el aseguramiento de la información, para cumplir este propósito se propone el diseño de una política de seguridad de la información basado en la norma ISO/IEC 27002:2013 ya que este documento servirá como una guía para que el área de TICs y todos los colaboradores de la organización puedan proteger y dar un buen tratamiento a la información.

4.2 Alcance

Diseñar la política de seguridad que sirva como una guía para el área de Tecnologías de la información de SWEADEN Seguros, mediante la implementación de controles y procedimientos seguros, que le permitan gestionar sus procesos de manera que se garantice la protección y calidad de la información.

Como punto adicional y no menos importante se busca generar conciencia de seguridad en el personal de Tecnología y en todos los colaboradores de la aseguradora, a través de planes de capacitación para dotar de conocimientos a los usuarios que les permita aplicar buenas prácticas de seguridad en las actividades diarias para evitar pérdida de información, e interrupciones en la infraestructura tecnológica.

4.3 Definiciones y abreviaturas

Activo de Información: Es un dato, información o elemento que tienen valor para la organización.

Seguridad de la información: Se refiere a proteger la información y sus activos relacionados

mediante controles y medidas de protección que garanticen el adecuado tratamiento a los riesgos de la información permitiendo con esto la continuidad del negocio.

Confidencialidad: Es garantizar que la información sea utilizada solo por las personas autorizadas.

Integridad: Garantiza que la información esté completa y que se permita el tratamiento de esta, solo a las personas autorizadas.

Disponibilidad: Debe garantizar que la información y sus activos se mantengan disponibles siempre cuando se los requiera.

Usuario: Es la persona que hace uso de los servicio y recursos tecnológicos (usuarios, asesores, proveedores, clientes de la organización)

Vulnerabilidad: Buendía (2013) describe a una vulnerabilidad como una falla o defecto de un sistema, aplicación que al ser detectada por un atacante puede ser aprovechada a su criterio.

Amenaza: Como lo menciona Chávez (2015) una amenaza informática es un evento de riesgo que puede causar una afectación a los activos de información, por lo general está relacionada con las personas, fallas técnicas o eventos naturales.

Evento de seguridad de la información: Se denomina evento de seguridad a cualquier suceso

relacionado con la seguridad pero que no necesariamente tiene una repercusión negativa sobre la información.

Incidente de Seguridad de la información: Se puede considerar a un incidente de seguridad a algún cambio o suceso que tiene una afectación negativa como sobre los recursos de información.

Malware: Soto (2018) menciona en su libro Análisis de Malware para Sistemas Windows que la guía NIST SP 800-83 *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* define el término malware como aquel programa que se oculta dentro de otro programa con la intención de afectar a la información, ejecutar programas destructivos o intrusivos, o comprometer de cualquier a la confidencialidad, integridad y disponibilidad de la información, aplicaciones o el sistema operativo de la víctima.

VPN: (*Virtual Private Network)* en español Red Virtual Privada, esta tecnología permite acceder desde una red externa a la red local de manera segura.

TIC: Tecnologías de la información y la comunicación

4.4 Responsabilidades

- El directorio de SWEADEN Seguros tiene como responsabilidad, revisar y aprobar la política de seguridad de la información.

- La Alta Dirección de SWEADEN Seguros tiene como responsabilidad autorizar y proveer de los recursos necesarios para la implementación y mantenimiento de la política de seguridad.

- Es responsabilidad de la Alta Dirección y del Área de Tecnologías de la información de SWEADEN Seguros promover una cultura de seguridad informática en todos los colaboradores de la organización.

- El coordinador del área de TICs de SWEADEN Seguros tiene como responsabilidad, crear, actualizar, conocer, aplicar y verificar el cumplimiento de la política de seguridad.

- Los usuarios de SWEADEN Seguros tienen como responsabilidad dar cumplimiento a los lineamientos estipulados en la política de seguridad organizacional.

En base a la normativa ISO/IEC 27002:2013, a continuación, se describen todos los lineamientos y controles para SWEADEN Seguros logre controlar los riesgos relacionados con la seguridad de la información.

4.5 Política de seguridad de la información para SWEADEN Seguros

4.5.1 POLÍTICA DE SEGURIDAD

4.5.1.1 Directrices de la Dirección en seguridad de la información

Objetivo: La Dirección debe comprometerse con el apoyo y soporte sobre la gestión de la seguridad de la información.

a) Conjunto de políticas para la seguridad de la información

Literal 1. Es responsabilidad del coordinador del área de TICs gestionar la aprobación del documento que contenga la política de seguridad de la información para la organización.

Literal 2. Es responsabilidad del coordinador del área de TICs gestionar la publicación y sociabilización de la política de seguridad de la información con los colaboradores de la organización

Literal 3. Es compromiso de la Alta Dirección apoyar con la actualización y mantenimiento de la política de la seguridad de la información.

Literal 4. Es responsabilidad de todo el personal de la organización conocer la política y dar cumplimiento a sus lineamientos.

b) Revisión de las políticas para la seguridad de la información

Literal 5. El coordinador del área de TICs de SWEADEN Seguros deberá revisar y actualizar la política de seguridad de la información por lo menos una vez al año.

4.5.2 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

4.5.2.1 Organización interna

Objetivo: Establecer las directrices para la gestión, tratamiento y vigilancia en la implementación de la seguridad de la información institucional.

a) Segregación de tareas

Literal 6. Para garantizar una adecuada gestión dentro del proceso de Desarrollo, SWEADEN Seguros debe segregar las funciones de tecnología habilitando responsables en cada fase del proceso, para ello se propone que existan:

- Coordinador de Desarrollo y QA
- Analistas Programadores
- Gestor de Base de datos

Literal 7. Para garantizar la integridad y confidencialidad de la información es recomendable separar las funciones de seguridad como una unidad independiente del área de TICs, evitando así conflictos de intereses.

4.5.2.2 Dispositivos para movilidad y teletrabajo

Objetivo: Se busca proteger la información cuando se utilizan recursos de informática móviles como laptops, y en la gestión del teletrabajo.

a) Teletrabajo

Literal 8. Para asegurar la confidencialidad de la información, el analista de soporte deberá entregar al usuario el equipo portátil con el disco cifrado, con la finalidad de que la información no sea comprometida ante un evento de pérdida o robo.

Literal 9. Para realizar operaciones de teletrabajo, los usuarios o externos deben firmar un contrato de confidencialidad para la entrega de su acceso VPN.

Literal 10. Para que los usuarios puedan acceder a la información o servicios de la red local cuando se encuentren fuera de las instalaciones de la organización, el analista de soporte deberá instalar el software cliente de VPN y configurar los accesos.

Literal 11. El área de TICs deberá entregar los equipos portátiles a los usuarios de la organización con las unidades extraíbles USB, CD/DVD bloqueadas.

Literal 12. Las contraseñas de los equipos portátiles entregados a los usuarios deberán ser administradas con sigilo y resguardo, no pueden ser divulgadas bajo cualquier circunstancia.

Literal 13. Para la activación de unidades extraíbles se generará un ticket de soporte para que el analista de seguridad lo gestione luego de la autorización necesaria.

