



UNIVERSIDAD TECNICA DEL NORTE

FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS

CARRERA DE INGENIERIA EN ELECTRONICA Y REDES DE COMUNICACIONES

**METODOLOGÍA DE UN SISTEMA DLP (DATA LOSS PREVENTION) PARA LA
ENTIDAD FINANCIERA “COOPERATIVA DE AHORRO Y CRÉDITO SANTA ANITA
LTDA.” BASADA EN LA NORMA ISO/IEC 27002:2022, SECCIÓN 5.12 Y 8.12**

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

AUTOR: MARÍA JOSÉ CAUJA ALTAMIRANO

DIRECTOR: MSC. MAURICIO HERNÁN DOMÍNGUEZ LIMAICO

ASESOR: MSC. FABIÁN GEOVANNY CUZME RODRÍGUEZ.

Ibarra- Ecuador

2024



UNIVERSIDAD TÉCNICA DEL NORTE BIBLIOTECA UNIVERSITARIA

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

1. IDENTIFICACIÓN DE LA OBRA

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

DATOS DE CONTACTO		
CÉDULA DE IDENTIDAD:	1003785381	
APELLIDOS Y NOMBRES:	Cauja Altamirano María José	
DIRECCIÓN:	Río Curaray y Río Quinindé	
EMAIL:	mjcaujaa@utn.edu.ec	
TELÉFONO FIJO:	062605033	TELÉFONO MÓVIL: 0984987837


DATOS DE LA OBRA	
TÍTULO:	Metodología de un sistema DLP (Data Loss Prevention) para la entidad financiera "Cooperativa de Ahorro y Crédito Santa Anita Ltda." Basada en la norma ISO/IEC 27002:2022, sección 5.12 y 8.12
AUTOR (ES):	Cauja Altamirano María José
FECHA DE APROBACIÓN:	05 de febrero de 2024
PROGRAMA:	<input checked="" type="checkbox"/> PREGRADO <input type="checkbox"/> POSGRADO
TÍTULO POR EL QUE OPTA:	Ingeniería en Electrónica y Redes de Comunicación
ASESOR /DIRECTOR:	MSc. Mauricio Hernán Domínguez Limaico MSc. Fabián Geovanny Cuzme Rodríguez

2. CONSTANCIAS

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

Ibarra, a los 5 días del mes de febrero de 2024

EL AUTOR:

(Firma) 
Nombre: Cauja Altamirano María José
1003785381



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS
CARRERA DE INGENIERIA EN ELECTRONICA Y REDES DE
COMUNICACIONES

CERTIFICACIÓN

MAGISTER MAURICIO DOMÍNGUEZ, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN CERTIFICA:

Que el presente trabajo de Titulación: "METODOLOGÍA DE UN SISTEMA DLP (DATA LOSS PREVENTION) PARA LA ENTIDAD FINANCIERA "COOPERATIVA DE AHORRO Y CRÉDITO SANTA ANITA LTDA." BASADA EN LA NORMA ISO/IEC 27002:2022, SECCIÓN 5.12 Y 8.12". Ha sido desarrollo por la señorita Cauja Altamirano María José bajo mi supervisión

Es todo cuanto puedo certificar en honor a la verdad.

A handwritten signature in blue ink, written over a horizontal line. The signature is stylized and appears to read 'Mauricio Domínguez'.

MSc. Mauricio Hernán Domínguez Limaico

DIRECTOR

DEDICATORIA

Este trabajo de titulación no solo simboliza un logro individual, sino también un homenaje que dedico a mi hija por su amor incondicional, su apoyo constante y su fe inquebrantable en mí, los cuales han sido mi principal fuente de motivación en este trayecto.

Lo dedico a mi familia, que siempre han apoyado cada paso. A mi madre, quien ha sido un ejemplo vivo de lucha y paciencia, una inspiración constante. A mis hermanos, quienes han representado el equilibrio entre los momentos de triunfo y los desafíos.

Y a mi pareja, por ser esa persona que siempre me ha impulsado con sus ocurrencias y palabras de ánimo, mi cómplice en innumerables momentos y un ejemplo de lealtad incondicional.

Este logro es fruto del esfuerzo conjunto y, en cada página de este trabajo, se reflejan, el esfuerzo y el compromiso compartidos, los desafíos superados en nuestra travesía juntos. A lo largo de los años, ustedes han sido mi red de seguridad, mi fuente de fortaleza y mi constante fuente de inspiración.

AGRADECIMIENTO

Quiero expresar mi gratitud a Dios, cuya fe me ha permitido comprender que, con dedicación, todo es posible. En este viaje académico, he aprendido que la perseverancia es una parte esencial de este camino.

Agradezco a mi hija Katalyna por ser mi motivación para continuar, agradeciéndole por su fe en mí y reconociendo que su amor y comprensión han sido un sostén invaluable que me ha impedido rendirme.

A mi madre Magdalena, mis hermanos Freddy, Jenny, Liliana, y mi hermana gemela Belén, les agradezco por su apoyo incondicional para alcanzar mis sueños y finalizar este ciclo importante en mi vida.

A Ayrthon, quien nunca perdió la fe en mi capacidad y estuvo presente en todas mis etapas, su respaldo y afecto alimentaron mi esperanza de lograr este objetivo.

A los amigos que hice durante la carrera, quiero agradecerles; porque fueron aquellos que, a través de risas, noches difíciles, frustraciones y logros, me enseñaron el valor de la amistad. Fueron fundamentales en mi crecimiento profesional y emocional, demostrándome que un gran equipo se forma con respeto y responsabilidad.

Agradezco a la institución financiera "Cooperativa de Ahorro y Crédito Santa Anita Ltda" por su colaboración esencial en la elaboración de este trabajo de grado. En particular, mi reconocimiento al departamento de TIC, que me proporcionó orientación y la información necesaria para llevar a cabo la investigación.

Por último, a mi director de tesis MSc Mauricio Domínguez y a mi asesor Msc. Fabián Cuzme, les agradezco su disposición y compromiso con mi crecimiento académico y personal es algo que siempre atesoraré y valoraré.

Contenido

DEDICATORIA	III
AGRADECIMIENTO	V
RESUMEN	XIV
1. CAPITULO I	1
ANTECEDENTES	1
1.1. Tema.....	1
1.2. Planteamiento del Problema.....	1
1.3. Objetivos	2
1.3.1. Objetivo General.....	2
1.3.2. Objetivos Específicos.....	2
1.4. Alcance.....	3
1.5. Justificación.....	5
2. CAPITULO II.....	7
FUNDAMENTACIÓN TEÓRICA	7
2.1. Seguridad de la Información	7
2.1.1. Tipos de Seguridad	8
2.1.2. Principios de la seguridad	8
2.1.3. Prevención de fuga de información	10
2.2. Metodología para análisis y gestión de riesgo Magerit V3.0.....	11
2.2.1. Organización de las guías	12
2.2.2. Método de análisis de riesgo.....	13
2.3. Organización Internacional para la Estandarización – ISO.....	21
2.3.1. ISO/IEC 27000- Seguridad de la Información.....	22
2.3.2. Análisis de la norma técnica ISO/IEC 27002	24

2.3.3.	Actualización de la Norma ISO 27002:2022	24
2.3.4.	Requisitos según la norma ISO/IEC 27002:2022	25
2.3.5.	Estructura de la Norma 27002:2022	28
2.4.	Data Loss Prevention	33
2.4.1.	Funcionamiento de DLP	34
2.4.2.	Productos Data Loss Prevention	36
2.4.3.	Método DLP.....	37
2.4.4.	Arquitectura DLP.....	38
2.4.5.	Plataforma de Software DLP	40
3.	CAPITULO III.....	43
	SITUACIÓN ACTUAL.....	43
3.1.	Situación Actual	43
3.1.1.	Misión	44
3.1.2.	Visión.....	44
3.1.3.	Servicios prestados por la COAC Santa Anita Ltda.	44
3.1.4.	Política de Privacidad	45
3.1.5.	Organigrama Estructural.....	46
3.2.	Sistema de Gestión por Procesos	48
3.2.1.	Mapa de Procesos	48
3.2.2.	Macroprocesos	49
3.2.3.	Proceso.....	50
3.2.4.	Manual y Procedimiento.....	50
3.2.5.	Procedimiento de recuperación operativa.....	51
4.	CAPITULO IV.....	54
	METODOLOGIA DE SEGURIDAD Y ANALISIS DE RIESGO.....	54

4.1. Metodología de Investigación	54
4.1.1. Tipo de investigación	54
4.1.2. Técnicas de recolección de información	55
4.2. Matriz de los activos de información	56
4.3. Análisis y Gestión de riesgo mediante la Metodología Magerit v3.0	63
4.3.1. Contexto	63
4.3.2. Determinación de activos	64
4.3.3. Se elabora identificación de los activos de información	66
4.3.4. Dependencia entre activos	70
4.3.5. Valoración de activos	70
4.3.6. Identificación de amenazas	72
4.3.7. Valoración de amenazas	74
4.3.8. Impacto acumulado	75
4.3.9. Riesgo Acumulado	77
4.3.10. Salvaguardas	78
4.3.11. Valoración de Salvaguardas	81
4.4. Desarrollo de manual para la prevención de fuga de información	82
4.4.1. Reportes de cumplimiento de la norma 27002:2022	82
4.4.2. Manual para prevención de fuga de información	83
4.4.3. Manual de Políticas y Procedimiento de Prevención de Fuga de Información	
83	
5. CAPITULO V	86
HERRAMIENTA DATA LOSS PREVENTION	86
5.1. Requerimientos para la herramienta Data Loss Prevention	86
5.1.1. Stakeholders	86

5.1.2.	Requerimientos de Stakeholders	87
5.1.3.	Requerimientos del sistema	88
5.1.4.	Requerimientos de Arquitectura	91
5.2.	Comparativa de Herramientas de análisis	92
5.3.	Herramienta ManageEngine DataSecurity Plus	93
5.3.1.	Arquitectura LAN	94
5.3.2.	Detalles de la licencia	96
5.3.3.	Cotización de precio de la herramienta ManageEngine	97
5.3.4.	Módulo de prevención de pérdida de datos	99
5.3.5.	Manual de configuración herramienta ManageEngine Data Loss Prevention 101	
6.	CONCLUSIONES	111
7.	RECOMENDACIONES	113
8.	REFERENCIAS.....	114
9.	ANEXOS	120

Índice de Figuras

Figura 1. Marco de Trabajo para la gestión de riesgos	12
Figura 2. Elementos de análisis de riesgos potenciales	14
Figura 3. Datos en Reposo	35
Figura 4. Datos en Movimiento	35
Figura 5. Datos en Uso.....	36
Figura 6. Inspección profunda de contenido (DCI)	38
Figura 7. Representación técnica de Datos en uso y movimiento	39
Figura 8. Representación técnica de Datos en reposo.....	40
Figura 9. Arquitectura Típica DLP	40
Figura 10. Servicios prestados por la COAC Santa Anita Ltda.....	45
Figura 11. Organigrama Estructural	47
Figura 12. Sistema de Gestión de Procesos	48
Figura 13. Mapa de Procesos Integral.....	49
Figura 14. Macroprocesos.....	50
Figura 15. Procesos de Gestión de Negocios.....	50
Figura 16. Procedimientos de Gestión de crédito y cobranzas	51
Figura 17. Estructura de los procedimientos para la recuperación operativa	53
Figura 18. Creación del proyecto PILAR	64
Figura 19. Código de Identificación	66
Figura 20. Activos del proceso de recuperación operativa	69
Figura 21. Dependencia de activos	70
Figura 22. Valoración de activos Software PILAR	71

Figura 23. Valoración del dominio de seguridad de los activos de la información	72
Figura 24. Valor de activos Proceso Recuperación Operativa	72
Figura 25. Identificación de amenazas de los activos de recuperación operativa	73
Figura 26. Valoración según su nivel y porcentaje	75
Figura 27. Impacto acumulativo	76
Figura 28. Impacto acumulado en el proceso de recuperación operativa	77
Figura 29. Riesgo Acumulado	78
Figura 30. Peso Relativo	80
Figura 31. Identificación de salvaguardas la entidad financiera COAC Santa Anita	80
Figura 32. Valoración de Salvaguardas	81
Figura 35. Arquitectura LAN dispositivos finales	94
Figura 36. Módulos de prevención de pérdida de datos	100

Índice de Tablas

Tabla 1. Criterio de evaluación de degradación.....	27
Tabla 2. Probabilidad de ocurrencia	27
Tabla 3. Valores representativos para estimar el riesgo	29
Tabla 4. Matriz de impacto	30
Tabla 5. Norma ISO/IEC 27000	32
Tabla 6. Tabla de Atributos de Clasificación de la información	38
Tabla 7. Prevención de fuga de información	40
Tabla 8. Participantes y responsabilidades	61
Tabla 9. Descripción de activo de la información	66
Tabla 10. Identificación Básica del activo de la información.....	68
Tabla 11. Identificación Básica del activo de la información.....	70
Tabla 12. Tipos de activos según Metodología Magerit.....	72
Tabla 13. Clasificación de Activos	74
Tabla 14. Probabilidad de ocurrencia	80
Tabla 15. Tipo de protección	86
Tabla 20.Requerimientos	90
Tabla 21. Abreviatura de Stakeholders	91
Tabla 22. Requerimientos de Stakeholder	91
Tabla 23. Requerimiento de sistema.....	91
Tabla 24. Requerimientos de Arquitectura	95

Índice de Anexos

9.1. ANEXOS A Entrevista para levantamiento de información de activos de información	120
9.2. ANEXOS B. Entrevista la Infraestructura Tecnológica COAC “Santa Anita”	122
9.3. ANEXOS C. Encuesta sobre la herramienta Data Loss Prevention	123
9.4. ANEXOS D. Matriz Levantamiento Activos de la Información	126
9.5. ANEXOS E. Valoración de activos para COAC “Santa Anita Ltda”	128
9.6. ANEXOS F. Valoración de Amenazas para COAC “Santa Anita Ltda”	146
9.7. ANEXOS G. Análisis de Riesgo para COAC “Santa Anita Ltda”	155
9.8. ANEXOS H. Cumplimiento ISO/IEC 27002:2022	168
9.9. ANEXOS I. Guía Para Elaboración y Gestión De Documento	171

RESUMEN

Este proyecto de titulación analiza la metodología de un sistema de prevención de filtración de datos para la entidad financiera "Cooperativa de Ahorro y Crédito Santa Anita Ltda", basado en las secciones 5.12 y 8.12 de la norma ISO/IEC 27002:2022. Esta guía tiene como objetivo prevenir la filtración de información mediante políticas de seguridad de la información.

La metodología se divide en varias etapas. En la primera etapa, se lleva a cabo un relevamiento de la información de los activos de la entidad financiera según lo establecido en la sección 5.12 de la norma ISO/IEC 27002:2022. En la segunda etapa, se realiza un análisis de riesgos utilizando la Metodología MAGERIT V3 para recopilar información sobre amenazas y salvaguardas, lo que permite analizar la prevención de la filtración de información y los riesgos asociados a los activos de información. La tercera etapa implica el establecimiento de políticas y procedimientos adecuados para la prevención de la filtración de información dentro del proceso de recuperación operativa de la entidad financiera, basados en las buenas prácticas de seguridad de la información y en el marco de la norma ISO/IEC 27002:2022. Finalmente, en la cuarta etapa, se presenta una herramienta que satisfaga las necesidades de la entidad financiera y permita establecer políticas de seguridad de la información, junto con un manual de configuración como resultado entregable.

Esta investigación da como resultado una estructura documental que consta de dos manuales y una guía. El Manual de Prevención de Fuga de Información describe cómo el procedimiento de recuperación operativa de la entidad financiera cumple con los requisitos de la norma ISO/IEC 27001, utilizando la metodología ISO/IEC 27002:2022 siendo el punto de partida para el análisis de las políticas y procedimientos de prevención de filtración de información. Además, la guía de elaboración y gestión de documentos establece formatos que ayudan a determinar ciertas características de la información necesaria para comprender el proceso.

ABSTRACT

This degree project analyzes the methodology of a data leak prevention system for the financial entity "Cooperativa de Ahorro y Crédito Santa Anita Ltda", based on sections 5.12 and 8.12 of the ISO/IEC 27002:2022 standard. This guide aims to prevent information leaks by determining information security policies.

The methodology is divided into several stages. In the first stage, one survey of the information on the assets of the financial entity is carried out as established in section 5.12 of the ISO/IEC 27002:2022 standard. In the second stage, one risk analysis is carried out using the MAGERIT V3 Methodology to collect information on threats and safeguards, which makes it possible to analyze the prevention of information leakage and the risks associated with information assets. The third stage involves the establishment of appropriate policies and procedures for the prevention of information leaks within the operational recovery process of the financial entity, based on good information security practices and within the framework of the ISO/IEC standard. 27002:2022. Finally, in the fourth stage, a tool is presented that meets the needs of the financial institution and allows establishing information security policies, along with a configuration manual as a deliverable result.

This investigation results in a documentary structure that consists of two manuals and one guide. The Information Leak Prevention Manual describes how the financial institution's operational recovery procedure meets the requirements of the ISO/IEC 27001 standard, using the ISO/IEC 27002:2022 methodology as a starting point for policy analysis. and information leak prevention procedures. In addition, the document preparation and management guide establishes formats that help determine certain characteristics of the information necessary to understand the process.

1. CAPITULO I

ANTECEDENTES

Este capítulo detalla las bases fundamentales para el desarrollo de trabajo de titulación basada en la norma ISO/IEC 27002:2022, para la entidad financiera Cooperativa Santa Anita Ltda. Se describe de manera precisa el tema, la problemática, los objetivos, el alcance y la justificación, con el propósito de denotar la importancia de llevar a cabo este trabajo

1.1.Tema

Metodología de un Sistema DLP (Data Loss Prevention) para la entidad financiera “Cooperativa de Ahorro y Crédito Santa Anita Ltda.” Basada en la norma ISO/IEC 27002:2022, sección 5.12 y 8.12.

1.2.Planteamiento del Problema

La (Cooperativa de Ahorro y Crédito Santa Anita Ltda., 2011) Es una institución financiera que ha tenido un crecimiento progresivo de agencias por el cual se han expandido en diferentes lugares del país, por otro lado, la información que administra es su activo principal, por lo tanto, la protección de los datos conlleva diversos escenarios y responsables de preservarla, si por el contrario la información se encuentra propensa a la filtración de datos esto podría ocasionar varias consecuencias desafortunadas, si llegara a manos equivocadas.

Actualmente, la entidad carece de controles que protejan la información y prevenga violaciones de datos, internas como externas, debido a que son organizaciones que manejan información valiosa y económica de sus clientes, de este modo cualquier usuario que acceda a los equipos puede sustraerla por medio de cualquier dispositivo de almacenamiento. En realidad, la institución no presenta ningún mecanismo dedicado para el control, prevención y detección de fuga de información que asegure la confidencialidad y privacidad de la información.

En este sentido, la institución debe determinar las amenazas y vulnerabilidades, simultáneamente establecer la estructura de la organización para adecuarlo a las políticas de seguridad, permitiendo verificar el potencial de riesgo que presenta, además permita dar cumplimiento a la normativa legal presente en Ecuador. (Abg. Cuarán Betty, 2021)

Según (Yuya & Ramani, 2017), el sistema de prevención de pérdida de datos (DLP) se ha convertido en una estrategia importante de seguridad en la época informática. Los programas Data Loss Prevention son productos o servicios que protegen la información confidencial del uso compartido accidental o malicioso fuera de las áreas de confianza especificadas.

En síntesis, lo que se pretende frente al problema anteriormente descrito, es dar una solución mediante la implementación de controles de filtración de datos accidentales y malintencionadas de la entidad financiera con el objetivo de dar cumplimiento a la seguridad informática.

1.3.Objetivos

1.3.1. Objetivo General

Proponer una metodología de seguridad basada en la ISO/IEC 27002:2022 con la herramienta Data Loss Prevention para la detección de fuga de datos, dirigido a la entidad financiera Cooperativa de Ahorro y Crédito Santa Anita Ltda., para que los datos confidenciales no sean vulnerados

1.3.2. Objetivos Específicos

- Fundamentar el estado del arte en bases bibliográficas, con el fin de comprender el funcionamiento y características del sistema Data Loss Prevention, así como la normativa ISO/IEC 27002, sección 5.12 y 8.12.

- Establecer el estado actual de los datos de la entidad financiera según las políticas y procedimientos de seguridad que requieren.
- Proponer la metodología de seguridad basada en el estándar ISO/IEC 27002, sección 5.12 y 8.12, aplicado a la infraestructura tecnológica de la institución financiera.
- Proporcionar una guía sobre la documentación fundamental que respalda todos los criterios de seguridad, el cual se implementa en el sistema Data Loss Prevention

1.4.Alcance

La propuesta de trabajo de investigación plantea el desarrollo de una metodología de seguridad basada en la Norma ISO/IEC 27002 vigente al 2022, para la entidad financiera Cooperativa de Ahorro y Crédito Santa Anita Ltda. con el propósito de habilitar un conjunto de controles globales de seguridad de la información estandarizado, de manera que faculte complementarlo con el sistema Data Loss Prevention (DLP),

Se inicia con el desarrollo de un estudio bibliográfico que brinda una descripción detallada de la norma (ISO/IEC 27002, 2022a), esto va a permitir determinar que sección puede ser aplicable según las especificaciones requeridas, del mismo modo se investiga el funcionamiento y las características del sistema Data Loss Prevention determinando los requerimientos para el sistema, para lo cual la observación directa de la documentación verifica las actividades realizadas.(Wáshington Marcelo Contero Ramos, 2019)

Luego de obtener todos los conocimientos teóricos, se continúa con el análisis de la situación actual de los datos, esto se realiza con la ayuda de los administradores del sistema de gestión de seguridad de la información (SGSI). De esta manera, se efectuará un levantamiento de información para identificar los datos, determinar las políticas y procedimientos aplicables con base (ISO/IEC 27002, 2022a) en la sección 5.12, perteneciente a la clasificación de la información,

de acuerdo a las necesidades de seguridad de los datos, las organizaciones pueden determinar el nivel de protección para cada activo de información en función de la importancia y sensibilidad de la información confidencial para clasificarla y etiquetarla, según los estándares reconocidos de la industria en diferentes niveles de riesgo.(Ministerio de Tecnologías de la Información y Comunicaciones de COLOMBIA, 2016)

Por lo tanto, se utilizará como referencia la norma (ISO/IEC 27002, 2022a) para definir e implementar controles y prevenir riesgos de seguridad de la información, que define ciertos requisitos que permiten a cualquier organización planificar, implementar y gestionar las actividades necesarias para su desarrollo y satisfacción del cliente/usuario, siempre con un enfoque basado en procesos. Aunque el estándar se encuentra estructurado en diferentes secciones, en el desarrollo de este trabajo se consideran únicamente los enunciados 5.12 antes mencionado, y 8.12 que se basa estrictamente en la prevención de fugas de información, la cual se trata de un control dual tanto preventivo como detectivo, que modifica el riesgo mediante la implementación de medidas técnicas, que detectan y previenen proactivamente la divulgación y/o recuperación de datos, ya sea por personal interno y/o externo, o sistemas lógicos.(Romo Daniel & Valarezo Joffre, 2012)

Las etapas establecidas para la metodología se llevará inicialmente la fase de clasificación de la información con base en el apartado 5.12 de la norma ISO/IEC 27002:2022 proporciona las directrices de clasificación correspondientes a los criterios establecidos por la entidad financiera que debe optar por definir el esquema adecuado de clasificación, basándonos en el esquema de clasificación se detalla así el método por el cual se etiquetan de acuerdo con el medio de almacenamiento de activos de información de la entidad. La fase de Prevención de fugas de información se desarrolla a partir de la sección 8.12, de la citada norma, en la que se efectuarán

las políticas teniendo en cuenta las medidas proactivas para la prevención de filtración de los datos, así también la restricción según los requerimientos y administración de cada usuario. Finalmente, la fase de resultados es validada por el sistema Data Loss Prevention implementando las políticas y limitaciones que se han expuesto. (ISMS, 2022)

Se propone en base a la investigación expuesta, un sistema Data Loss Prevention que pueda ser implementada en el sistema operativo Windows y permita monitorear, inspeccionar y prevenir la fuga de datos de información en la red. Con la utilización de políticas y una adecuada supervisión para prevenir la fuga de información, los administradores de la entidad financiera puedan gestionar el riesgo de filtraciones. Finalmente se proporcionará una guía detallada que pueda usarse como punto de partida para luego establecer e implementar políticas de seguridad basadas en un proceso de Data Loss Prevention, el cual será flexible y estará sujeto a revisiones, modificaciones a medida que la realidad vaya cambiando. (Edwar Rodolfo Chalá Ibarra, 2020)

1.5. Justificación

La seguridad de la información es la protección de datos mediante diferentes implementaciones, procesos de respaldo establecidos y el almacenamiento de datos en ubicaciones restringidas. Sin embargo, las instituciones financieras son vulnerables a los riesgos y amenazas comunes de las brechas de seguridad, y que a menudo, resulta en la pérdida de información, debido a la falta de controles físicos y lógicos apropiados. (Yandún Marco & Cando Eduardo Patricio, 2018)

En Ecuador, la (Superintendencia de Economía Popular y Solidaria, 2022) emite una resolución referente a “Normas de control sobre los principios y lineamientos de educación financiera”. Bajo la supervisión de la misma, explica la necesidad de emitir normas de gestión de

seguridad de la información que ayuden a fortalecer los procesos internos de las instituciones del Sector Financiero Popular y Solidario.

Por ende, la entidad financiera Cooperativa de ahorro y crédito “Santa Anita”. Ltda. conforma el régimen especial, en el que de acuerdo con el Artículo 19, Medidas de seguridad de la información, deberá aplicarse los controles mínimos. Este trabajo propuesto se justifica con los apartados respecto al Inventario y clasificación de información, que se ajusta a las normas de control de gestión, y aquellos procedimientos para el Respaldo y resguardo de información sensible o crítica, para la administración del riesgo legal en las entidades del Sector Financiero Popular y Solidario bajo el control de la Superintendencia de Economía Popular y Solidaria. (Superintendencia de Economía Popular y Solidaria, 2022).

Por tanto, ejecutar una metodología de enfoque acorde a la norma ISO/IEC 27002:2022 permitirá la organización y coordinación de cada proceso, que se realiza de forma aislada y mal organizada, para evitar fugas de información, permitiendo además mantener una infraestructura tecnológica segura, sobre todo en el manejo de recursos y hará posible la administración de políticas de seguridad tanto internas como externas. (Ministerio de Industria y Comercio de España, 2017)

El Manual de control de seguridad de la información para la prevención y gestión de fuga de información propuesto en el presente trabajo, será de gran utilidad porque recopilará datos de la institución financiera y acciones que los responsables del manejo del Sistema de Gestión de Seguridad de la información deben llevar a cabo para garantizar que los procesos se realicen bajo condiciones controladas. Además, la propuesta, brinda la posibilidad de contar con un documento técnico y formal que servirá como principio para una posterior implementación del SGSI

2. CAPITULO II

FUNDAMENTACIÓN TEÓRICA

Este capítulo se enfoca en presentar una fundamentación teórica relevante para el análisis de la norma ISO/IEC 27002:2022 y su impacto en las organizaciones financieras. Se detalla específicamente los controles 5.12 (Clasificación de la información) y 8.12 (Prevención de fuga de información), y se explica cómo llevar a cabo la gestión de la información. También se determinan las características de las plataformas de Prevención de Pérdida de Datos (DLP), que se podrá utilizar como herramienta para demostrar las políticas de seguridad de la entidad financiera.

2.1.Seguridad de la Información

De acuerdo con la (ISO 27001, 2013), la información puede ser una herramienta poderosa que puede ayudar a una organización a prosperar o a destruirse. La gestión adecuada de la seguridad de la información brinda confianza y permite a las empresas expandirse, renovarse y aumentar su base de clientes, con la certeza de que sus datos confidenciales se mantendrán de esa manera.

Si bien la seguridad de la información y la seguridad informática comparten algunos puntos clave, existen diferencias importantes entre ambos conceptos, especialmente en términos de su ámbito de aplicación.

La seguridad informática se refiere a un conjunto de procesos, dispositivos y herramientas diseñados para mantener la privacidad, integridad y disponibilidad de los datos almacenados en un sistema informático, al tiempo que se reducen las posibles amenazas.

Por otro lado, de acuerdo con (Romero Castro et al., 2018) la seguridad de la información no se focaliza en los sistemas informáticos como tal, sino en todas las cosas susceptibles de contener información.

2.1.1. Tipos de Seguridad

Las medidas de seguridad más próximas a los activos de información son la identificación, autenticación y autorización de usuarios, contraseñas, claves, firewall, encriptación, antivirus, entre otros.

Estas se dividen en dos tipos diferentes, sean seguridad activa o seguridad pasiva, con el fin de prevenir contrarrestar o disminuir riesgos

Seguridad Pasiva. La seguridad pasiva consiste en los mecanismos puestos en marcha para mejorar el proceso de recuperación tras un percance en su seguridad. Estas defensas no reducen el riesgo del incidente, sino, tienen como finalidad minimizar sus efectos negativos o remediar los daños que se hayan producido. (Ruiz Larrocha Elena, 2017)

La seguridad pasiva aplica la protección de los componentes físicos del sistema de información, los cuales incluyen tanto elementos físicos como los sistemas operativos, aplicaciones y contenido de información. Estos elementos son susceptibles a accidentes de seguridad, por lo que hay que aplicar medidas de recuperación. (Aguilera López, 2011)

Seguridad Activa. Los elementos y procedimientos de seguridad activa tienen el propósito de descubrir o impedir los peligros que afectan al sistema de información. Estas acciones de seguridad se realizan tanto en los aspectos físicos como lógicos de un sistema de información. (Aguilera López, 2011)

Igualmente, que los mecanismos de seguridad pasiva, estos se incorporan tanto a las partes hardware como a las lógicas del sistema y pueden ser tanto materiales como digitales.

2.1.2. Principios de la seguridad

(Singh et al., 2018) considera que cualquier sistema de información, como una red informática, software, computación en la nube, etc., requiere la presencia de tres factores para la

seguridad de los datos o información contenida en el sistema. Esto se conoce como triada CIA, que hace referencia a Confidencialidad, Integridad y Disponibilidad.

Confidencialidad. Como señala (Vega Briceño Edgar, 2020), es la condición que garantiza que la información no esté disponible o que no pueda ser descubierta por personas, entidades o procesos no autorizados. Por ejemplo, cuando se realiza una transacción con tarjeta de crédito en línea, el número de la tarjeta debe ser transmitido desde el comprador al comerciante. Si una persona con intenciones maliciosas logra acceder al número de tarjeta, se infringe la confidencialidad.

En entornos comerciales, la confidencialidad garantiza la protección que brindan leyes y estrategias para salvaguardar la información privada. Entre los mecanismos usados para mantener la confidencialidad se incluyen el control de acceso a los sistemas a través de técnicas específicas y el cifrado de datos confidenciales.

Integridad. Citando a (Bijani Chiquero Gopal, 2017), la integridad se encarga de garantizar que la información almacenada no sea manipulada o corrompida por usuarios no autorizados, ya sea desde su creación o transmisión por medio de una red informática.