Literal 14. Para operaciones de teletrabajo los usuarios generarán un ticket de soporte el mismo que deberá ser aprobado por sus superiores, para que el coordinador de TICs gestione los accesos y autorización respectiva.

Literal 15. Para operaciones de teletrabajo el área de TICs debe crear un documento con el procedimiento para la utilización de VPNs, el mismo que será sociabilizados con los usuarios autorizados.

4.5.3 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

4.5.3.1 Antes de la contratación

Objetivo: Se busca garantizar que los empleados sean aptos para su cargo y que entiendan claramente sus funciones, mediante la previa revisión de antecedentes se puede reducir el fraude o robo.

a) Investigación de antecedentes

Literal 16. Para la contratación del personal el área de Talento Humano debe realizar revisiones y verificación de antecedentes de los postulantes, con mucho mayor detalle y control cuando se trate de cargos críticos, estos cargos serán estipulados por la Alta Dirección.

b) Términos y condiciones de contratación

Literal 17. Todos los colaboradores de la organización, contratistas y usuarios externos de los servicios de procesamiento de la información deben firmar un acuerdo de responsabilidad sobre sus funciones y responsabilidades con relación a la seguridad e información.

Literal 18. Los colaboradores de la organización que ejercen las funciones de cargos críticos deben firmar un acuerdo de confidencialidad y no divulgación de información.

4.5.3.2 Durante la contratación

Objetivo: Se busca asegurar que los empleados sepan claramente cuáles son sus funciones y responsabilidades con respecto a la seguridad de la información durante su relación laboral con la organización.

a) Responsabilidades de gestión.

Literal 19. Los colaboradores de la organización deberán usar los canales adecuados para la solicitud de soporte, gestión de incidentes o problemas, los canales oficiales de SWEADEN Seguros son: el Sistema de Tickets de soporte como servicio primario, y vía telefónica como secundario.

Literal 20. Los usuarios solo utilizarán los equipos que se le hayan asignados para ejecutar las actividades laborales.

Literal 21. Los usuarios son responsables del uso del ordenador asignado y deben estar obligatoriamente protegidos por una contraseña con la complejidad requerida, es decir, no trivial o evidente.

Literal 22. Es responsabilidad del usuario proteger su equipo de trabajo, aplicando el bloqueo de pantalla (Bloqueo de Sesión), cuando se ausente de su lugar de trabajo, evitando que personas no autorizadas acedan a la información almacenada en el mismo.

Literal 23. Los colaboradores de la organización deberán asegurar sigilosamente sus contraseñas, evitando escribirlas sobre papel, superficies visibles o de fácil acceso.

Literal 24. Los colaboradores de la organización no pueden usar equipos informáticos personales como: tabletas, ipads, laptops, en su área de trabajo.

b) Capacitación, educación y concienciación en seguridad de la información.

Literal 25. El área de TICs debe generar planes de capacitación de manera periódica sobre temas de seguridad y gestión de la información, para impartirlos a los empleados de la organización.

Literal 26. En el ingreso de un nuevo empleado a la organización, el área de TICs deberá brindar una inducción inicial de los sistemas y recursos informáticos de la organización.

Literal 27. El analista de soporte es responsable de instalar y mantener actualizado el antivirus en todas las estaciones de la organización.

Literal 28. Es responsabilidad de la organización proveer los recursos para el licenciamiento de un antivirus corporativo.

Literal 29. Se prohíbe a los usuarios utilizar módems, proxys o cualquier sistema de conexión que no esté autorizado por la organización.

4.5.3.3 Cese o cambio de puesto de trabajo

Objetivo: Se busca proteger los activos de información cuando existen cambios de funciones o salida del colaborador.

a) Cese o cambio de puesto de trabajo

Literal 30. El área de Talento de Humano debe informar de manera escrita al área de TICs de la salida, ingreso o cambio de los colaboradores, para proceder con el procedimiento de Alta y Baja de usuarios según sea el caso.

Literal 31. El área de TICs debe ejecutar el procedimiento de Baja de usuarios inmediatamente cuando Talento Humano genere la notificación de la salida de los colaboradores de la organización.

4.5.4 GESTIÓN DE ACTIVOS

4.5.4.1 Responsabilidad sobre los activos

Objetivo: Llevar un inventario de los activos de información de la organización con la finalidad de establecer las protecciones adecuadas sobre estos.

a) Inventario de activos

Literal 32. El área de TICs debe mantener un inventario actualizado de los activos de información más importantes para la organización de manera que estos sean claramente identificados.

b) Devolución de activos

Literal 33. Es responsabilidad del coordinador de cada área (jefaturas) y el analista de seguridad ejecutar el protocolo para devolución de activos cuando un colaborador termina su relación laboral con la organización.

4.5.4.2 Clasificación de la información

Objetivo: Es asegurar que existan niveles protección de acuerdo con la clasificación de la información.

a) Directrices de clasificación

Literal 34. Tanto el área de TICs como la Alta Dirección de SWEADEN Seguros deben generar un esquema de clasificación de la información considerando parámetros como legalidad, confidencialidad y criticidad para su respectiva valoración y tratamiento respectivo.

b) Etiquetado y manipulado de la información

Literal 35. El área de TICs en conjunto con la Alta Dirección de la organización tiene que diseñar procedimientos para el etiquetado y calificación de la información.

4.5.4.3 Manejo de los soportes de almacenamiento

Objetivo: Busca controlar que los datos de los activos de información almacenados en los soportes no sean divulgados, modificados, o destruidos sin autorización.

a) Gestión de soportes extraíbles

Literal 36. El área de TICs debe bloquear el uso de almacenamientos extraíbles como USB, DVD en todos los equipos de la organización y se desbloqueará bajo aprobación de los altos mandos.

b) Eliminación de soportes

Literal 37. El área de TICs debe ejecutar procedimientos seguros para la eliminación de medios de almacenamiento cuando estos ya no sean requeridos para las operaciones de la organización.

4.5.5 CONTROL DE ACCESOS

4.5.5.1 Requisitos de negocio para el control de accesos

Objetivo: Busca controlar el acceso a los diferentes sistemas y servicios informáticos de SWEADEN Seguros.

c) Política de control de accesos

Literal 38. Para garantizar el acceso autorizado a los diferentes sistemas y recursos de información, la organización y específicamente el área de TICs debe contar con las herramientas que permitan gestionar correctamente los accesos, para ello es muy importante implementar un controlador de dominio o directorio activo.

Literal 39. Es responsabilidad del área de TICs documentar y revisar periódicamente los lineamientos para el control de acceso a los recursos de información, según las necesidades de seguridad de la organización.

Literal 40. Es política de SWEADEN Seguros que las contraseñas establecidas para los sistemas y aplicaciones tengan un grado de complejidad Alto, para ello deben cumplir con los siguientes requerimientos:

- Mayor a 8 caracteres.
- La contraseña debe ser alfanumérica.
- Debe contener por lo menos un carácter especial.
- Deben combinarse caracteres mayúsculas y minúsculas
- La contraseña debe tener vigencia mínima de 6 meses, para el cambio no deberá ser una anterior.

Literal 41. Los empleados de la organización deben obligatoriamente cambiar las contraseñas temporales que se les asignan para los diferentes sistemas y recursos tecnológicos de la organización, utilizando lo que dicta el literal anterior.