Esto significa que cuando los datos sean extraídos o recuperados nuevamente, deben tener los mismos valores cargados originalmente sin ningún cambio en su forma o contenido.

Disponibilidad. La disponibilidad de la información según (Singh et al., 2018), se relaciona a la accesibilidad de los datos y recursos cuando se lo requiera, ya sea por usuarios autorizados, entidades o dispositivos. Los efectos de la no disponibilidad de la información dependen de su nivel de confidencialidad. También corresponde a la protección de los recursos y las capacidades necesarias asociadas.

2.1.3. Prevención de fuga de información

Los profesionales de seguridad de datos tienen como una de sus principales preocupaciones la mitigación de las amenazas internas y la prevención de filtraciones de datos. Lamentablemente, las amenazas internas a menudo pasan desapercibidas. En la mayoría de los casos, cuanto más tiempo pase sin ser detectadas, mayores serán los daños resultantes.

La prevención de pérdida de datos (DLP) comenzó a utilizarse en 2006 y ganó cierta popularidad en 2007.

(Alkilani et al., 2019) menciona que Data Loss Prevention es un conjunto de tecnologías productos y técnicas diseñadas para evitar que la información sensible salga de una organización. Un sistema de DLP incluye un conjunto de reglas y políticas que clasifican los datos, el cual el sistema supervisa las actividades de los usuarios finales, el flujo de datos, así como el acceso a la información confidencial, así como los datos enviados a través de la red. Si se detecta alguna actividad sospechosa, se activa una alerta del sistema.

Riesgo. Es cierto que los riesgos que se originan a partir de tecnología suelen ser cometidos por usuarios inexpertos, no se limitan exclusivamente a ellos, ya que también pueden ser causados por usuarios malintencionados o por fallas en los sistemas y aplicaciones utilizados por la empresa. Por lo tanto, es crucial tener medidas de seguridad informática adecuadas y actualizadas para prevenir y reducir estos riesgos.

De acuerdo con lo que menciona (Baca Urbina Gabriel, 2016), la importancia de alinear la arquitectura de la organización y la tecnología para garantizar una implementación efectiva de las medidas de seguridad informática.

Es esencial que la arquitectura de seguridad informática esté adecuada y adaptada a las necesidades de las instituciones, ya que si no está bien diseñada o no se actualiza regularmente,

puede haber vulnerabilidades en los sistemas y aplicaciones utilizados. Los expertos en seguridad informática pueden detectar estas vulnerabilidades y corregirlas antes de que sean explotadas por usuarios malintencionados.

Amenazas. Según la recomendación (*UIT-T X.800*, 1996), se considera una amenaza de seguridad cuando hay una posibilidad latente de que se produzca un cambio no autorizado e intencional en el estado de un sistema, lo que podría resultar en una violación de la seguridad. Esto puede incluir actividades como la modificación, destrucción, robo o divulgación no autorizada de información valiosa. Además, también se considera una amenaza de seguridad cuando hay una fuga de información, como la extracción de datos confidenciales como contraseñas, que podrían ser utilizados por terceros para realizar actividades malintencionadas, como transferencias electrónicas de dinero.

Vulnerabilidad. Las vulnerabilidades son fallos o puntos débiles en la implementación, configuración o funcionamiento de un sistema que permiten que una amenaza se materialice. Estas debilidades pueden originarse por errores de diseño, acciones maliciosas o equivocaciones humanas. Si una organización posee una vulnerabilidad en su sistema de seguridad informática, implica que existe una debilidad que podría ser explotada por un atacante para llevar a cabo una violación de seguridad. (Baca Urbina Gabriel, 2016)

2.2. Metodología para análisis y gestión de riesgo Magerit V3.0

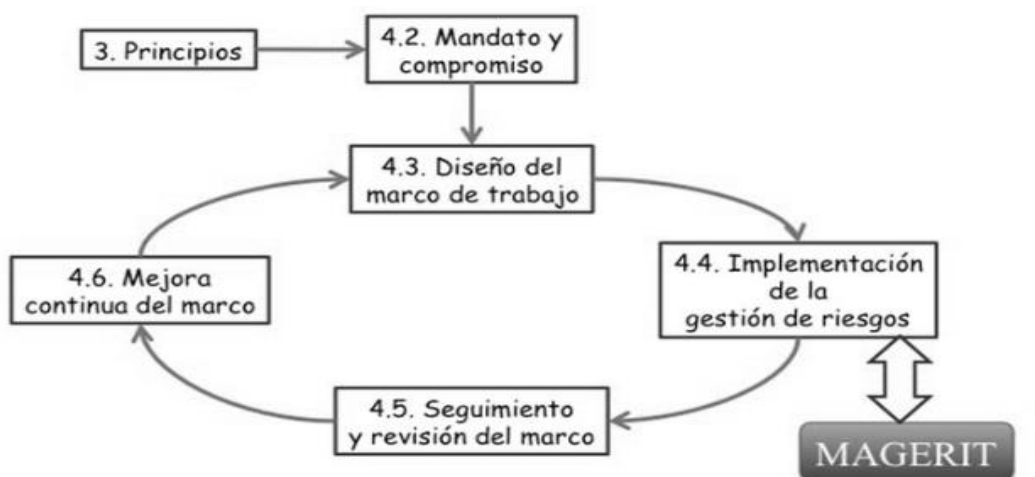
(MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información, 2012). Esta metodología es de dominio público, lo que significa que se puede utilizar libremente sin necesidad de autorización previa. Magerit se encarga de implementar el Proceso de Gestión de Riesgos dentro de un marco de trabajo, permitiendo a los órganos de gobierno tomar decisiones considerando los riesgos asociados con el uso de tecnologías de la información.

Su objetivo principal es generar conciencia entre los responsables de las organizaciones acerca de la existencia de riesgos y la importancia de manejarlos de manera adecuada. Además, ofrece un enfoque sistemático para analizar los riesgos relacionados con el uso de tecnologías de la información y comunicaciones (TIC). Asimismo, facilita la identificación y planificación del tratamiento apropiado para mantener bajo control los riesgos indirectos.

La estructura de la Metodología de análisis y riesgos de los sistemas informáticos se muestra en la Figura 1.

Figura 1.

Marco de Trabajo para la gestión de riesgos



Nota: La autoría corresponde a (MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información, 2012)

2.2.1. Organización de las guías

La versión 3.0 de la metodología Magerit se ha organizado en dos libros y una guía técnica, que se dividen de la siguiente manera:

- El Libro I- Método, proporciona una descripción detallada de los pasos y actividades necesarios para la planificación y estructura del proyecto de implementación de análisis y gestión de riesgos.

- El Libro II - Catálogo de elementos, ofrece una guía detallada sobre cómo llevar a cabo un análisis de riesgos y presenta un catálogo que abarca diferentes aspectos, como los tipos de activos, las dimensiones de valoración de dichos activos, los criterios utilizados para valorar los activos, las amenazas típicas que afectan a los sistemas de información y las salvaguardas que se deben considerar para proteger dichos sistemas.
- Guía de Técnicas: Recopilación de técnicas de diversos tipos que pueden ser útiles para aplicar el método.

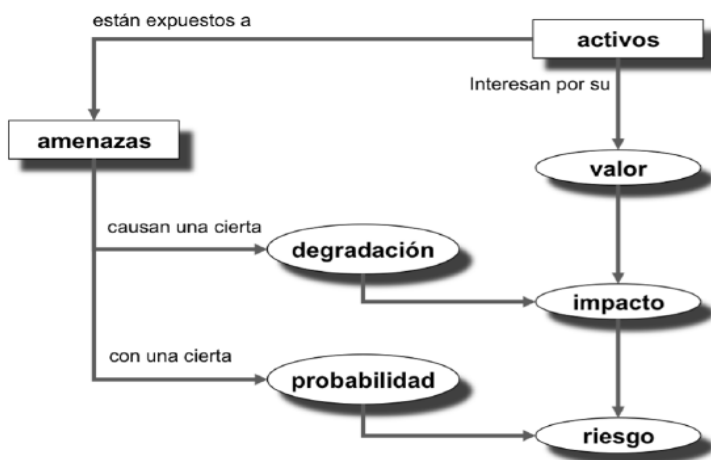
2.2.2. Método de análisis de riesgo

El libro inicial de la metodología (MAGERIT - Versión 3.0 Libro I - Método, 2012) establece los componentes del análisis de riesgo, que se representan en la Figura 2. Este libro ofrece un enfoque sistemático que orienta la evaluación del riesgo mediante una secuencia de pasos organizados de manera estructurada.

1. Identificar los activos relevantes para la organización, así como comprender su interrelación y valor, evaluando el posible perjuicio económico que podría resultar de su degradación.
2. Analizar las amenazas a las que se exponen dichos activos, identificando los posibles riesgos asociados.
3. Evaluar las salvaguardas existentes y determinar su efectividad en mitigar los riesgos identificados.
4. Estimar el impacto potencial, es decir, el daño que podría sufrir un activo específico en caso de materialización de una amenaza.
5. Calcular el riesgo, que se define como el impacto ponderado por la probabilidad de ocurrencia de la amenaza

Figura 2.

Elementos de análisis de riesgos potenciales



Nota. Autoría atribuidos a (MAGERIT – Versión 3.0 Libro I - Método, 2012)

2.2.2.1. Identificación de Activos

Los activos de la información son los elementos o funcionalidades de un sistema de información que pueden ser objeto de ataques intencionales o accidentales, y cuyas consecuencias podrían afectar a la organización.

- **Dependencias**

Los activos esenciales, que son la información y los servicios proporcionados, dependen de otros activos más tangibles, como equipos, comunicaciones, instalaciones y, a menudo, se olvidan las personas que trabajan con ellos.

Se considera que un "activo de nivel superior" depende de un "activo de nivel inferior" cuando las necesidades de seguridad del primero se reflejan en las necesidades de seguridad del segundo. En otras palabras, la materialización de una amenaza en el activo de nivel inferior tiene como resultado un perjuicio en el activo de nivel superior.

- **Valoración**

Cada activo dentro de una organización posee un valor que depende de su importancia y relevancia para la misma. A medida que aumenta el valor de un activo, también aumenta la necesidad de protegerlo adecuadamente.

El valor de un activo puede ser intrínseco o puede estar relacionado con el valor acumulado que tiene al estar vinculado con otros activos. En un esquema de dependencias, los activos de nivel inferior acumulan el valor de los activos que dependen de ellos. El valor principal suele estar asociado con la información que el sistema maneja y los servicios que se prestan (activos esenciales), mientras que los demás activos se subordinan a las necesidades de explotación y protección de los activos esenciales.

- **Dimensiones**

Dentro de los activos puede ser evaluado en diferentes dimensiones:

- **Confidencialidad:** Esta evaluación es típica en el caso de datos confidenciales y se centra en el posible perjuicio que podría ocasionarse si estos datos son revelados a personas no autorizadas.

¿Qué daño causaría que lo conociera quien no debe?

- **Integridad:** Se refiere al perjuicio que podría causar si el activo estuviera dañado o corrupto. Esta evaluación es común en datos, ya que podrían ser manipulados, falsificados total o parcialmente, o incluso faltar datos.?’

¿Qué perjuicio causaría que estuviera dañado o corrupto?

- **Disponibilidad:** Se refiere al perjuicio que causaría no tener acceso o no poder utilizar el activo. Esta evaluación es común en servicios y recursos.

¿Qué perjuicio causaría no tenerlo o no poder utilizarlo?

2.2.2.2. Identificación de Amenazas

Un posible origen de un incidente que puede ocasionar daños a un sistema de información o a una organización son las amenazas. Estas amenazas son sucesos que ocurren y nuestra preocupación radica en cómo pueden impactar nuestros recursos y causar perjuicios.

En relación a las distintas categorías de riesgos habituales, podemos mencionar las siguientes:

De origen natural: Existen fenómenos naturales que pueden ocurrir de manera impredecible. Aunque el sistema de información es una víctima pasiva frente a estos eventos, es importante tener en consideración las posibles consecuencias que puedan surgir.

Del entorno: Existen incidentes industriales ante los cuales el sistema de información se convierte en una víctima pasiva. Sin embargo, no debemos confundir pasividad con vulnerabilidad, ya que es importante tomar medidas para protegerse y no permanecer indefensos.

Defectos de las aplicaciones: Existen dificultades que surgen directamente en el equipamiento propio debido a defectos en su diseño o implementación, lo cual puede tener consecuencias negativas para el sistema. Estos problemas a menudo se conocen como vulnerabilidades técnicas o simplemente como "vulnerabilidades"

Causadas por las personas de forma accidental: Las personas que tienen acceso al sistema de información pueden ser responsables de problemas no intencionales, generalmente debido a errores o descuidos involuntarios.

Causadas por las personas de forma deliberada: Las personas que tienen acceso al sistema de información pueden ser responsables de problemas intencionales: llevando a cabo ataques deliberados, ya sea con el objetivo de obtener beneficios indebidos o de causar daños y perjuicios a los legítimos propietarios.

- **Valoración de las amenazas**

Cuando un activo se encuentra frente a una amenaza, su impacto no es uniforme en todas sus dimensiones ni en la misma medida. Después de identificar que una amenaza puede afectar a un activo, es necesario evaluar su influencia en el valor del activo en dos aspectos: la degradación, que determina el nivel de perjuicio que podría sufrir el valor del activo, y la probabilidad, que establece qué tan probable o improbable es que la amenaza se materialice.

La degradación es una medida del daño causado por un incidente en caso de que ocurra, por lo tanto, en la Tabla 1 se pueden identificar los criterios de evaluación para determinar la degradación.

Tabla 1.

Criterio de evaluación de degradación

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

Nota. Autoría propia adaptada del ejemplo proporcionado (*MAGERIT – Versión 3.0 Libro I - Método, 2012*)

Determinar y expresar la probabilidad de ocurrencia es un proceso más complejo. En ocasiones, se representa de forma cualitativa mediante el uso de una escala nominal, como se muestra en la Tabla 2.

Tabla 2.

Probabilidad de ocurrencia

	VALOR	DETALLE	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

Nota. Autoría propia adaptada del ejemplo proporcionado (*MAGERIT – Versión 3.0 Libro I - Método*, 2012)

2.2.2.3. Determinación del impacto potencial

El impacto se refiere a la medida del daño causado al activo como resultado de la materialización de una amenaza. Teniendo en cuenta el valor de los activos en diversas dimensiones y la degradación causada por las amenazas, es posible determinar directamente el impacto que estas tendrían en el sistema.

La única consideración restante se relaciona con las dependencias entre los activos. Es común que el valor del sistema se centre en la información que maneja y los servicios que brinda, pero las amenazas suelen manifestarse en los medios. Para establecer las conexiones entre ellos, recurrimos al uso de un grafo de dependencias.

Para determinar el valor del impacto, es necesario utilizar la Ecuación 1, la cual debe ser aplicada.

$$\text{Impacto} = \text{Valor del activo} * \text{Degradación del Valor}$$

Ecuación 1. Impacto potencial

2.2.2.4. Determinación del riesgo potencial

El riesgo es la evaluación del daño probable en un sistema. Se puede calcular derivando el riesgo a partir del impacto de las amenazas en los activos y considerando la probabilidad de ocurrencia. El riesgo se incrementa con un mayor impacto y probabilidad, y existen diferentes zonas que requieren atención en la gestión del riesgo.

La metodología Magerit clasifica el riesgo en cuatro zonas distintas que son:

- **Zona 1:** Se refiere a riesgos con una alta probabilidad de ocurrencia y un impacto extremadamente significativo.
- **Zona 2:** abarca un amplio espectro que va desde situaciones poco probables, pero con impacto moderado, hasta situaciones muy probables, pero con impacto bajo o muy bajo.
- **Zona 3:** Se refiere a riesgos poco probables y con un impacto bajo.
- **Zona 4:** Se trata de riesgos poco probables, pero con un impacto extremadamente significativo.
- **Riesgo acumulado**

El riesgo acumulado se calcula para cada activo, en relación a cada amenaza y en cada dimensión de valoración. Esto se logra mediante una función que tiene en cuenta el valor acumulado, la degradación causada y la probabilidad de la amenaza, como se muestra en la Ecuación 2. Al calcular el riesgo acumulado en los activos que respaldan el sistema de información, es posible identificar las salvaguardas necesarias para los recursos de trabajo, como la protección de los equipos y la realización de copias de respaldo.

$$\text{Riesgo} = \text{Probabilidad de amenaza} * \text{Impacto}$$

Ecuación 2. Riesgo

Tanto la probabilidad como la magnitud pueden adoptar valores representativos específicos para estimar el valor del riesgo, los cuales se presentan en la Tabla 3.

Tabla 3.

Valores representativos para estimar el riesgo

Valor representativo	Probabilidad de amenazas	Magnitud del Daño
5.Catastrófico	100	10
4.Crítico	10	8-9
3.Alto	1	6-7
2.Medio	1/10	4-5

1.Bajo

1/100

0-3

Nota. Autoría propia adaptada del ejemplo proporcionado (*MAGERIT – Versión 3.0 Libro I - Método, 2012*)

Al realizar el cálculo del riesgo, es esencial crear una matriz de riesgos, tal como se ilustra en la Tabla 4. Esta matriz permite comprender, según los colores utilizados, la zona de riesgo a la que pertenece, de acuerdo con la metodología Magerit.

Tabla 4.

Matriz de impacto

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

Nota. Autoría propia adaptada del ejemplo proporcionado (*MAGERIT – Versión 3.0 Libro I - Método, 2012*)

2.2.2.5.Salvuardas

Por lo tanto, se evalúan los impactos y riesgos a los que estarían expuestos los activos en caso de no contar con ninguna protección. En la práctica, es poco común encontrar sistemas completamente desprotegidos: las medidas mencionadas indican lo que sucedería si se eliminaran las salvuardas existentes.

Las salvuardas o contramedidas se definen como procedimientos o mecanismos tecnológicos que reducen el riesgo. Algunas amenazas pueden ser contrarrestadas mediante una adecuada organización, mientras que otras requieren elementos técnicos como programas o equipos, seguridad física e incluso políticas de personal.

2.2.2.6.Vulnerabilidades

Se define la vulnerabilidad como cualquier debilidad que puede ser aprovechada por una amenaza, o más específicamente, las debilidades en los activos o en las medidas de protección que facilitan el éxito de una amenaza potencial.

En términos utilizados anteriormente, las vulnerabilidades incluyen todas las ausencias o ineficiencias de las salvaguardas pertinentes para proteger el valor propio o acumulado en un activo. A veces, se utiliza el término "insuficiencia" para resaltar el hecho de que la efectividad medida de la salvaguarda no es suficiente para preservar el valor del activo expuesto a una amenaza.

2.3.Organización Internacional para la Estandarización – ISO

La Organización Internacional de Estandarización (ISO) es una entidad sin ánimo de lucro y no gubernamental que se dedica a desarrollar estándares internacionales en diversas áreas, como la fabricación y los servicios. Desde su creación en 1947, su objetivo principal ha sido facilitar transacciones internacionales y fomentar la cooperación entre países en los ámbitos científico, tecnológico y económico.

La ISO se compone de múltiples comités técnicos y grupos de trabajo que se encargan de elaborar y revisar normas en una amplia variedad de temas. Estos comités cubren desde estándares relacionados con el papel hasta las últimas tecnologías en el campo de las telecomunicaciones.

Las normas internacionales establecidas por la ISO son de gran importancia, ya que garantizan la calidad, seguridad y eficiencia de productos y servicios a nivel mundial. Además, ayudan a las empresas a mejorar su eficiencia y reducir costos al seguir un conjunto estandarizado de reglas y regulaciones.(Universidad EAFIT, n.d.)

2.3.1. ISO/IEC 27000- Seguridad de la Información

La (ISO/IEC 27000, 2018) es un conjunto de pautas y estándares que proporciona las mejores prácticas para la gestión de la seguridad de la información en diversas organizaciones de diferentes sectores. Estas normas han sido desarrolladas conjuntamente por la Organización Internacional de Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

La serie de estándares ISO 27000 abarca una variedad de normas que abordan diversos aspectos de la seguridad de la información. La norma principal es la ISO 27001, que establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI). La norma ISO/IEC 27002 proporciona un conjunto de prácticas recomendadas para la implementación y mantenimiento de un SGSI. Además de estas dos normas, existen otras en la serie ISO 27000 que también pueden ser relevantes para la implementación de un SGSI. La Tabla 5 detalla las diferentes normas de la serie ISO/IEC 27000.

Tabla 5.

Familia de la Norma ISO/IEC 27000

NORMA ISO/IEC 27000			
Aspectos	Norma	Año	Descripción
Requisitos	ISO 27001	2022	Establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Esta norma se enfoca en el proceso de gestión de la seguridad de la información, desde la planificación hasta la evaluación y mejora continua.
	ISO 27006	2015	Establece los requisitos para la certificación de un SGSI
	ISO 27009	2020	Se enfoca en los requisitos de inclusión de controles adicionales de seguridad de la información en sectores específicos.

Guía de aplicación	ISO 27002	2022	Es un código de prácticas para la gestión de la seguridad de la información. Esta norma proporciona un conjunto de controles y directrices para ayudar a las organizaciones a proteger su información y reducir el riesgo de pérdida, robo o daño a la misma.
	ISO 27003	2017	La norma proporciona orientación para la implementación de un SGSI basado en la norma ISO/IEC 27001
	ISO 27004	2016	Establece los requisitos para la medición y evaluación de la eficacia de un SGSI
	ISO 27005	2022	Proporciona directrices para la gestión de riesgos de seguridad de la información.
	ISO 27007	2020	Se enfoca en la auditoría de un SGSI, brindando orientación sobre los principios de auditoría, la gestión de un programa de auditoría, la realización de auditorías y la evaluación de la competencia de los auditores.
Requisitos Específicos	ISO 27010	2015	Estableciendo los requisitos y las mejores prácticas para garantizar la seguridad de la información en las comunicaciones entre organizaciones.
	ISO 27011	2016	Proporciona directrices específicas para la gestión de la seguridad de la información en las telecomunicaciones, tanto en las redes como en los servicios de telecomunicaciones.
	ISO 27017	2015	Establece directrices para la seguridad de la información en la nube. Se aplica a cualquier tipo de organización, incluyendo proveedores de servicios en la nube, clientes de servicios en la nube y proveedores de servicios de seguridad.

Nota. Desarrollo original con información resumida de (ISO/IEC 27000, 2018)

Estos estándares son útiles para cualquier tipo de organización, independientemente de su tamaño o sector económico, y pueden ser utilizados para implementar un SGSI eficaz que ayude a proteger la información y reducir el riesgo de pérdida, robo o daño a la misma.

2.3.2. Análisis de la norma técnica ISO/IEC 27002

La norma (*ISO/IEC 27002, 2022b*), provee un conjunto de controles genéricos de seguridad de la información junto con guías para su implementación. Esta norma ha sido creada para ser utilizada por organizaciones que buscan mejorar su seguridad de la información y puede ser usado de tres formas diferentes:

- a) En el contexto de un sistema de gestión de la seguridad de la información basado en la norma ISO/IEC 27001, para aplicar controles basados en las mejores prácticas internacionales, o
- b) Para desarrollar directrices de gestión de la seguridad de la información específicas para la organización.
- c) Esta norma incluye controles para la gestión de accesos, la gestión de activos, la gestión de incidentes de seguridad, la gestión de la continuidad del negocio, la gestión de la seguridad física, la gestión de la seguridad de la red y la gestión de la seguridad de los proveedores, entre otros

2.3.3. Actualización de la Norma ISO 27002:2022

La versión más reciente de la norma ISO 27002 ha experimentado cambios significativos en comparación con su edición anterior. Uno de los cambios más destacados es la modificación del nombre de la norma, que ha eliminado el término "Código de prácticas". Ahora se denomina "Controles de seguridad de la información para la seguridad de la información, ciberseguridad y

protección de la privacidad", lo cual refleja una perspectiva más amplia que abarca medidas para prevenir, detectar y responder a ciberataques, así como salvaguardar los datos.

Además, la nueva versión de la norma ISO 27002 ha introducido modificaciones en los controles de seguridad en comparación con la edición anterior de 2013. Mientras que la versión previa incluía 114 controles divididos en 14 anexos, la versión actual de 2022 presenta 93 controles clasificados en 4 cláusulas, con un enfoque específico en el contexto de aplicación de cada control.

Los cambios en los controles de seguridad de la norma ISO 27002:2013 son significativos en su versión de 2022, ya que se redujeron de 114 a 93 controles y se dividieron en cuatro cláusulas enfocadas en el contexto de aplicación. (Villamizar Carlos, 2023)

Estas cláusulas son:

- Controles Organizativos con 37 controles,
- Controles de Personas con 8 controles,
- Controles Físicos con 14 controles y
- Controles Tecnológicos con 34 controles.

Entre los 93 controles actuales, 58 han sido actualizados, 24 son una fusión de controles anteriores y 11 son nuevos controles. Además, se eliminó el concepto de "objetivo de control" y se incluyó un atributo que permite la clasificación específica del control en una o más de las 15 categorías establecidas.

2.3.4. Requisitos según la norma ISO/IEC 27002:2022

Según la (ISO/IEC 27002, 2022b), es fundamental que una organización establezca sus necesidades de seguridad de la información, por lo que existen tres fuentes principales de estos requisitos.

- a) Es importante que la organización realice una evaluación de riesgos considerando su estrategia y objetivos generales. Para ello, se puede llevar a cabo una evaluación específica de riesgos de seguridad de la información. El resultado de esta evaluación debe ser la identificación de los controles necesarios para asegurar que el riesgo residual cumpla con los criterios de aceptación de riesgos establecidos por la organización.
- b) Los requisitos legales, estatutarios, reglamentarios y contractuales que se aplican a una organización, así como a sus socios comerciales, proveedores de servicios y entorno sociocultural.
- c) Y el conjunto de principios, objetivos y requisitos empresariales que una organización ha establecido para respaldar sus operaciones en todas las etapas del ciclo de vida de la información

Temas y atributos. La organización tiene la capacidad de crear diferentes perspectivas de los controles mediante el uso de atributos que permiten categorizarlos desde diferentes puntos de vista. Estos atributos pueden utilizarse para filtrar, ordenar o presentar los controles de acuerdo a la audiencia correspondiente.

Como ejemplo, cada control ha sido asociado con cinco atributos que tienen valores correspondientes (precedidos por "#" para facilitar su búsqueda):

Tipo de control. El atributo de "tipo de control" proporciona una forma de visualizar los controles en términos de su impacto en la reducción del riesgo de un incidente de seguridad de la información, así como en el momento en que se implementan. Los valores del atributo incluyen:

- Preventivo: El control que busca prevenir la ocurrencia de un incidente de seguridad de la información

- **Detectivo:** Pertenece al control que se activa después de la ocurrencia de un incidente de seguridad de la información
- **Correctivo** Se puede describir este tipo de control como aquel que se aplica una vez que se ha producido un incidente de seguridad de la información.

Conceptos de ciberseguridad. Los controles pueden ser vistos desde la perspectiva de su asociación con los conceptos de ciberseguridad definidos en el marco de ciberseguridad descrito en (*ISO/IEC TS 27110*, 2021) utilizando el atributo de "Conceptos de ciberseguridad". Los valores del atributo incluyen Identificar, Proteger, Detectar, Responder y Recuperar.

Capacidades operativas. Los atributos de capacidades operativas permiten al profesional de seguridad de la información ver los controles desde la perspectiva de las habilidades necesarias para su implementación efectiva. Entre estos atributos, se encuentra *Protección_de_información*, el cual será útil para analizar la sección de análisis de estado actual de la institución financiera.

Dominios de seguridad. Los atributos de dominios de seguridad permiten visualizar los controles desde la perspectiva de dominios de seguridad de la información: "Protección" que engloba áreas como "Arquitectura de seguridad de TI", "Administración de seguridad de TI", "Gestión de la identidad y el acceso", "Mantenimiento de la seguridad informática" y "Seguridad física y medioambiental". "Defensa" incorpora "Detección" y "Gestión de incidentes de seguridad informática."

Las organizaciones tienen la opción de no considerar algunos de los atributos mencionados o incluso crear sus propios atributos personalizados con valores correspondientes para establecer sus propias perspectivas organizacionales.

2.3.5. Estructura de la Norma 27002:2022

La tercera edición de la norma 27002:2022 reemplaza y anula la segunda edición (ISO/IEC 27002:2013), que ha sido revisada técnicamente y también incluye las correcciones técnicas ISO/IEC 27002:2013/Cor. 1:2014 e ISO/IEC 27002:2013/Cor. 2:2015. Las actualizaciones más destacadas se reflejan en la modificación del título y la estructura del documento, que ahora presenta los controles de manera más clara y organizada a través de una taxonomía simple y atributos asociados. Además, se han fusionado algunos controles, eliminado otros y añadido nuevos controles.

La información presentada en este segmento está respaldada por la norma (*ISO/IEC 27002, 2022b*), que establece los controles importantes para el desarrollo del proyecto. En particular, el control 5.12 (Clasificación de la información), se aborda en la versión ISO/IEC 27002:2013, pero ha experimentado diferencias clave en los procesos actuales de la organización. Por otro lado, el control 8.12 (Prevención de fugas de información) corresponde a las actualizaciones recientes y proporciona una guía para el control de la información. La norma (*ISO/IEC 27002, 2022b*) describe detalladamente cada uno de estos controles.

2.3.5.1. Control 5.12: Clasificación de la información

El control 5.12 se enfoca en la prevención y ayuda a las organizaciones a identificar riesgos al permitirles determinar el nivel de protección necesario para cada activo de información. Este nivel se basa en requisitos de confidencialidad, integridad y disponibilidad, y se asigna a activos relevantes mediante categorías. La Tabla 6 presenta un esquema característico de la tabla de atributos de clasificación de la información.

Tabla 6.

Tabla de Atributos de Clasificación de la información

Tipo de control	Propiedades de seguridad de la información	Conceptos Ciberseguridad	Capacidades Operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identidad	#Proteccion_Información	#Protección #Defensa

Nota. Elaborado a partir de (ISO/IEC 27002, 2022b).

– Controlar

Es necesario categorizar la información según las necesidades de seguridad de la organización, teniendo en cuenta aspectos como la confidencialidad, integridad, disponibilidad y los requerimientos de las partes involucradas.

– Finalidad

Es importante asegurarse de identificar y comprender las necesidades de protección de la información según su importancia para la institución.

– Guía

Es necesario que la organización defina una política transparente y detallada sobre cómo se debe clasificar la información en función de su importancia y que se comunique a todas las partes interesadas relevantes.

Así mismo, los requisitos empresariales de compartir o restringir la información, la protección de la integridad de la información y la garantía de la disponibilidad, junto con los requisitos legales sobre confidencialidad, integridad y disponibilidad, deben tenerse en cuenta al establecer las clasificaciones y controles de protección de la información. Además, se puede clasificar otros activos distintos de la información en función de este proceso, que se almacena en ellos, se procesa, se maneja o protege de otra manera con estos.