Literal 42. El área de TICs debe establecer los mecanismos apropiados para asegurarse que los usuarios a cambien las contraseñas por defecto o temporales de los diferentes sistemas y recursos tecnológicos, esto se realizará obligatoriamente en el primer intento de autenticación.

Literal 43. El área de TICs debe garantizar que el almacenamiento de contraseñas de los empleados se lo realice utilizando métodos criptográficos para garantizar su confidencialidad.

Literal 44. El área de TICs se reserva el derecho de monitorear, auditar y bloquear los accesos de los usuarios a la información cuando lo amerite.

Literal 45. El área de TICs restringirá el acceso a los sistemas cuando se generen mantenimientos a los mismos.

Literal 46. El área de TICs no ejecutará el procedimiento de Alta de usuarios si no existe la solicitud de acceso de manera formal por parte de Talento Humano, la solicitud se la realizará mediante el uso del sistema de Tickets de soporte que maneja la organización.

d) Control de acceso a las redes y servicios asociados

Literal 47. Para garantizar el acceso autorizado a las redes y servicios informáticos, la organización debe contar con las herramientas que permitan gestionar correctamente el acceso, para ello es muy importante y obligatorio contar un controlador de dominio o directorio activo.

Literal 48. Para evitar el acceso no autorizado a la red de la organización, el área de TICs deberá desactivar lógicamente en los conmutadores los puntos de red no utilizados, controlando de esta manera el acceso no autorizado.

Literal 49. Los usuarios o personal externo no pueden hacer uso de los puntos de red sin previa autorización del área de TICs.

4.5.5.2 Gestión de acceso de usuario

Objetivo: Busca garantizar el acceso autorizado a los diferentes sistemas y servicios informáticos de SWEADEN Seguros.

e) Gestión de altas/bajas en el registro de usuarios

Literal 50. En el proceso de vinculación del personal, Talento Humano solicitará mediante un ticket de soporte al área de TICs la creación de accesos para el nuevo colaborador, luego de que este haya sido registrado en el módulo de nómina.

Literal 51. Es responsabilidad exclusiva del área de Talento Humano solicitar la creación de usuarios al área de TICs.

Literal 52. El área de Talento Humano notificará de manera escrita al área de TICs sobre la desvinculación de los colaboradores para ejecutar inmediatamente el procedimiento de Baja de usuarios.

f) Gestión de los derechos de acceso asignados a usuarios

Literal 53. El área de TICs asignará los accesos a los usuarios sobre las funciones de los sistemas sólo con la autorización de las jefaturas nacionales, luego de haberse ingresado el ticket de soporte.

Literal 54. Para la asignación de funciones en el sistema SIA, el área de TICs empleará el procedimiento de asignación de roles SIA estipulado.

Literal 55. La asignación de funciones, roles en los diferentes sistemas, obligatoriamente deben tener la autorización de las jefaturas nacionales.

g) Gestión de los derechos de acceso con privilegios especiales

Literal 56. El área de TICs asignará acceso con privilegios especiales para los recursos informáticos siempre que exista una autorización de la Alta Dirección de SWEADEN Seguros.

Literal 57. El coordinador de TICs deberá asignar privilegios de gestión a sus colaboradores para servidores GNU/Linux habilitando el programa **sudo**, de esta manera se garantiza el acceso y ejecución de programas con privilegios de seguridad para cada usuario.

h) Retirada o adaptación de los derechos de acceso

Literal 58. El área de Talento Humano notificará por escrito al área de TICs del cambio o cese de funciones de los empleados para que se ejecute el procedimiento de Alta y Baja de Usuarios.

4.5.5.3 Responsabilidades de los usuarios

Objetivo: Se busca que los usuarios sean responsables sobre la protección de la información aplicando mecanismos de seguridad que garanticen su identificación y acceso.

i) Uso de información confidencial para la autenticación

Literal 59. Los usuarios no deberán mostrar ni compartir sus contraseñas a terceros.

Literal 60. Los usuarios de SWEADEN Seguros no deberán usar las credenciales de usuario de otro colaborador para acceder a los sistemas de información y aplicaciones de la organización.

Literal 61. Es responsabilidad de los usuarios almacenar de manera segura sus contraseñas evitando ser mostradas o anotadas en lugares de fácil acceso como monitores, o escritorios.

Literal 62. Los usuarios deberán bloquear sus pantallas o sesiones al ausentarse de sus puestos de trabajo.

Literal 63. Es responsabilidad de los usuarios el uso que haga con los accesos asignados para los diferentes sistemas de información y aplicaciones de la organización.

Literal 64. En caso de que los usuarios identifiquen alguna anomalía, fallo o amenaza en los sistemas de producción de la organización o en los programas informáticos utilizados, deberán reportar al área de TICs para su respectivo proceso de verificación y tratamiento.

Literal 65. Es responsabilidad del usuario crear una contraseña con un alto nivel de complejidad para el uso de correo electrónico corporativo, la misma que no deberá ser divulgada a terceros.

Literal 66. El usuario es el único responsable del uso que le pueda dar al correo electrónico corporativo.

Literal 67. Es responsabilidad del usuario crear contraseñas con un alto nivel de complejidad para el uso los sistemas y aplicaciones de la organización, las mismas que no deberán ser divulgadas a terceros.

4.5.5.4 Control de acceso a sistemas y aplicaciones

Objetivo: Este objetivo de control busca garantizar el acceso a los sistemas y recursos de información de SWEADEN Seguros sea el autorizado.

j) Procedimientos seguros de inicio de sesión

Literal 68. Con respecto a dispositivos de comunicación como: *switchs, routers, firewalls* el área de TICs de SWEADEN Seguros deberá modificar las contraseñas por defecto antes de colocar estos equipos en producción.

Literal 69. Para el acceso a los diferentes recursos de información de SWEADEN Seguros deberá contar con un gestor de acceso a la información, entiéndase a este gestor como un controlador de dominio o directorio activo.

Literal 70. Los inicios de sesión de los usuarios a los diferentes sistemas y aplicaciones obligatoriamente deberán guardar un histórico o *logs* para temas de auditorías e incidentes de seguridad.

Literal 71. Las contraseñas de los usuarios para los sistemas SIA, Diamante, correo electrónico corporativo y aplicaciones obligatoriamente deberán tener un nivel Alto de complejidad.

Literal 72. Para el inicio de sesión de sistemas críticos se deberán establecer obligatoriamente mecanismos de seguridad con factor de doble autenticación.

Literal 73. El área de TICs debe asegurarse que todos los usuarios establezcan contraseñas para el acceso e inicio de sesión en los ordenadores asignados.

4.5.6 CIFRADO

4.5.6.1 Controles criptográficos

Objetivo: Busca garantizar la confidencialidad, autenticidad y la integridad de la información mediante la implementación de algoritmos criptográficos seguros.

a) Política de uso de los controles criptográficos

Literal 74. El área de TICs debe implementar mecanismos de seguridad para sus procesos a través de la utilización de algoritmos de encriptación siendo por defecto AES.

Literal 75. Para garantizar la confidencialidad y autenticidad de la información, el área de TICs debe garantizar que cualquier contraseña de los usuarios se almacene de manera encriptada en las bases de datos implementadas.