Se puede determinar la clasificación de la información según el impacto que tendría en las instituciones en caso de ser comprometida. Se debe asignar un nombre a cada nivel de clasificación que tenga sentido dentro del contexto de la aplicación del esquema. Para garantizar la coherencia en toda la organización, el esquema debe incluirse en los procedimientos y asegurarse de que todos los miembros clasifiquen la información y los activos asociados de manera consistente.

- Otra información

La clasificación de la información proporciona una guía clara sobre cómo manejar y proteger la información. Esta clasificación se realiza mediante la creación de grupos de información con necesidades de protección similares y la definición de procedimientos de seguridad que se aplican a todo el grupo, lo que reduce la necesidad de evaluar riesgos individualmente y diseñar controles personalizados. Es importante tener en cuenta que la sensibilidad y criticidad de la información pueden cambiar con el tiempo y la clasificación debe actualizarse en consecuencia. Una clasificación excesiva puede generar costosos controles innecesarios, mientras que una clasificación insuficiente puede resultar en controles inadecuados para proteger la información. Además, una vez que la información se ha hecho pública, ya no requiere confidencialidad, pero puede seguir necesitando protección para garantizar su integridad y disponibilidad.

2.3.5.2.Control 8.12: Prevención de fuga de datos

El control 8.12 tiene un doble propósito, ya que es tanto preventivo como detectivo. Este control permite controlar las modificaciones de los riesgos que presentan los activos de información mediante la implementación de medidas técnicas que detecten y eviten la divulgación o extracción de información, ya sea por personal interno o externo. El esquema de la tabla de atributos de prevención de fuga de información se puede visualizar en la Tabla 7.

Tabla 7.

Prevenición de fuga de información

Tipo de control	Propiedades de seguridad de la información	Conceptos Ciberseguridad	Capacidades Operativas	Dominios de seguridad
#Preventivo	#Confidencialidad	#Protector	#Protección_información	#Protección
#Detectivo		#Detector		#Defensa

Nota. Elaborado a partir de (ISO/IEC 27002, 2022b).

– Controlar

Es importante implementar medidas de seguridad para evitar la fuga de información en los dispositivos, redes y sistemas que se encargan de procesar, almacenar o transmitir información confidencial.

– Finalidad

Identificar y evitar que personas o sistemas no autorizados divulguen o extraigan información de forma indebida.

– Guía

Se deben considerar los siguientes aspectos para disminuir el riesgo de filtración de datos por parte de las entidades:

- a) Se debe identificar y clasificar la información para prevenir la divulgación no autorizada de datos, como información personal, modelos de precios y diseños de productos.
- b) Una medida importante para reducir el riesgo de fuga de datos es monitorear los canales por los cuales la información puede filtrarse, tales como el correo electrónico, transferencias de archivos, dispositivos móviles y de almacenamiento portátiles.
- c) Se debe tomar acción para evitar la divulgación de información, como, por ejemplo, poner en cuarentena los correos electrónicos que contengan información confidencial.

Se debe hacer uso de las herramientas de prevención de fuga de datos para:

- a) Emplear herramientas de prevención de fuga de datos para detectar y controlar información confidencial que se encuentre en peligro de ser divulgada sin autorización, incluso si esta información se encuentra en datos no estructurados dentro del sistema de un usuario.
- b) Utilizar herramientas de prevención de fuga de datos para identificar la divulgación no autorizada de información sensible, por ejemplo, al cargarla en servicios de nube de terceros no confiables o al enviarla por correo electrónico.
- c) Impedir las acciones del usuario o transmisiones de red que puedan poner en riesgo la información sensible, como, por ejemplo, bloqueando la copia de entradas de bases de datos en una hoja de cálculo u otras acciones que puedan exponer la información.

La organización debe aplicar tecnología, como herramientas de prevención de fuga de datos o la configuración de herramientas existentes, para permitir que los usuarios accedan y manejen datos almacenados de forma remota, pero impedir que se copien y peguen fuera del control de las entidades.

Para el caso de exportar datos, es importante que el titular de los datos autorice dicha exportación y que se responsabilice a los usuarios de sus acciones.

Si la institución necesitase copias de seguridad, se deben tomar medidas para proteger la información sensible, como el cifrado, el control de acceso y la protección física de los medios de almacenamiento que contengan la copia de seguridad.

Además, es necesario considerar la prevención de fugas de datos para protegerse contra las acciones de inteligencia de adversarios que intenten obtener información confidencial o secreta, ya sea de interés para el espionaje o crítica para la comunidad.

Para evitar la fuga de datos, es necesario tomar medidas que puedan confundir a posibles adversarios. Una opción podría ser reemplazar información verdadera por información falsa, ya sea como una medida independiente o como respuesta a las acciones de inteligencia del adversario.

- Otra información

Las herramientas de prevención de fuga de datos tienen como objetivo identificar y supervisar los datos, y tomar medidas para prevenir la fuga de información, por ejemplo, notificar a los usuarios sobre su comportamiento de riesgo y bloquear la transferencia de datos a dispositivos de almacenamiento portátiles.

Sin embargo, la prevención de la fuga de datos implica la necesidad de monitorear las comunicaciones y actividades en línea del personal y, por consiguiente, también los mensajes de terceros, lo cual puede plantear problemas legales que deben ser considerados antes de implementar estas herramientas.

2.4.Data Loss Prevention

(Brian Svidergol & Robert Clements, 2019), define que la tecnología de Prevención de Pérdida de Datos (DLP) es una combinación de hardware y software que busca prevenir, minimizar o proteger contra la pérdida o acceso no autorizado de datos. En ciertos casos, su implementación se relaciona con el cumplimiento de regulaciones gubernamentales o de conformidad en empresas. En otras situaciones, se utiliza para mejorar la seguridad de una organización, especialmente para evitar la pérdida de propiedad intelectual.

Por otro lado (Stallings William, 2018), explica que la pérdida de datos se refiere a la divulgación no intencionada o intencionada de información a un ambiente no confiable. La prevención de Pérdida de Datos (DLP), también conocida como fuga de información, es un enfoque completo que involucra a las personas, procesos y sistemas para identificar, supervisar y

proteger los datos en uso, en movimiento y en reposo. Esto se logra mediante una inspección exhaustiva del contenido y un marco de gestión centralizado.

Basándose en las definiciones mencionadas, se ha investigado que la infraestructura de prevención de pérdida de datos (DLP) ofrece una solución sólida para detectar, supervisar, proteger y gestionar la información sensible, teniendo en cuenta su categorización, el medio de almacenamiento y los propietarios identificados. Estas funciones se logran a través de:

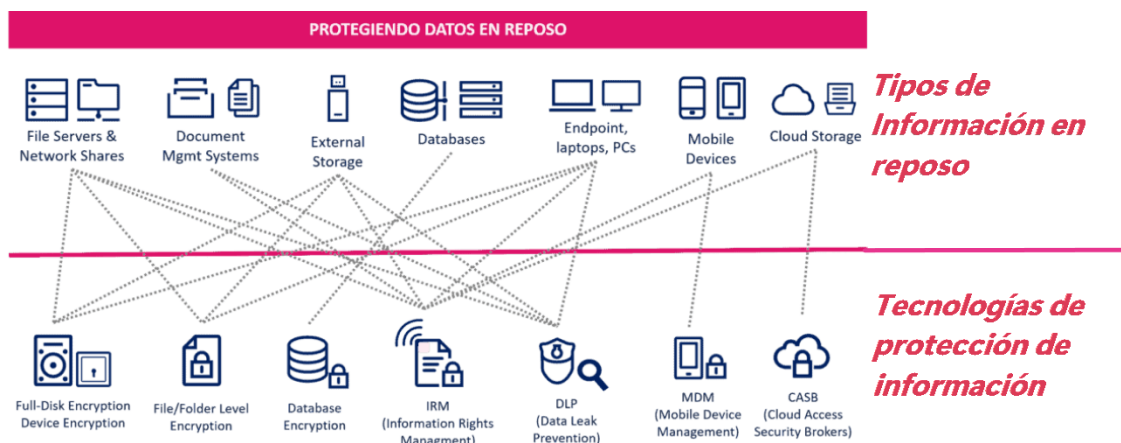
- Detección de información sensible en su medio de almacenamiento, creando un inventario de datos e identificando a sus propietarios, con el objetivo de simplificar el manejo de la información relacionada.
- Supervisar cómo se utiliza la información confidencial por parte de los usuarios y los procesos organizativos involucrados, asegurando su visibilidad.
- Proteger la información mediante la aplicación automatizada de políticas de seguridad, anticipándose a posibles fugas de información.
- Administrar políticas globales de prevención de pérdida de datos en toda la organización, identificar incidentes de seguridad y generar informes de manera centralizada a través de una plataforma unificada y centralizada. (Martínez Miguel Ángel DLP & Martínez Miguel Ángel, n.d.)

2.4.1. Funcionamiento de DLP

Se identifican tres estados para la información o los datos, y uno de ellos es el estado de información en Reposo, que se refiere a la información almacenada en un medio físico o lógico que no está siendo accedida, utilizada o procesada. Algunos ejemplos de esto incluyen archivos almacenados en servidores de archivos, registros en bases de datos y documentos en unidades flash o discos duros. De acuerdo a la ilustración de Figura 3.

Figura 3.

Datos en Reposo

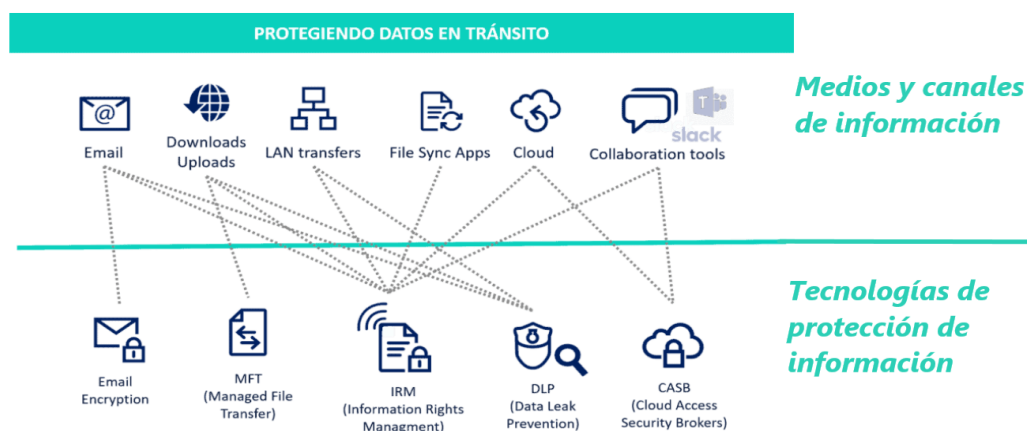


Nota. La autoría pertenece a (Sealpath, 2020)

La Información en Tránsito o Movimiento se refiere a la información que se está transmitiendo a través de diferentes canales de comunicación, ya sea correo electrónico, aplicaciones de trabajo en equipo como Slack o Microsoft Teams, mensajería instantánea, entre otros. Se trata de información que se encuentra en movimiento de un lugar a otro. Como se representa en la Figura 4.

Figura 4.

Datos en Movimiento

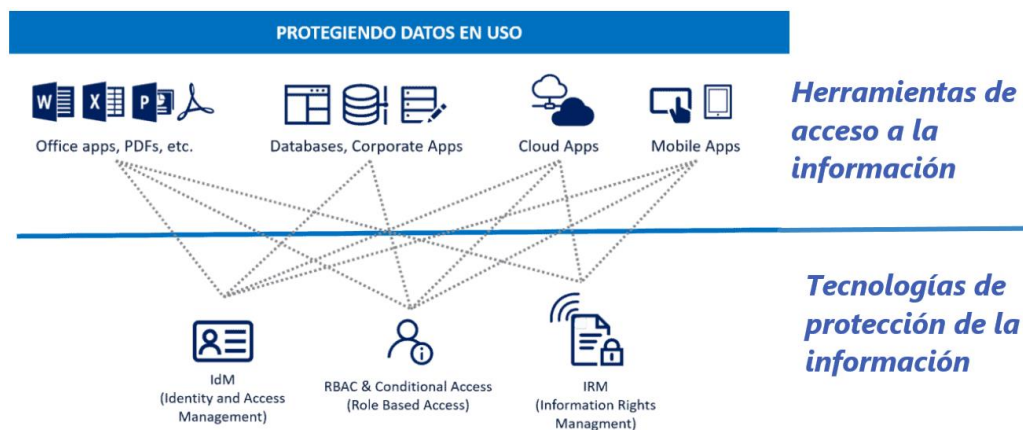


Nota. La autoría pertenece a (Sealpath, 2020)

La información en uso se refiere a los datos que son procesados por una o varias aplicaciones. En la mayoría de los casos, un usuario es el que accede a los datos a través de la aplicación para visualizarlos, modificarlos u otras acciones similares. Tal y como se aprecia en la Figura 5.

Figura 5.

Datos en Uso



Nota. Autoría original del ejemplo proporcionado en (Sealpath, 2020)

2.4.2. Productos Data Loss Prevention

Existen diversas soluciones de Prevención de Pérdida de Datos (DLP), cada una enfocada en una tarea específica, pero con el mismo propósito de evitar la pérdida de datos.

- Network DLP se centra en los datos en movimiento que circulan por la red corporativa y está integrada en el software o hardware de la plataforma, lo que permite monitorear, rastrear y generar informes sobre todo el tráfico de datos en la red. Los datos recopilados se almacenan en una base de datos de fácil administración.
- Storage DLP se enfoca en los datos en reposo y escanea y protege los archivos confidenciales almacenados y compartidos por los usuarios que tienen acceso a la red corporativa. Esta solución es particularmente útil para el control de datos en la nube.

- Endpoint DLP se refiere a dispositivos como laptops y ordenadores, y se instala en todas las estaciones de trabajo y dispositivos utilizados por los empleados de la empresa para supervisar y evitar la filtración de datos confidenciales.
- Management DLP se refiere a la plataforma central de gestión que consta de un servidor de gestión y una base de datos. Todos los usuarios se conectan a la consola de gestión, que gestiona todas las políticas de Prevención de Pérdida de Datos, el flujo de trabajo, los informes, los usuarios, las funciones, la gestión del sistema y la seguridad. La plataforma de gestión administra todos los servidores de detección enviando políticas, detección y configuración a los servidores de detección.(Bottini Claudio, 2022)

2.4.3. Método DLP

La tecnología de prevención de pérdida de datos (DLP), utiliza la Inspección Profunda de Contenidos (DCI), que es una evolución de la Inspección Profunda de Paquetes, con la capacidad de analizar el contenido real en lugar de enfocarse en paquetes individuales o múltiples.

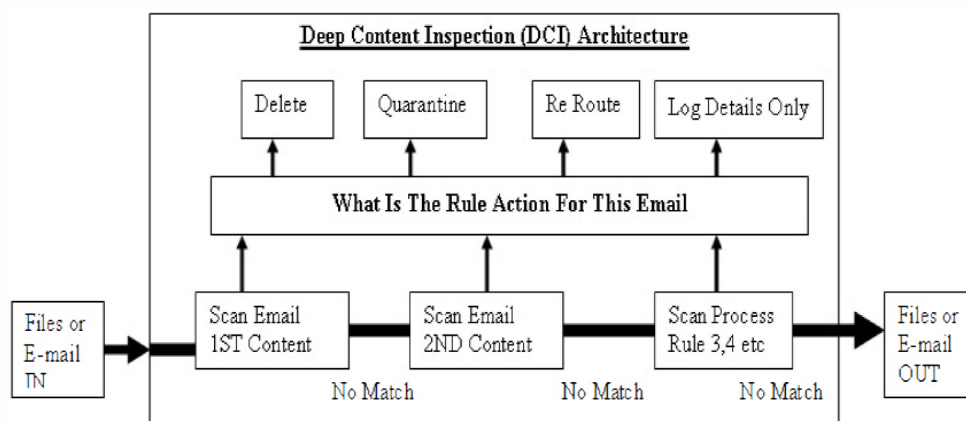
La Inspección Profunda de Contenidos permite a los servicios rastrear el contenido a través de varios paquetes, lo que permite que las firmas de búsqueda atraviesen los límites de los paquetes y sean identificadas. DCI clasifica el contenido que pasa a través de reglas, que incluyen información de la capa 7.