4.5.7 SEGURIDAD FÍSICA Y AMBIENTAL

4.5.7.1 Áreas seguras

Objetivo: Evitar el daño, robo e interrupción y acceso no autorizado a las instalaciones y áreas de procesamiento de información.

Literal 76. El acceso a los sitios de procesamiento y almacenamiento de información exclusivamente los centros de datos deben poseer la seguridad física necesaria, esto quiere decir que deben brindar la seguridad contra accesos no autorizados, mediante el uso de mecanismos seguros que permitan la autenticación monitoreo y registro.

Literal 77. El acceso al área de TICs está restringido para el personal externo, proveedores, asesores de seguros, clientes.

Literal 78. Todos los accesos a los centros de datos como oficinas deben ser actualizados, monitoreados y revocados según sea el caso.

4.5.7.2 Seguridad de los equipos

Objetivo: Evitar el daño, robo de los activos de información.

a) Instalaciones de suministro

Literal 79. Los equipos de la organización deben contar con fuentes adicionales de energía (UPS).

Literal 80. El centro de datos de SWEADEN Seguros debe contar obligatoriamente con respaldos de energía de manera que no se vean afectadas las operaciones del negocio por la interrupción del fluido eléctrico.

b) Mantenimiento de los equipos

Literal 81. Es responsabilidad del analista de soporte de SWEADEN Seguros diseñar el cronograma de mantenimiento correctivo y preventivo de equipos de manera anual.

Literal 82. El analista de soporte es el responsable de ejecutar el cronograma de mantenimiento correctivo y preventivo de equipos.

Literal 83. El mantenimiento correctivo y preventivo de equipos es una función exclusiva del área de TICs.

Literal 84. Para una mejor coordinación el analista de soporte debe notificar a los usuarios con anticipación del mantenimiento correctivo de equipos.

c) Seguridad de los equipos y activos fuera de las instalaciones

Literal 85. Es obligación del usuario notificar al área de TICs cuando un equipo va a salir de la organización, para gestionar su autorización.

d) Política de puesto de trabajo despejado y bloqueo de pantalla

Literal 86. Para evitar el acceso a la información o a aplicaciones sin autorización, los usuarios deben emplear obligatoriamente el bloqueo de pantalla cuando se ausenten de su lugar de trabajo.

Literal 87. El área de TICs debe implementar políticas de bloqueo de sesión en los ordenadores luego de 10 minutos de inactividad de manera obligatoria.

4.5.8 SEGURIDAD EN LA OPERATIVA

4.5.8.1 Responsabilidades y procedimientos de operación

Objetivo: Asegurar la correcta operación de las funciones del área de TICs.

a) Documentación de procedimientos de operación

Literal 88. El área de TICs debe documentar y actualizar los manuales de subprocesos de tecnología de manera periódica según corresponda.

Literal 89. Para SWEADEN Seguros los subprocesos de tecnología mínimos requeridos serán: de desarrollo, de soporte, de respaldos, de bases de datos, de contingencias.

Literal 90. Es responsabilidad del coordinador de TICs de SWEADEN Seguros gestionar la aprobación de los manuales de subprocesos del área de TICs.

Literal 91. El área de TICs debe sociabilizar con la organización los manuales de los subprocesos de tecnología.

Literal 92. El área de TICs debe generar manuales e instructivos sobre la operación de los diferentes sistemas implementados, para ser sociabilizados con todos los involucrados.

Literal 93. Las bases de datos de la organización no deben ser manipuladas por ninguna circunstancia, de existir casos extraordinarios se debe aplicar el procedimiento de cambios en bases de datos luego de obtener la aprobación de la Alta Dirección y del coordinador de TICs además de ser una tarea ejecutada exclusivamente por el administrador de bases de datos.

b) Separación de entornos de desarrollo, pruebas y producción

Literal 94. El área de TICs debe separar los ambientes de desarrollo y producción para la implementación de los desarrollos *in-house* que ejecuta.

Literal 95. Es responsabilidad de los desarrolladores utilizar el entorno de desarrollo y pruebas para sus implementaciones antes del paso a producción, de esta manera se evita el acceso y afectación no autorizada a los sistemas de producción.

4.5.8.2 Copias de seguridad

Objetivo: Proteger la información mediante copias de seguridad y definir un grado aceptable contra la pérdida de datos.

a) Copias de seguridad de la información

Literal 96. El área de TICs debe establecer mecanismos seguros para la ejecución, monitoreo y control de copias de seguridad de la información crítica: Bases de datos, versionamiento del código fuente de los sistemas desarrollados.

Literal 97. Es responsabilidad del coordinador del área de TICs establecer la periodicidad de las copias de seguridad de información crítica.

Literal 98. Es responsabilidad del analista de seguridad monitorear y comprobar que las copias de seguridad generadas sean útiles, para garantizar la recuperación de la información ante algún evento o incidente de seguridad.

Literal 99. Es responsabilidad de cada usuario almacenar en las nubes de almacenamiento asignadas la información que considere crítica.

Literal 100. El área de TICs debe garantizar que las copias de seguridad de la información crítica tengan redundancia, es decir debe existir respaldos a nivel local como fuera de las instalaciones para garantizar la continuidad de las operaciones.

Literal 101. El coordinador del área de TICs es el único responsable de eliminar copias de seguridad, para lo cual previamente deberá informar a la Dirección y solicitar su autorización.

4.5.8.3 Gestión de la vulnerabilidad técnica

Objetivo: Proteger los activos de información ante la explotación de vulnerabilidades técnicas publicadas.

a) Gestión de las vulnerabilidades técnicas

Literal 102. Es responsabilidad del área de TICs mantener actualizados los sistemas operativos en los servidores donde se ejecutan las aplicaciones y bases de datos de la organización.

Literal 103. El coordinador del área de TICs es el responsable de gestionar las actualizaciones en los servidores donde se ejecutan las aplicaciones y bases de datos de la organización.

Literal 104. El coordinador de TICs es el responsable de gestionar la aplicación de parches de seguridad crítica, en los servidores donde se ejecutan las aplicaciones y bases de datos de la organización.

Literal 105. El coordinador del área de TICs es el responsable de autorizar o ejecutar operaciones de reinicio, apagado o encendido en los servidores donde se ejecutan las aplicaciones y bases de datos de la organización.

Literal 106. El área de TICs es responsable de aplicar parches de seguridad a los sistemas operativos de todos los equipos de los usuarios de la organización, para esto deberá establecer un plan de actualización de software, asegurando que las últimas versiones y parches de seguridad sean instalados lo antes posible, con la finalidad de evitar que alguna vulnerabilidad sea explotada.

Literal 107. El analista de seguridades establecerá los procedimientos para la gestión de las vulnerabilidades con el objetivo de analizar las amenazas de seguridad de manera periódica, considerando las publicaciones de las agencias especializadas como CVE y OWASP, a fin de establecer las mitigaciones correspondientes.