La figura 6 ilustra la arquitectura de la Inspección Profunda de Contenidos, que consiste en la adquisición de datos representados por archivos o correos electrónicos. Posteriormente se realiza un análisis exhaustivo del contenido usando la técnica de comparación de contenidos que funciona con datos estructurados y no estructurados, utilizando diferentes criterios como palabras clave regulares, tipos de archivo, tamaño de archivo, propiedades de archivo, remitente, destinatario y el protocolo de red para detectar pérdida de datos. A continuación, los datos son

clasificados en diferentes categorías según su sensibilidad, utilizando algoritmos de coincidencia de contenido con el uso de Match-Join que comparan duplas de datos, si coinciden para cada atributo categórico común y están en la misma ruta de generalización en el árbol taxonómico de cada categoría, estas se clasificarán según su riesgo asociado. Una vez clasificados se establecen políticas de seguridad que van a determinar el nivel de confidencialidad y acciones específicas para proteger la información, tales como bloquear, enviar alertas a los administradores o bloquear el acceso. (Tahboub & Saleh, 2014)

Figura 6.

Inspección profunda de contenido (DCI)



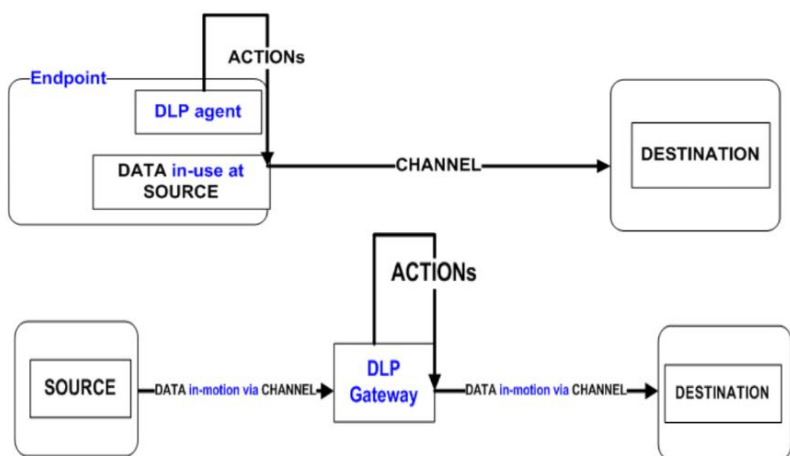
Nota. Autoría atribuidos a (Tahboub & Saleh, 2014)

2.4.4. Arquitectura DLP

La prevención de fuga de datos se determina mediante la perspectiva técnica enfocada en los datos en uso y movimiento. Si los Datos fluyen de la FUENTE (Source) al DESTINO (Destination) a través del CANAL (Channel), el sistema toma ACCIONES (Actions). Según se representa en la Figura 7.

Figura 7.

Representación técnica de Datos en uso y movimiento



Nota. Autoría atribuidos a (Liwei Ren, 2013)

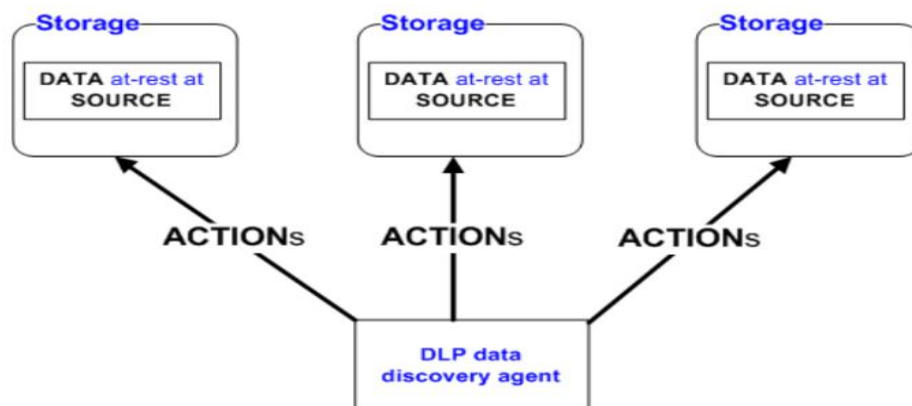
Donde se especifican qué los datos confidenciales están definidos por el sistema como información que necesita protección. La fuente de los datos puede ser un usuario, un punto final, una dirección de correo electrónico o un grupo de ellos. El destino de los datos puede ser un punto final, una dirección de correo electrónico o un grupo de ellos, o simplemente el mundo exterior. El canal por el cual los datos pueden ser filtrados se llama "canal de fuga" y puede ser a través de USB, correo electrónico, protocolos de red, etc. Finalmente, la acción que el sistema de DLP debe llevar a cabo cuando se produce un incidente también es especificada.

Por otro lado, la perspectiva enfocada en los datos en reposo se refiere a, Si los DATOS residen en la FUENTE (Storage), el sistema toma ACCIONES (Actions).

Se especifica qué datos son considerados confidenciales y tienen potencial de fuga. La fuente de estos datos puede ser un endpoint, un servidor de almacenamiento o un grupo de ellos. Además, se establece la acción que debe tomar el sistema DLP cuando se detectan datos confidenciales en reposo. (Liwei Ren, 2013)

Figura 8.

Representación técnica de Datos en reposo

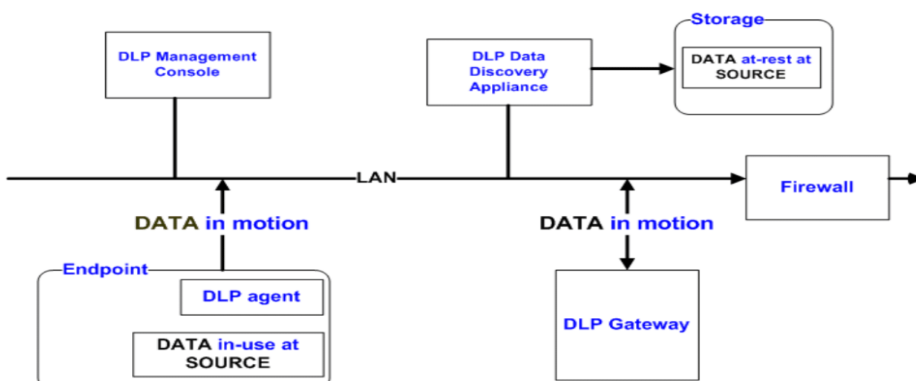


Nota. Autoría atribuidos a (Liwei Ren, 2013)

Cada proveedor presenta un producto que se adapta a los diferentes estados de información manejados por un sistema, tomando acciones basadas en las políticas establecidas para los datos confidenciales. En resumen, los productos están diseñados para cumplir con los requisitos específicos de protección de datos de cada organización.

Figura 9.

Arquitectura Típica DLP



Nota. Autoría atribuidos a (Liwei Ren, 2013)

2.4.5. Plataforma de Software DLP

En el mercado hay diversas opciones de plataformas de software para la Prevención de fugas de información (DLP), por lo que resulta crucial analizar las características y requisitos

particulares de cada una para determinar cuál se ajusta mejor a las necesidades específicas según la normativa de referencia.

2.4.5.1. ManageEngine DataSecurity Plus

La aplicación (ManageEngine DataSecurity Plus, 2023), cuenta con herramientas que integran el análisis de archivos y la evaluación de riesgos de datos, lo que le permite detectar información delicada, evaluar todos los datos asociados y determinar si existe algún peligro debido a factores como la ubicación de almacenamiento, la propiedad o los permisos de seguridad asignados. Después, se puede aplicar un proceso de clasificación de datos para etiquetarlos con información contextual, como su tipo, grado de sensibilidad, nivel de confidencialidad y valor para la organización.

Las características de esta aplicación incluyen asegurar el uso exclusivo de dispositivos de almacenamiento extraíbles seguros en su organización mediante el uso de listas de bloqueo para evitar el uso de dispositivos no examinados. También impide la exposición de datos al prohibir actividades de copia de archivos de alto riesgo en dispositivos USB y recursos compartidos locales y de red. Además, brinda un control detallado sobre el uso de varios dispositivos de punto final, como Wi-Fi, Bluetooth y unidades de CD/DVD. También evita que archivos que contienen datos altamente confidenciales, como información de identificación personal (PII) o información de salud electrónica (ePHI), se compartan como archivos adjuntos en correos electrónicos en Outlook.

La aplicación también detecta comportamientos anormales de los usuarios y evita la transferencia de archivos a través de dispositivos de almacenamiento externos. Además, permite la eliminación o aislamiento de archivos, detiene la transferencia de datos USB y ofrece otros remedios activos predefinidos para prevenir la fuga de datos.

2.4.5.2.Safetica

(Safetica NXT, 2023) es una solución de protección de datos de última generación en la modalidad de software como servicio (SaaS). Su función principal es detectar y mitigar de manera temprana posibles amenazas y riesgos a la seguridad de los datos en una organización. Además, ayuda a proteger los datos confidenciales, establecer políticas para su manejo, educar a los empleados y cumplir con las normativas. Utiliza tecnologías avanzadas para evaluar el riesgo de cada archivo y usuario, y puede detectar y bloquear incidentes de seguridad en la transferencia de datos salientes.

Safetica realiza auditorías silenciosas de las actividades de los puntos finales y almacena de forma segura la información en la plataforma de Microsoft Azure. La solución permite tomar medidas correctivas y cambiar el comportamiento de los empleados o procesos de la empresa para prevenir la filtración de datos. Así también proporciona la visibilidad y protección necesarias para los flujos de datos entre puntos finales, nubes y usuarios.

3. CAPITULO III

SITUACIÓN ACTUAL

En este capítulo se ofrece una descripción exhaustiva de las actividades internas que actualmente se llevan a cabo en la entidad financiera Cooperativa Santa Anita Ltda. Se detallan la estructura organizativa, las aplicaciones utilizadas y la infraestructura empleada por la institución. A continuación, se realiza un análisis diagnóstico de la información en relación con los requisitos establecidos en la norma ISO 27002:2022. El objetivo es determinar qué aspectos se cumplen, qué secciones de la normativa son aplicables y qué documentos deben ser desarrollados como mínimo para demostrar el cumplimiento de la norma. Por último, con base en este conocimiento, se propone una metodología que permita establecer las políticas de seguridad en la herramienta de Prevención de Pérdida de Datos (DLP).

3.1.Situación Actual

La (Cooperativa de Ahorro y Crédito Santa Anita Ltda., 2011), establecida en 2001 por iniciativa de La UNORCAC, Unión de Organizaciones Campesinas e Indígenas de Cotacachi, tiene como objetivo respaldar el desarrollo económico y social de los sectores indígenas campesinos de Cotacachi, en la provincia de Imbabura.

Hasta ahora, la cooperativa ha abierto siete oficinas, incluyendo la sede central en Cotacachi, y sucursales en Atuntaqui, Imantag e Ibarra en la provincia de Imbabura, así como una agencia en Mira, Las Parcelas y San Rafael en la provincia de Carchi. Su principal enfoque de mercado se centra en la población rural de estos cantones.

La Cooperativa obtiene la mayoría de sus fondos a través de los ahorros de sus socios, pero también tiene acceso a líneas de crédito de prestamistas externos. En cuanto a los servicios, la Cooperativa ofrece tanto tecnologías individuales como grupales solidarias

3.1.1. Misión

La entidad financiera define su misión de “Somos una Cooperativa de Ahorro y Crédito confiable y solvente del sector financiero Popular y solidario que ofrece productos y servicios dirigidos a nuestros socios y clientes en la región sierra Norte del País, impulsando el crecimiento económico, cuidado al medio ambiente, desarrollo social e inclusión financiera de la comunidad”

3.1.2. Visión

La visión de la entidad financiera se establece como “Ser una Cooperativa de Ahorro y Crédito sostenible, reconocida por preservar la inclusión social, promover la calidad humana en nuestra gente, brindar productos y servicios para satisfacer las necesidades financieras de socios y clientes.”

3.1.3. Servicios prestados por la COAC Santa Anita Ltda.

La institución financiera brinda una amplia gama de servicios financieros que incluyen asesoramiento estratégico para negocios, comercialización de productos y servicios, operaciones de crédito, inversiones y liquidez, cuentas corrientes de ahorro, certificados de depósito y servicios de información y gestión. La Figura 10, proporciona más detalles que se pueden encontrar en su página web. Además, la entidad también ofrece servicios no financieros, como seguros y asistencia técnica. En cuanto a las garantías, la cooperativa acepta actualmente distintos tipos, como garantías quirografarias, prendarias, hipotecarias y sobre inversiones, y se sugiere mantener esta opción disponible.

Figura 10.

Servicios prestados por la COAC Santa Anita Ltda.



Nota. Autoría atribuidos a (Cooperativa de Ahorro y Crédito Santa Anita Ltda., 2011)

La elección del tipo de garantía requerida depende del nivel de riesgo asociado a la operación, y se deben tener en cuenta diversas variables, como el plazo del crédito, el propósito del préstamo, el porcentaje de deuda en relación con el patrimonio personal, la calificación crediticia y el monto del crédito. Además, la cooperativa ofrece una aplicación móvil que permite a los socios realizar transacciones y acceder a información sobre sus operaciones bancarias a través de la banca virtual en la app o mediante el servicio de banca móvil. Todo esto tiene como objetivo mantener una atención excelente y brindar un servicio mejorado a los socios de la cooperativa.

3.1.4. Política de Privacidad

En esta sección se explican las políticas de uso y protección de datos personales implementadas por la Cooperativa Santa Anita Ltda. Al brindar información personal al personal de atención, acceder a la página web o utilizar la aplicación móvil, se aceptan automáticamente las normas de uso, protección y seguridad establecidas en esta sección.

La Cooperativa Santa Anita Ltda. valora la privacidad de sus clientes y socios, y se compromete a tratar cualquier información proporcionada con cuidado y la máxima seguridad posible. Los datos personales solo se utilizarán de acuerdo con las restricciones de privacidad establecidas. La cooperativa solo recopilará información personal cuando el cliente o socio la proporcione de manera voluntaria y consciente al convertirse en miembro o cliente de la entidad financiera.