4.5.9 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

4.5.9.1 Seguridad en los procesos de desarrollo

Objetivo: Busca garantizar que los desarrollos de los sistemas se diseñen e implementen considerando el ciclo de vida de desarrollo.

a) Política de desarrollo seguros de software

Literal 108. Para cambios significativos en los sistemas debe existir un Consejo Consultor de Cambios CAB (*Change Advisory Board*), el mismo que estará compuesto por integrantes de todas

las áreas involucradas y por integrantes del área de TICs con la finalidad de evaluar, autorizar y priorizar la programación de los cambios.

Literal 109. El área de TICs debe operar ambientes de desarrollo y producción por separado, además de gestionar versionamiento en el código fuente y ejecutables de los sistemas de la organización.

Literal 110. Todos los desarrollos de la organización deben ser incluidos en un repositorio central SVN para tener control de versiones de código y administrar los archivos y directorios a lo largo del tiempo por los desarrolladores de una forma segura y adecuada.

Literal 111. El área de TICs tiene como responsabilidad gestionar y llevar un inventario de las copias de seguridad del código fuente de los sistemas.

Literal 112. Es responsabilidad de los desarrolladores de SWEADEN Seguros generar e incluir *logs* de seguridad en las aplicaciones implementadas con la finalidad de establecer trazabilidad de las operaciones realizadas por los usuarios en los sistemas desarrollados.

b) Procedimientos de control de cambios en los sistemas

Literal 113. Es responsabilidad del gestor de bases de datos documentar y mantener actualizado el diccionario de datos para llevar un control de las definiciones de los datos.

Literal 114. Es responsabilidad y función exclusiva del gestor de base de datos, gestionar los permisos, privilegios y administración de las bases de datos de la organización.

Literal 115. Para toda solicitud de desarrollo o cambios en los sistemas se debe generar un ticket de desarrollo para empezar con el subproceso de Desarrollo de Software *In House* de la organización.

Literal 116. Es responsabilidad exclusiva de las jefaturas nacionales registrar o autorizar las solicitudes de cambio de sistemas en la herramienta de *HelpDesk* organizacional.

Literal 117. Toda elaboración de sistemas debe cumplir con las normas establecidas en el subproceso de Desarrollo de Software *In House* de la organización. El cumplimiento de las normas es un requisito indispensable para considerar un sistema apto para su liberación definitiva a producción.

Literal 118. Es responsabilidad del responsable de aseguramiento de calidad de software (QA) gestionar la liberación de los desarrollos a producción.

Literal 119. Es responsabilidad del responsable de aseguramiento de calidad de software (QA) gestionar y controlar todas las fases del subproceso de Desarrollo de Software *In House*.

Literal 120. Es responsabilidad del área de TICs actualizar periódicamente las normas y lineamientos del subproceso de Desarrollo de Software *In House* de la organización, con el objetivo de fomentar la aplicación de buenas prácticas para el desarrollo seguro.

Literal 121. Es responsabilidad del área de Desarrollo de sistemas documentar todas las solicitudes de cambios en los sistemas considerando lo que dicta el subproceso de Desarrollo de Software *In House* de la organización.

Literal 122. En la elaboración y diseño de sistemas informáticos el área de Desarrollo será responsable de cumplir con el ciclo de vida de un sistema mediante la metodología institucional adoptada. Entre los documentos que se generarán por los desarrolladores, están: la solicitud de desarrollo, manual de procedimientos, documento de análisis, documento de diseño, documento de pruebas técnicas y manual de usuario.

c) Pruebas funcionales en el desarrollo de los sistemas

Literal 123. Es responsabilidad del área de Desarrollo hacer uso de los ambientes de desarrollo para realizar las pruebas funcionales de los sistemas implementados antes de ser implantados en producción.

d) Pruebas de aceptación

Literal 124. En el manual de subprocesos de Desarrollo *In House* se deben estipular los procedimientos para que los usuarios o solicitantes acepten y se aprueben los cambios antes de dar paso a producción.

Literal 125. Ningún desarrollo será liberado a producción sin que el usuario solicitante y el responsable del aseguramiento de calidad del software (QA) hayan realizado pruebas funcionales y aceptado los cambios del requerimiento mediante un email o respuesta al ticket de solicitud de cambio.

4.5.10 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

4.5.10.1 Gestión de incidentes en la seguridad de la información y mejoras

Objetivo: Una vez que los incidentes de seguridad hayan sido comunicados, se deben establecer los mecanismos y procedimientos para su tratamiento.

a) Notificación de los eventos de seguridad de la información

Literal 126. Todos los empleados de SWEADEN Seguros que utilicen los sistemas de información, tienen la obligación de reportar al área de TICs cualquier incidente o falla de seguridad detectado en los sistemas.

Literal 127. Es responsabilidad del área de TICs documentar y administrar una bitácora de eventos e incidentes de seguridad con la finalidad de puedan ser solventados o mitigados de manera que no sean un riesgo para las operaciones de la organización.

Literal 128. El área de TICs debe realizar capacitar de manera periódica a los usuarios para que estos puedan detectar e informar de los eventos e incidentes de seguridad que pueden generarse.

b) Respuesta a los incidentes de seguridad

Literal 129. El área de TICs y el Analista de seguridades de la información deben establecer los procedimientos y planes de respuesta ante los posibles incidentes de seguridad, el objetivo es contener los daños y minimizar los riesgos.

Literal 130. Es responsabilidad del analista de seguridades de la información realizar evaluaciones de forma regular para detectar vulnerabilidades, amenazas del entorno y de los sistemas con el objeto de aplicar los procedimientos adecuados para su control y mitigación.

4.5.11 ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

4.5.11.1 Continuidad de la seguridad de la información

Objetivo: Establecer los mecanismos y procedimientos para poder reaccionar ante fallas, ataques o desastres en los sistemas de información minimizando las interrupciones en las operaciones del negocio

a) Planificación de la continuidad de la seguridad de la información

Literal 131. Es responsabilidad del área de TICs y del Analista de seguridad planificar y diseñar los planes de continuidad del negocio como BCP y DRP para contrarrestar las interrupciones o amenazas.

Literal 132. La continuidad del negocio de las operaciones del área de TICs debe cumplir con los siguientes puntos:

- Identificación de los activos críticos a proteger.
- Elaborar el plan de continuidad del negocio y contingencias donde se establecerán los responsables y las responsabilidades de los usuarios.
- Se deberán realizar pruebas periódicas a los planes para garantizar su efectividad.
- Los planes de continuidad del negocio y contingencias siempre deberán estar actualizados.

b) Implantación de la continuidad de la seguridad de la información

Literal 133. La Alta Dirección de SWEADEN Seguros debe apoyar al área de TICs para la implementación de un Plan de Continuidad del Negocio BCP (*Business Continuity Plan*), con esto la organización podría reaccionar ante un incidente de seguridad permitiéndole restablecer sus operaciones de manera segura.

Literal 134. La organización debe implementar con un Plan de Recuperación de Desastres DRP (*Disaster Recovery Plan*), con la finalidad de proteger los datos, el hardware y el software crítico del negocio, dotándole de mecanismos que le permitan recuperarse ante un desastre natural o daños provocados por el ser humano.

Literal 135. La organización debe apoyar, aprobar los presupuestos de los recursos necesarios para que el área de TICs pueda implementar planes de continuidad y contingencias, sitios alternos, redundancias que permitan restablecer las operaciones del negocio ante un evento de seguridad de la información o desastres naturales.

CAPÍTULO V

CONCLUSIONES Y TRABAJOS FUTUROS

5.1 Conclusiones

Mediante el uso de la metodología MAGERIT y dando cumplimiento al primero de los objetivos planteados en estas investigación, se pudo generar una matriz que permitió identificar todos los problemas y riesgos que mantiene la organización actualmente, entre los hallazgos se pudo notar que las falencias de mayor impacto sobre la seguridad de la información tienen relación con: Planes de contingencia y continuidad, Control de acceso y Proceso de Desarrollo, por lo que, la implementación de los controles basados en la norma ISO/IEC 27002:2013 generan ventajas frente al control y mitigación de las amenazas y vulnerabilidades de dichos riesgos ya que mejoran significativamente la confidencialidad, integridad y disponibilidad de la información.

Con la presente investigación se pudo mostrar que SWEADEN Seguros a pesar de poseer documentación de políticas de tecnología, y manuales de procedimientos de tecnología, carece aún de controles eficientes que le permitan gestionar adecuadamente la seguridad de la información, esto puede afectar a la organización con una interrupción temporal o definitiva de sus operaciones, para ello es necesario contar con una política de seguridad de manera formal la misma que permitirá controlar y mitigar los riesgos asociados con los activos de información.

De los resultados obtenidos en la encuesta realizada al personal de la organización sobre temas de Seguridad de la Información, se pudo evidenciar que el personal tiene un conocimiento básico referente a la protección de los datos organizacionales, por lo que es importante que el área de TICs de SWEADEN Seguros desarrolle talleres y capacitaciones de manera periódica para que todos los involucrados con los procesos de información conozcan los procedimientos y mejores prácticas para el adecuado tratamiento de esta.

Cada organización tiene necesidades específicas, por consiguiente, para la elaboración del diseño de una política de seguridad de la información no es necesario considerar todos los controles de seguridad estipulados en la norma ISO/IEC 27002, ya que la selección e implementación de estos dependerá de la priorización y necesidad del negocio para mitigar los riesgos que posee.

Tomando como referencia la norma ISO 27002:2013 se pudo determinar que SWEADEN Seguros posee una deficiencia significativa en los siguientes dominios de seguridad: Seguridad en las operaciones, Continuidad del negocio, Control de accesos, Seguridad ambiental y física y Seguridad en los Procesos de Desarrollo, por lo tanto, debe priorizarse la implementación de los controles en cada uno de estos dominios.

Finalmente, las ventajas de implementar los controles de la ISO 27002:2013 y contar con una política formal de seguridad de la información ayudan a que las empresas puedan: Generar conciencia sobre la seguridad de la información, Identificar y controlar riesgos asociados a la misma, controlar sus activos de información críticos, entre otros, reduciendo de esta manera los problemas con la seguridad de la información.

5.2 Recomendaciones

Se recomienda que la Política de Seguridad de la Información sea socializada con todo el personal de SWEADEN Seguros, para que se contribuya con la seguridad de esta y se conozcan los posibles riesgos y amenazas a las cuales están expuestos.

Se recomienda que la organización priorice e implemente los controles para la mitigación de los riesgos más críticos mencionados en la matriz de riesgo, entre ellos: Implementación de un controlador de dominio para controlar el acceso a la red y la implementación de los planes BCP y DRP de manera que se asegure la continuidad del negocio y sus operaciones.

Es importante mencionar que la seguridad de la información no depende únicamente del diseño de la Política de Seguridad propuesta, por lo que la implementación, evaluación y mejoramiento del plan de seguridad puede considerarse como parte de un trabajo futuro y que la organización debería ejecutar para proteger adecuadamente su información.

BIBLIOGRAFÍA

Agustín López Neira, J. R. (2012). iso27000.es. Obtenido de http://www.iso27000.es

Aliaga, L. (2013). DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA UN INSTITUTO EDUCATIVO . Lima.

Avellaneda, J. C. (2014). Ciberseguridad, minuto y resultado: Los malos 3, Los buenos 0. Obtenido de http://seguridad-de-la-informacion.blogspot.com/2014/05/ciberseguridad-minuto-y-resultado-los.html

Buendía, J. F. (2013). Seguridad Informática. Madrid: McGraw-Hill/Interamericana de España.

C., N. A. (2010). SEGURIDAD EN SISTEMAS DE INFORMACIÓN . Venezuela.

Carvajal, A. (2013). INSEGURIDAD DE LA INFORMACIÓN - GUÍA PRÁCTICA PARA IMPLEMENTAR LA SEGURIDAD DE LA INFORMACIÓN. Bogotá: UNIMINUTO.

Chávez, J. D. (2015). SEGURIDAD INFORMÁTICA PERSONAL Y CORPORATIVA. Venezuela: IEASS.

Consejo Superior de Administración Electrónica. (2012). Libro I MAGERIT.

Consejo Superior de Administración Electrónica. (2012). Libro II MAGERIT.

Consejo Superior de Administración Electrónica. (2012). Libro III MAGERIT.

Excellence, I. (1 de 2 de 2018). https://www.pmg-ssi.com. Obtenido de ISOTools: https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

Garzón, J. (2016). DESARROLLO DE UN PLAN DE RIESGOS DE SEGURIDAD PARA EL PROCESO DE EMISIÓN DE PÓLIZAS PARA UNA EMPRESA DE SEGUROS DEL ECUADOR, SIGUIENDO LA NORMA ISO 27001:20130. Guayaquil.

Huacanés, R. (2016). Implementacion de la Norma ISO/IEC 27002:2013 Sección Control de Acceso para las aplicaciones Informáticas de la Aseguradora del Sur. Quito.

INTECO. (2010). SGSI Implantación de un SGSI en la empresa.

ISO. (2005). International Organization for Standardization. Obtenido de https://www.iso.org/standard/42103.html

ISO. (2018). Obtenido de https://www.iso.org/standard/73906.html

ISO/IEC. (2018). International Standar ISO/IEC 27000.

ISO27002.es. (2013). Aquisición, desarrollo y Mantenimiento de los sistemas de información. Obtenido de

http://iso27000.es/iso27002_14.html

ISO27002.es. (2013). Aspectos de la SI en la Gestión de la Continuidad de Negocio. Obtenido de http://iso27000.es/iso27002_17.html

ISO27002.es. (2013). Aspectos Organizativos SI. Obtenido de http://iso27000.es/iso27002_6.html#home

ISO27002.es. (2013). Cifrado. Obtenido de http://www.iso27000.es/iso27002_10.html

ISO27002.es. (2013). Control de Accesos. Obtenido de http://iso27000.es/iso27002_9.html#home

ISO27002.es. (2013). Cumplimiento. Obtenido de http://iso27000.es/iso27002_18.html

ISO27002.es. (2013). Gestión Activos. Obtenido de http://iso27000.es/iso27002_8.html#home

ISO27002.es. (2013). Gestión de Incidentes. Obtenido de http://iso27000.es/iso27002_16.html

ISO27002.es. (2013). Políticas Seguridad. Obtenido de http://www.iso27000.es/iso27002_5.html

ISO27002.es. (2013). Relaciones con Suministradores. Obtenido de http://www.iso27000.es/iso27002_15.html

ISO27002.es. (2013). Seguridad en la Operativa. Obtenido de http://www.iso27000.es/iso27002_12.html

ISO27002.es. (2013). Seguridad en las Telecomunicaciones. Obtenido de http://iso27000.es/iso27002_13.html

ISO27002.es. (2013). Seguridad física y Ambiental. Obtenido de http://iso27000.es/iso27002_11.html#home

ISO27002.es. (2013). Seguridad Ligada a los recursos humanos. Obtenido de http://iso27000.es/iso27002_7.html#home

ISOTools. (2016). La norma ISO 27001: Aspectos claves de su diseño e implantación.