La institución financiera utilizará la información recopilada de la siguiente manera:

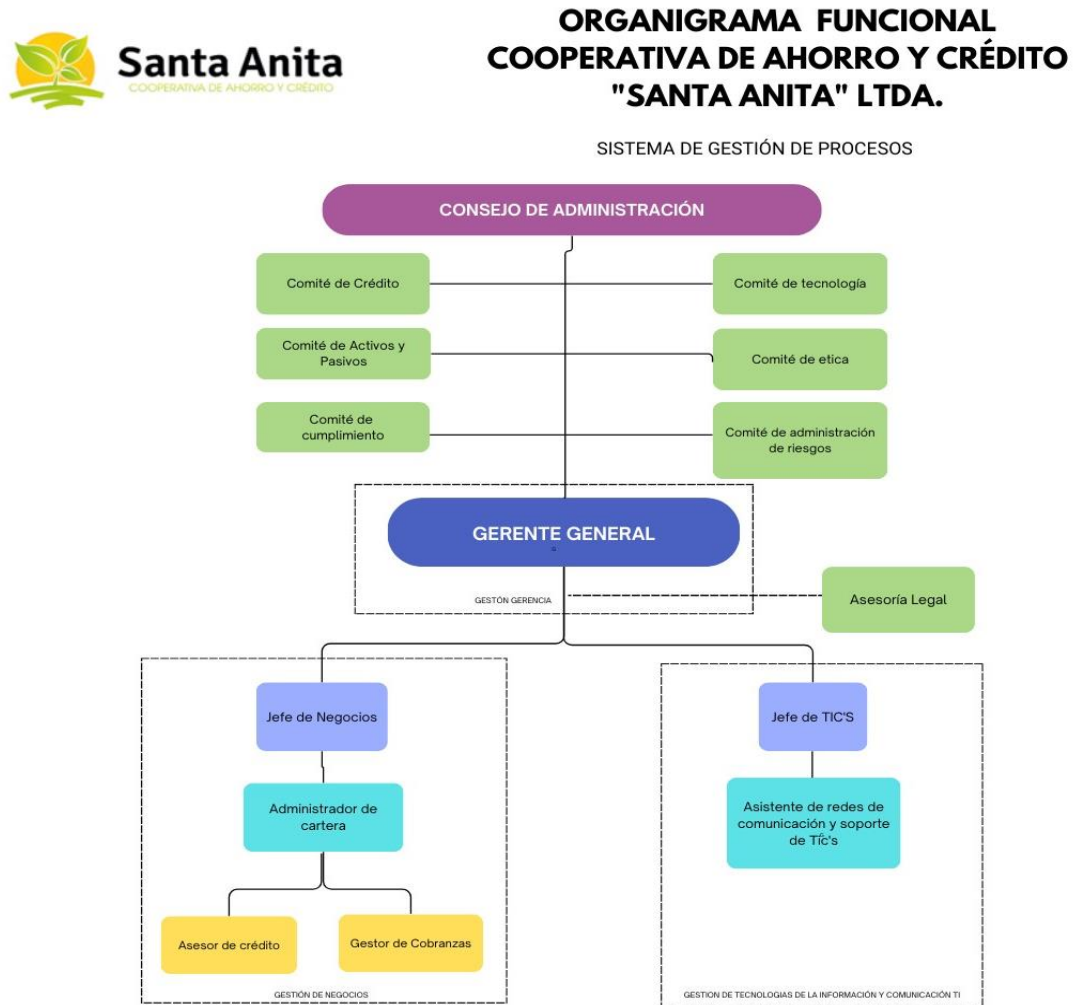
- a) Para el propósito específico para el cual se proporcionó.
- b) Para ampliar la oferta en el mercado y realizar publicidad de productos y servicios que puedan ser de interés, incluyendo la confirmación de la información.
- c) Para personalizar y mejorar nuestros productos y servicios.

Al proporcionar datos personales, las personas automáticamente autorizan a la Cooperativa Santa Anita Ltda. a utilizar dichos datos de acuerdo con esta política de seguridad y privacidad.

3.1.5. Organigrama Estructural

En esta sección se establece la estructura organizacional de la entidad financiera Cooperativa de Ahorro y Crédito "Santa Anita" Ltda. Se identifica la jerarquía y las relaciones de autoridad dentro de la organización, se definen los departamentos y las unidades de trabajo, y se describe el proceso de toma de decisiones. Además, en la figura 11 se presenta el organigrama funcional que representa el sistema de gestión por procesos, y se detallan las funciones asignadas a cada departamento.

Figura 11.
Organigrama Estructural



Nota. Autoría atribuidos a (Cooperativa de Ahorro y Crédito Santa Anita Ltda., 2011)

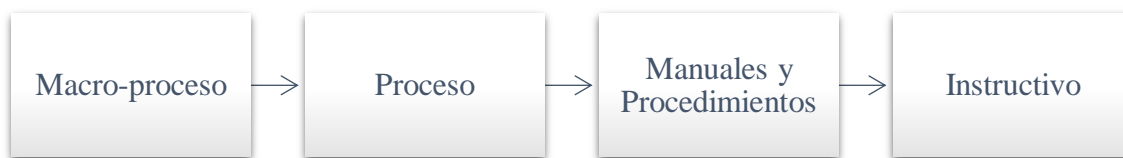
3.2.Sistema de Gestión por Procesos

Un (*Sistema de Gestión Por Procesos (BPM)*, 2020), es una metodología de trabajo empleada por empresas de diversos tamaños, incluyendo tanto grandes corporaciones como pequeñas y medianas empresas (Pymes). Esta metodología implica una serie de acciones que determinan la forma de trabajar, con el objetivo de optimizar los procesos y permitir mejoras y rediseños en el flujo de trabajo para adaptarse a las necesidades de los clientes.

En este sentido, la entidad financiera se adhiere al enfoque de Sistema de Gestión por Procesos, y se establecerá el estado actual de la entidad definiendo los diferentes procesos tal según se muestra en la Figura 12, de la siguiente manera:

Figura 12.

Sistema de Gestión de Procesos



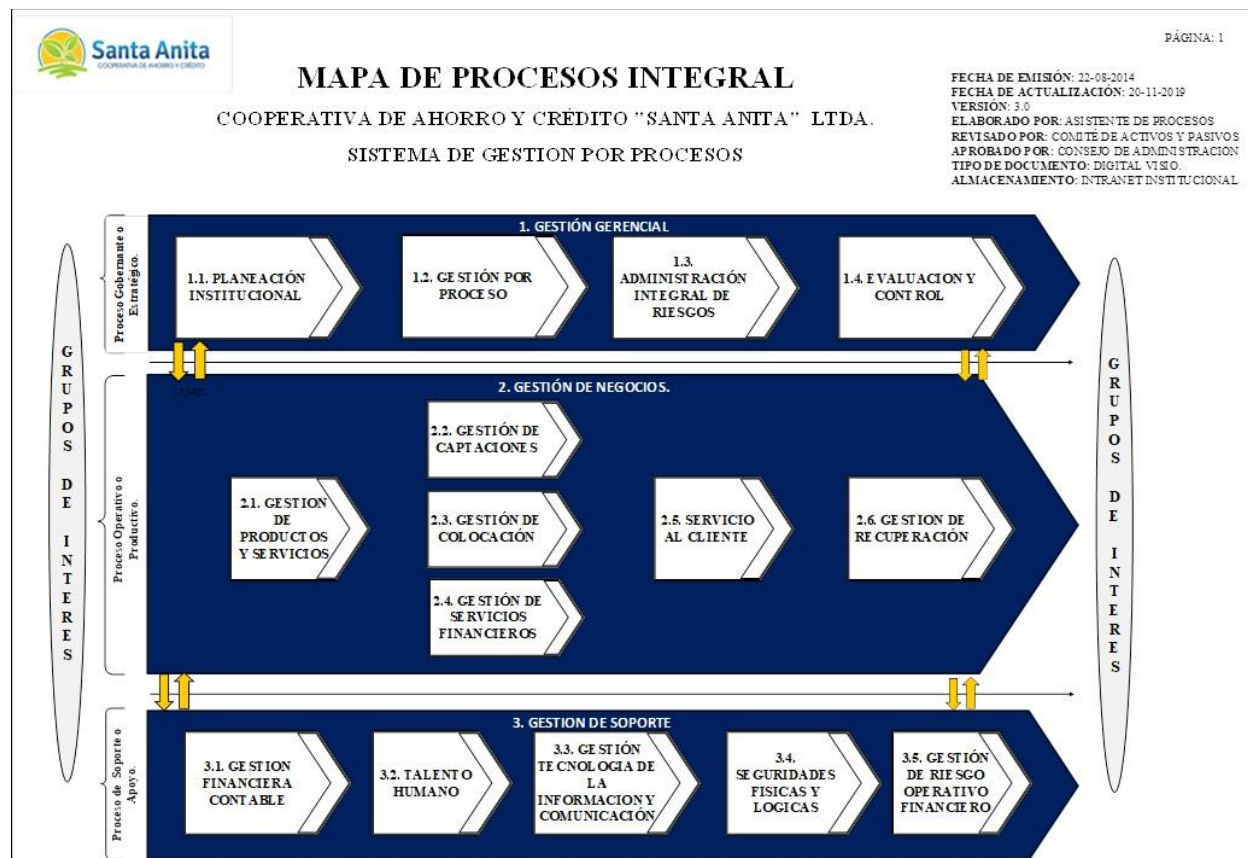
Nota. Elaborado a partir de (Cooperativa de Ahorro y Crédito Santa Anita Ltda., 2011)

3.2.1. Mapa de Procesos

La actividad a la que se dedica la entidad financiera está determinada por procesos que abarcan una serie de actividades necesarias para su correcto funcionamiento, tanto a nivel interno como externo. En este contexto, la entidad financiera identifica y define los grupos de interés y gestiona los procesos de manera estructurada. La mejora continua de cada uno de estos procesos constituye la base fundamental para el mejoramiento integral de la organización. El mapa de procesos integral se puede observar en la Figura 13.

Figura 13.

Mapa de Procesos Integral



Nota. Elaborado a partir de (Cooperativa de Ahorro y Crédito Santa Anita Ltda., 2011)

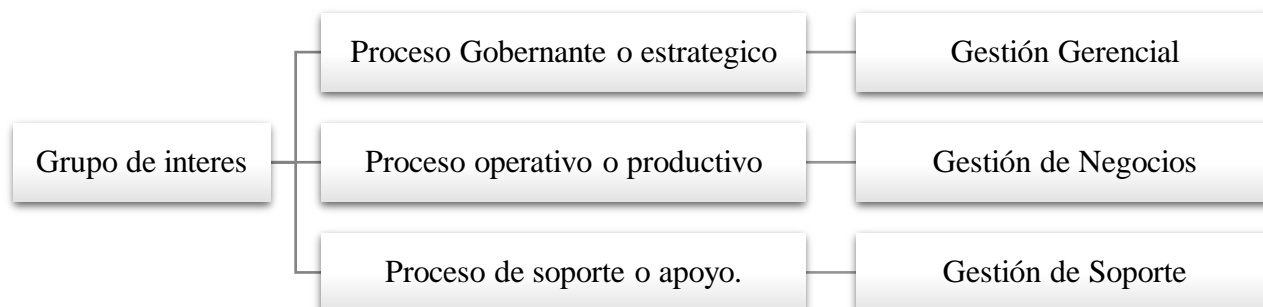
3.2.2. Macroprocesos

La entidad financiera se organiza en torno a tres macroprocesos fundamentales: Gestión Gerencial, Gestión de Negocios y Gestión de Soporte, según se ilustra en la Figura 14. Para este proyecto de grado en particular, se ha elegido el macroproceso centrado en el proceso operativo o productivo de Gestión de Negocios.

La Gestión de Negocios implica la administración y engloba todas las actividades llevadas a cabo por la entidad financiera para supervisar diferentes aspectos del negocio, con el propósito de lograr los objetivos estratégicos y asegurar el éxito y la continuidad de la organización financiera.

Figura 14.

Macroprocesos



Nota. Elaborado a partir de (Cooperativa de Ahorro y Crédito Santa Anita Ltda., 2011)

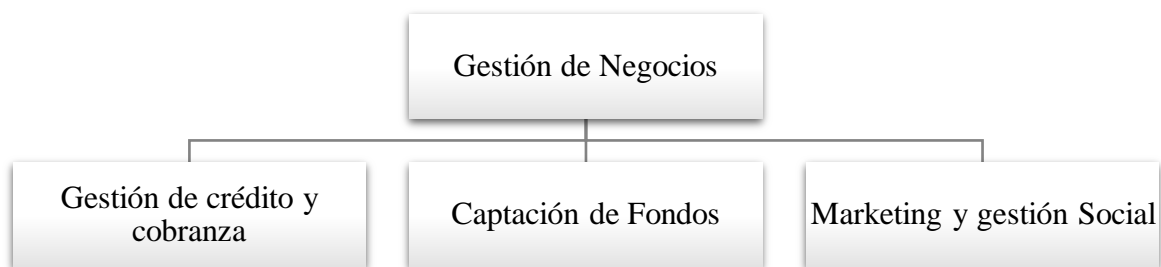
3.2.3. *Proceso*

En el marco del Macroproceso de Gestión de Negocios, la entidad ha implementado diversos procesos que se centran en diferentes áreas de gestión, como se puede apreciar en la Figura 15. En el desarrollo de este proyecto de titulación, se ha identificado como crucial para determinar la metodología al proceso de gestión de crédito y cobranza.

Para lograr esto, se establecen una serie de actividades que abarcan la evaluación, concesión y administración de los créditos, así como la recuperación de los pagos pendientes de los créditos otorgados.

Figura 15.

Procesos de Gestión de Negocios



Nota. Elaborado a partir de (Cooperativa de Ahorro y Crédito Santa Anita Ltda., 2011)

3.2.4. *Manual y Procedimiento*

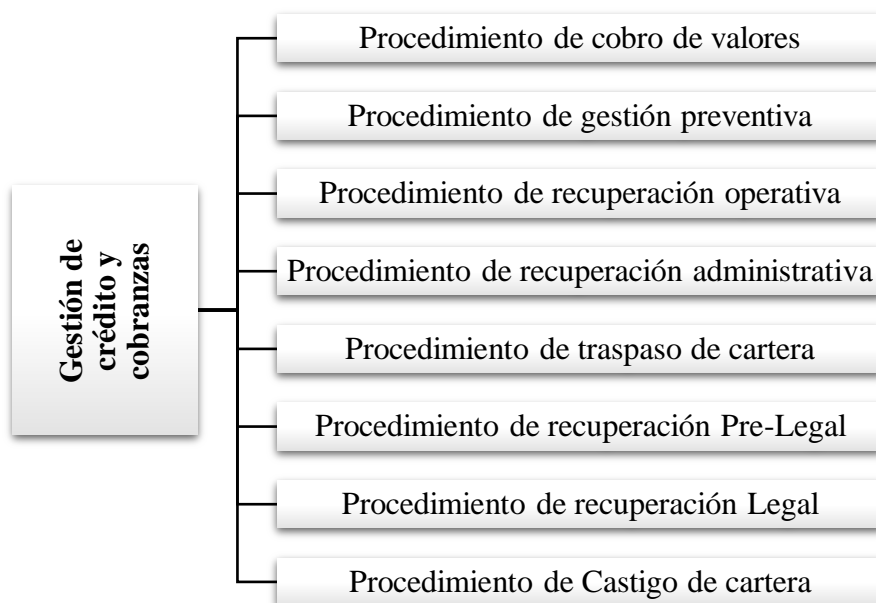
En el contexto del proceso de Gestión de crédito y cobranza, la entidad financiera establece procedimientos y manuales que establecen cómo se realizarán las distintas actividades asociadas

a la administración de los créditos y la recuperación de la cartera. Estos procedimientos se encuentran detallados en la Figura 16.

El procedimiento seleccionado para este trabajo de grado es el de recuperación operativa, el cual se centra en recuperar la cartera vencida durante el período de uno a treinta días de morosidad, con el propósito de reducir el riesgo de cartera. La elección de este procedimiento se fundamenta en que incluye pautas y reportes de información que posibilitarán el análisis de los riesgos asociados a su aplicación

Figura 16.

Procedimientos de Gestión de crédito y cobranzas



Nota. Elaborado a partir de (Cooperativa de Ahorro y Crédito Santa Anita Ltda., 2011)

3.2.5. Procedimiento de recuperación operativa

Este procedimiento se establece con el objetivo de recuperar la cartera que ha incurrido en morosidad desde el primer día hasta un máximo de 30 días. Para lograrlo, se llevan a cabo una serie de actividades que involucran el manejo de diversos tipos de información relacionada con los clientes.

3.2.5.1.Objetivo

La COAC “Santa Anita” Ltda., establece un proceso teniendo a lograr la recuperación de la cartera vencida del primero al trigésimo día de morosidad con el fin de minimizar el riesgo de cartera.