ISOTools. (2019). SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información . Obtenido de https://www.pmg-ssi.com/2016/09/iso-27001-diferencia-entre-evento-e-incidente/

Javier Ruiz Spohr, J. R. (2012). http://iso27000.es/. Obtenido de El portal de ISO 27001 en Español.

Martín, M. M. (2015). Guía de implantación de un SGSI basado en la norma UNE-ISO/IEC 27001. Universitat Oberta de Catalunya.

normasapa.com. (2019). NORMAS APA 2019 – EDICIÓN 6. Obtenido de https://normasapa.com/normas-apa-2019-cuestiones-mas-frecuentes/

Pereira, J. A. (2013). Plan de implementación de la norma ISO/IEC 27001. España.

Rodríguez, J. M., & Peralta, I. (2013). Gestión de Riesgos MAGERIT. Obtenido de https://www.tithink.com/publicacion/MAGERIT.pdf

Soriano, M. (2014). Seguridad en redes y seguridad de la información.

Soto, M. G. (2018). Análisis de Malware para. Madrid: RA-MA Editorial.

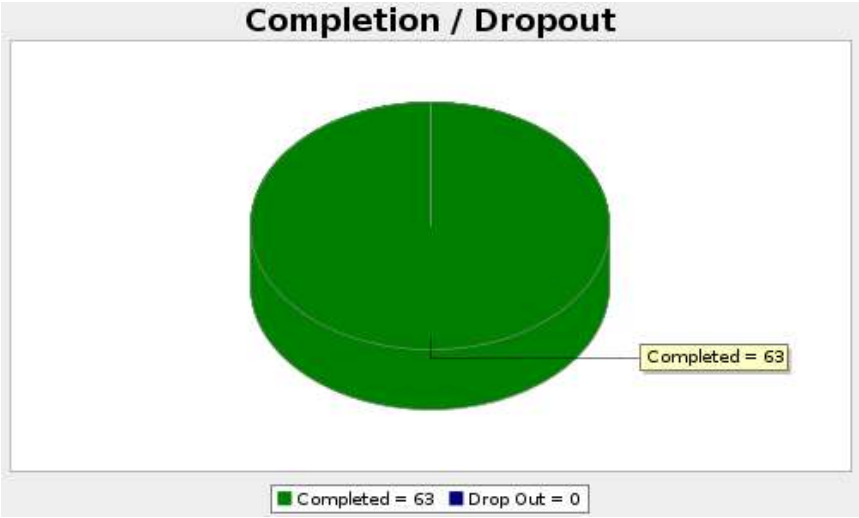
SUAREZ, S. (2015). ANÁLISIS Y DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA EN LA EMPRESA ASEGURADORA SUÁREZ PADILLA & CÍA.LTDA, QUE BRINDE UNA ADECUADA PROTECCIÓN EN SEGURIDAD INFORMÁTICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA ORGANIZACIÓN. Bogotá.

SWEADEN. (s.f.). Obtenido de https://www.sweadenseguros.com/index.php/info/gobierno-corporativo/codigo-de-etica

SWEADEN. (s.f.). Obtenido de https://www.sweadenseguros.com/index.php/nuestra-empresa/la-empresa/sobre-nosotros

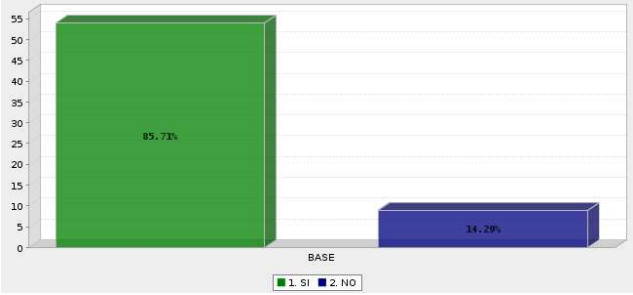
ANEXOS

Resumen Encuesta Test de seguridad



Vistas	Iniciado	Completado	Completion Rate	Drop Outs (After Starting)	Average Time to Complete Survey
111	**63**	**63**	**100%**	**0**	**3 minutes**

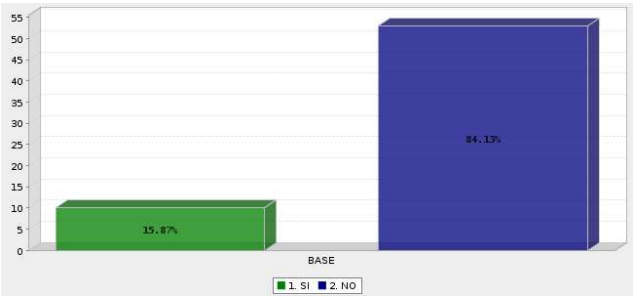
Q1. ¿Conoces que es una contraseña fuerte?



	Pregunta	Conteo	Porcentaje
1.	SI	54	85.71%
2.	NO	9	14.29%
	Total	63	100%

Mean : **1.143**	Confidence Interval @ 95% : **[1.056 - 1.230]**	Standard Deviation : **0.353**	Standard Error : **0.044**

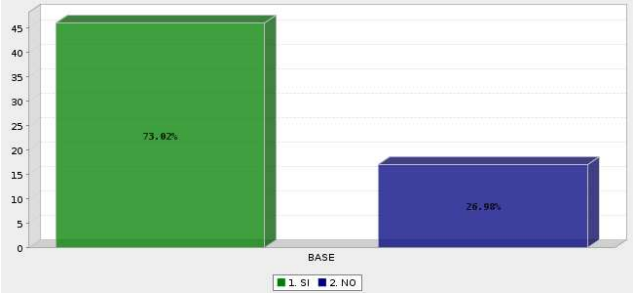
Q2. ¿Conoces que es un sistema de autenticación de doble factor?



	Pregunta	Conteo	Porcentaje
1.	SI	10	15.87%
2.	NO	53	84.13%
	Total	63	100%

Mean : **1.841**	Confidence Interval @ 95% : **[1.750 - 1.932]**	Standard Deviation : **0.368**	Standard Error : **0.046**

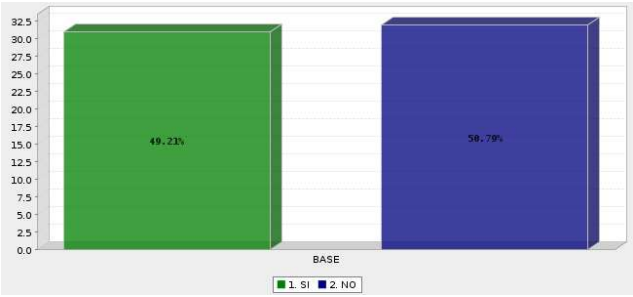
Q3. ¿Existe un departamento o encargado de seguridad informática en la organización?



	Pregunta	Conteo	Porcentaje
1.	SI	46	73.02%
2.	NO	17	26.98%
	Total	63	100%

Mean : **1.270**	Confidence Interval @ 95% : **[1.159 - 1.380]**	Standard Deviation : **0.447**	Standard Error : **0.056**

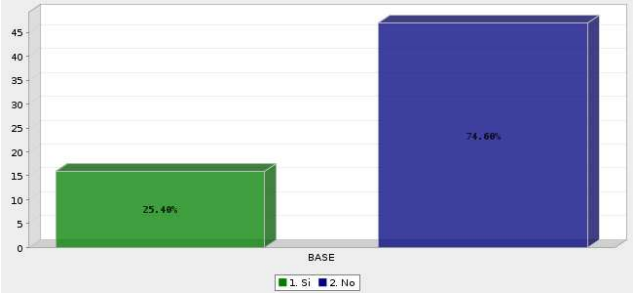
Q4. ¿Realizas copias de seguridad de tu información?



	Pregunta	Conteo	Porcentaje
1.	SI	31	49.21%
2.	NO	32	50.79%
	Total	63	100%

Mean : **1.508**	Confidence Interval @ 95% : **[1.383 - 1.632]**	Standard Deviation : **0.504**	Standard Error : **0.063**

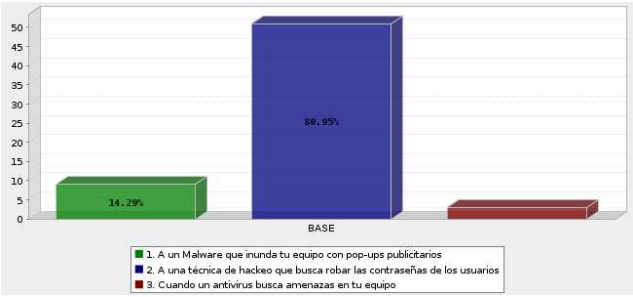
Q5. ¿Crees que es mejor tener una misma contraseña para todas tus cuentas?



	Pregunta	Conteo	Porcentaje
1.	Si	16	25.40%
2.	No	47	74.60%
	Total	63	100%

Mean : **1.746**	Confidence Interval @ 95% : **[1.638 - 1.854]**	Standard Deviation : **0.439**	Standard Error : **0.055**

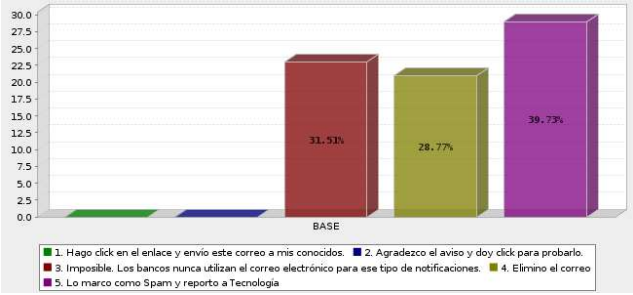
Q6. ¿A qué considerarías Phishing?



	Pregunta	Conteo	Porcentaje
1.	A un Malware que inunda tu equipo con pop-ups publicitarios	9	14.29%
2.	A una técnica de hackeo que busca robar las contraseñas de los usuarios	51	80.95%
3.	Cuando un antivirus busca amenazas en tu equipo	3	4.76%
	Total	63	100%

Mean : **1.905**	Confidence Interval @ 95% : **[1.799 - 2.011]**	Standard Deviation : **0.429**	Standard Error : **0.054**

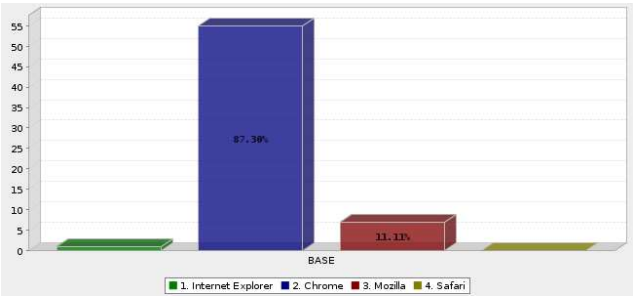
Q7. Tengo una cuenta de ahorros en MiBanco y me llega un correo de info@mibancos.ec donde me avisan de que hay una nueva web donde cambiar las claves:



	Pregunta	Conteo	Porcentaje
1.	Hago click en el enlace y envío este correo a mis conocidos.	0	0.00%
2.	Agradezco el aviso y doy click para probarlo.	0	0.00%
3.	Imposible. Los bancos nunca utilizan el correo electrónico para ese tipo de notificaciones.	23	31.51%
4.	Elimino el correo	21	28.77%
5.	Lo marco como Spam y reporto a Tecnología	29	39.73%
	Total	73	100%

Mean : **4.082**	Confidence Interval @ 95% : **[3.888 - 4.276]**	Standard Deviation : **0.846**	Standard Error : **0.099**

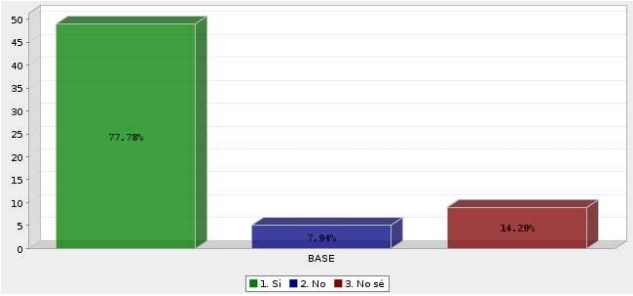
Q8. ¿Qué navegador web utilizas normalmente?



	Pregunta	Conteo	Porcentaje
1.	Internet Explorer	1	1.59%
2.	Chrome	55	87.30%
3.	Mozilla	7	11.11%
4.	Safari	0	0.00%
	Total	63	100%

Mean : **2.095**	Confidence Interval @ 95% : **[2.010 - 2.181]**	Standard Deviation : **0.346**	Standard Error : **0.044**

Q9. ¿Tienes software antivirus instalado en tu computador?



	Pregunta	Conteo	Porcentaje
1.	Si	49	77.78%
2.	No	5	7.94%
3.	No sé	9	14.29%
	Total	63	100%

Mean : **1.365**	Confidence Interval @ 95% : **[1.186 - 1.544]**	Standard Deviation : **0.725**	Standard Error : **0.091**

Q10. ¿Crees que es necesario una inducción sobre seguridad informática en la organización?

	Pregunta	Conteo	Porcentaje
1.	Si	63	100.00%
2.	No	0	0.00%
	Total	63	100%

Mean : **1.000**	Confidence Interval @ 95% : **[1.000 - 1.000]**	Standard Deviation : **0.000**	Standard Error : **0.000**

Controles ISO/IEC 27002:2013

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

5. POLÍTICAS 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. GESTIÓN 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.

ISO27002.es PATROCINADO POR:

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.