3.2.5.2.Alcance

COAC “Santa Anita” Ltda., determina que el presente procedimiento comprende desde los créditos que registran a partir de un día de mora hasta créditos con mora hasta 30 días.

3.2.5.3.Participantes y Responsabilidades

En el procedimiento se asignan funciones y responsabilidades específicas a los participantes, con el fin de llevar a cabo las actividades necesarias para alcanzar el objetivo principal. Los roles y responsabilidades están detallados en la descripción proporcionada en la Tabla 8.

Tabla 8.

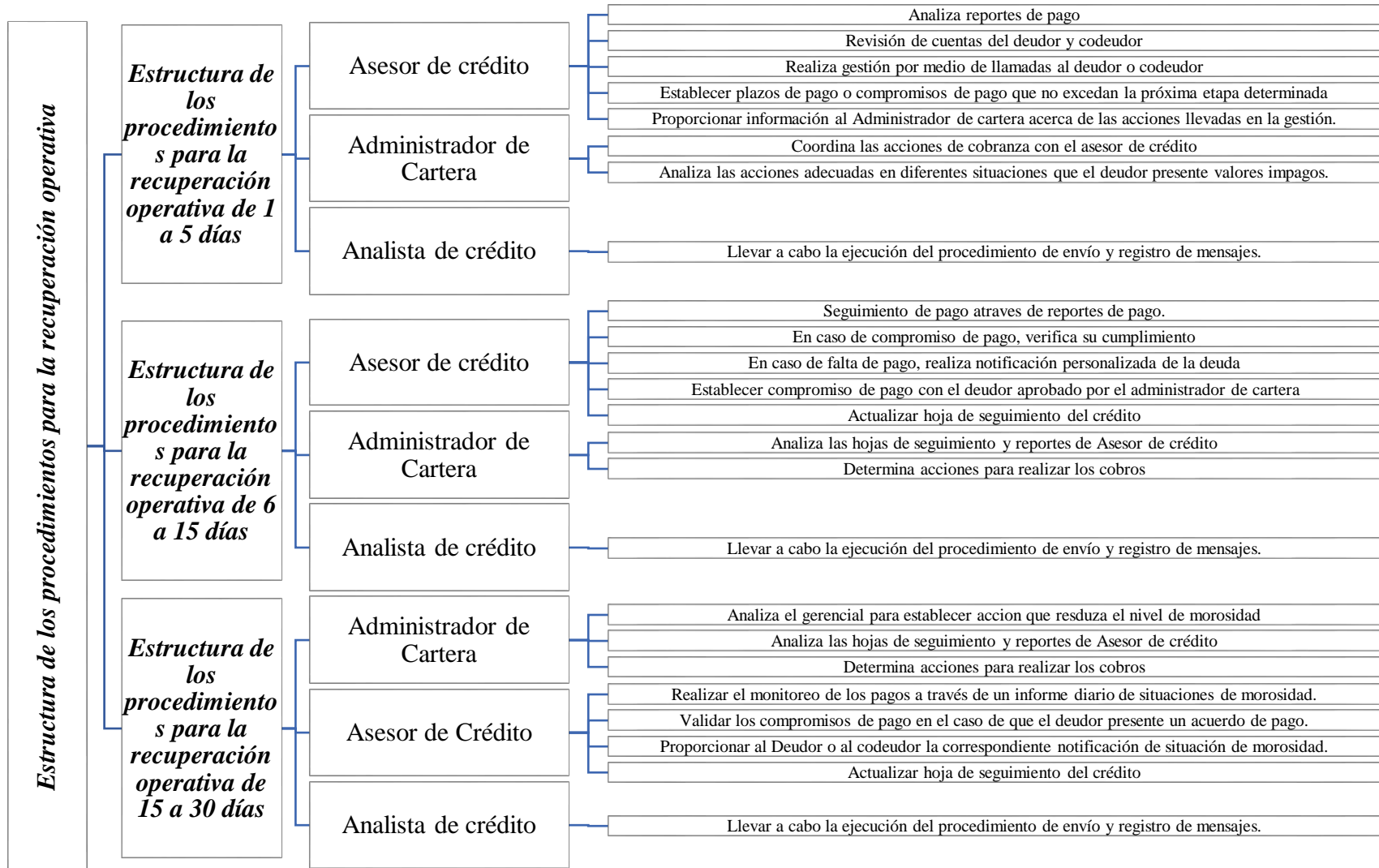
Participantes y responsabilidades

Autoridades	Responsabilidades
Asesor de crédito/ Gestor de Cobranzas	Es el encargado de la administración y supervisión de los socios a cargo, realizando un seguimiento constante de su gestión.
Administrador de Cartera	Su principal función proporciona apoyo y asistencia en los casos de socios que tienen una tendencia recurrente de morosidad.
Analista de Crédito	Se responsabiliza del envío de mensajes de textos como parte de gestión de cobranzas.

3.2.5.4.Estructura de los procedimientos para la recuperación operativa

Figura 17.

Estructura de los procedimientos para la recuperación operativa



4. CAPITULO IV

METODOLOGIA DE SEGURIDAD Y ANALISIS DE RIESGO

En esta sección se centra en un enfoque organizado y metódico empleada para evaluar y administrar los riesgos relacionados con la seguridad de la información. En esta parte, se define una metodología que se empleará para identificar y examinar los datos, así como para realizar un análisis de riesgos en relación con los activos de información. Finalmente, se elaborarán manuales que establecerán políticas basadas en la norma ISO/IEC 27002:2022

4.1. Metodología de Investigación

Esta parte es esencial para establecer la estrategia adecuada en la que se seleccionarán los enfoques para abordar el problema de investigación mediante la recolección de datos utilizando diferentes técnicas. Estas técnicas permitirán llegar a conclusiones sobre los datos obtenidos en la investigación.

4.1.1. Tipo de investigación

Para evaluar amenazas y vulnerabilidades en la seguridad de la información, se analizó la infraestructura tecnológica de la institución financiera COAC "Santa Anita Ltda.". Este análisis se realizó mediante dos tipos de investigación:

- Investigación Descriptiva: Se utilizó este enfoque para examinar las actividades, procedimientos y características fundamentales de la entidad financiera. El objetivo era evaluar los riesgos asociados con la seguridad de la información en el procedimiento de recuperación operativa.
- Investigación Mixta: Se aplicó este método para verificar las políticas existentes relacionadas con la seguridad de la información en la entidad financiera y en el

departamento de Tecnología. Se llevaron a cabo encuestas a los usuarios del sistema de evaluación docente para recopilar información sobre las políticas y prácticas vigentes.

4.1.2. Técnicas de recolección de información

Este enfoque implica identificar y adquirir información utilizando un método de recopilación de datos que incluye las siguientes técnicas de recolección de información:

Revisión documentación: Se solicitó la revisión de documentos relevantes para identificar los procesos internos relacionados con los riesgos en el procedimiento de recuperación operativa de la institución financiera COAC "Santa Anita Ltda.". Los documentos examinados incluyeron el inventario de activos fijos, el manual de políticas y procedimientos de cartera, el reglamento administrativo interno, y reglamento de buen gobierno

- Entrevista: Se realizaron dos entrevistas con personal involucrado en la gestión del área de tecnología en la entidad financiera. La primera entrevista se llevó a cabo con el equipo encargado del procedimiento de recuperación operativa, centrándose en el proceso de recuperación operativa de cartera vencida y el levantamiento de información (ver detalles en el Anexo A). La segunda entrevista tuvo lugar con el equipo responsable del departamento de tecnología, abordando preguntas específicas relacionadas con la infraestructura tecnológica gestionada en la entidad financiera (formato en el Anexo B).
- Encuesta: Se encuentra en proceso una encuesta dirigida a los grupos de trabajo establecidos en el procedimiento. Esta encuesta está enfocada tanto en el equipo de gestión de negocios en la COAC "Santa Anita Ltda." como en el departamento de tecnología, con el objetivo de recolectar información para identificar las características de la herramienta de prevención de pérdida de datos (Data Loss Prevention - DLP) (consultar detalles en el Anexo C).

- Observación de Campo: Se empleó la técnica de observación en el campo para obtener información directa sobre los activos involucrados en el procedimiento de recuperación operativa. Además, se buscó identificar posibles incidentes, peligros y circunstancias adversas que pudieran afectar negativamente a la entidad financiera. La técnica se realizó durante siete días, previa autorización, realizando visitas presenciales a las instalaciones físicas de los laboratorios en varias ocasiones.
- Check List: Después de aplicar la Metodología, se procedió a utilizar un Check List basado en los controles establecidos en la norma ISO 27002:2022. Esto se hizo para evaluar los resultados obtenidos y dar una recomendación adecuada a la entidad financiera.

4.2. Matriz de los activos de información

La matriz de activos de la información se emplea en el análisis de riesgos para identificar y clasificar los activos de información de una organización. Para su elaboración, se han realizado entrevistas que determinaron los archivos involucrados en el proceso de recuperación operativa y cómo la entidad financiera los clasifica para su control. La matriz está compuesta por filas y columnas que representan los distintos activos y las categorías de valoración correspondientes.

La Tabla 9 muestra los activos de información que se gestionan en el proceso, identificando el proceso y el procedimiento asociado a cada uno de ellos. Además, se proporciona una breve descripción del contenido de cada activo de información. En esta sección de descripción de los activos de información, se verifica la información sobre los propietarios, responsables y custodios de cada activo, lo cual nos permite comprender cómo se maneja dicha información dentro del procedimiento

Tabla 9.

Descripción de activo de la información

IDENTIFICACIÓN BÁSICA DEL ACTIVO								
No.	Nombre Del Activo De Información	Proceso	Procedimientos	Descripción (Descripción Del Contenido Del Activo De Información)	Propietario	Responsable	Custodio	Usuarios
1	Reportes de Mora	Gestión de Negocios	Procedimiento de recuperación operativa	Contiene información sobre los días de mora, y cuotas impagas.	Jefe de negocios	Administrador de cartera y Asesor	Administrador de cartera y Asesor	Gestor de Cobranzas, Asesor de Crédito y administrador de cartera
2	Cartera en mora del Asesor	Gestión de Negocios	Procedimiento de recuperación operativa	Información de gestión de recuperación de cartera vencida con clientes en mora de 1 a 30 días	Jefe de negocios	Administrador de cartera y Asesor	Administrador de cartera y Asesor	Gestor de Cobranzas, Asesor de Crédito y administrador de cartera
3	Hoja de seguimiento del crédito	Gestión de Negocios	Procedimiento de recuperación operativa	Seguimiento de los pagos a tiempo de los clientes con crédito.	Jefe de negocios	Administrador de cartera y Asesor	Administrador de cartera y Asesor	Gestor de Cobranzas, Asesor de Crédito y administrador de cartera
4	Registro de Llamadas	Gestión de Negocios	Procedimiento de recuperación operativa	Registro de las llamadas que se realizan para notificar la mora	Jefe de negocios	Asesor de Crédito	Asesor de Crédito	Gestor de Cobranzas, Asesor de Crédito y administrador de cartera
5	Notificaciones gestionadas	Gestión de Negocios	Procedimiento de recuperación operativa	El número de notificaciones y que proceso de gestión	Jefe de negocios	Asesor de Crédito	Asesor de Crédito	Gestor de Cobranzas, Asesor de Crédito y administrador de cartera

6	Reporte de primera notificación de pago	Gestión de Negocios	Procedimiento de recuperación operativa	La primera notificación que se realiza al deudor	Jefe de negocios	Asesor de Crédito	Asesor de Crédito	Gestor de Cobranzas, Asesor de Crédito y administrador de cartera
7	Notificación de morosidad	Gestión de Negocios	Procedimiento de recuperación operativa	Notificación física al deudor	Jefe de negocios	Asesor de Crédito	Asesor de Crédito	Gestor de Cobranzas, Asesor de Crédito y administrador de cartera
8	Notificación al garante	Gestión de Negocios	Procedimiento de recuperación operativa	Notificación física de morosidad al garante del deudor	Jefe de negocios	Asesor de Crédito	Asesor de Crédito	Gestor de Cobranzas, Asesor de Crédito y administrador de cartera
9	Compromiso de Pago	Gestión de Negocios	Procedimiento de recuperación operativa	En caso de llegar a un acuerdo de pago, con el deudor.	Jefe de negocios	Asesor de Crédito	Asesor de Crédito	Gestor de Cobranzas, Asesor de Crédito y administrador de cartera
10	Anexos de créditos vinculados	Gestión de Negocios	Procedimiento de recuperación operativa	Reporte de clientes con crédito	Jefe de negocios	Asesor de Crédito	Asesor de Crédito	Gestor de Cobranzas, Asesor de Crédito y administrador de cartera
11	Anexo de Depósitos a Plazo Fijo	Gestión de Negocios	Procedimiento de recuperación operativa	Reporte de clientes con depósitos a plazo fijo	Jefe de negocios	Asesor de Crédito	Asesor de Crédito	Gestor de Cobranzas, Asesor de Crédito y administrador de cartera
12	Anexo de Ahorros a la vista	Gestión de Negocios	Procedimiento de recuperación operativa	Reporte de clientes que optan por ahorros a la vista	Jefe de negocios	Asesor de Crédito	Asesor de Crédito	Gestor de Cobranzas, Asesor de Crédito y administrador de cartera
13	Base de Datos de Clientes en Mora	Gestión de Negocios	Procedimiento de recuperación operativa	Clientes cuyos pagos o vencimientos se han retrasado.	Jefe de negocios	Asesor de Crédito	Asesor de Crédito	Gestor de Cobranzas, Asesor de Crédito y administrador de cartera

Nota: Elaboración propia a partir de entrevistas realizadas a la entidad financiera.

En la tabla 10, se utilizan los activos analizados en el procedimiento de recuperación operativa para determinar el tipo de activo y su método de conservación. También se especifica el formato en el que se maneja cada activo. Además, se establece un cuestionario de referencia que ayudará a determinar la clasificación de la información asociada a cada activo.

Tabla 10.

Identificación Básica del activo de la información

No.	IDENTIFICACIÓN BÁSICA DEL ACTIVO					La información contiene datos personales	¿La información requiere de algún tipo de control que le brinde protección especial?	¿El Activo necesita de permisos especiales para acceder?	¿La información del activo es exclusivamente de uso interno?	¿En caso de pérdida de esta información, se incurriría en algún tipo de pérdida económica, multa, sanción o daño?	¿La información es para uso exclusivo del propietario o responsable?	¿Si la información no está disponible rápidamente por algún suceso inesperado, afecta negativamente el desarrollo del
	Nombre del Activo de información	Tipo de activo de información	Medio de conservación del Activo de Información	Formato	Respaldo (SI/NO/NA)							
1	Reportes de Mora	Información	Digital	Hoja de cálculo (incluye extensiones como .xls, .xlt, .csv)	NO	SI	SI	SI	SI	SI	NO	SI
2	Cartera en mora del Asesor	Información	Digital	Hoja de cálculo (incluye extensiones como .xls, .xlt, .csv)	NO	SI	SI	SI	SI	SI	NO	SI
3	Hoja de seguimiento del crédito	Información	Digital	Hoja de cálculo (incluye extensiones como .xls, .xlt, .csv)	NO	SI	SI	SI	SI	SI	NO	SI
4	Registro de Llamadas	Información	Digital	Hoja de cálculo (incluye extensiones como .xls, .xlt, .csv)	NO	SI	SI	SI	SI	SI	NO	SI

5	Notificaciones gestionadas	Información	Digital	Hoja de cálculo (incluye extensiones como .xls, .xlt, .csv)	NO	SI	SI	SI	SI	SI	NO	SI
6	Reporte de primera notificación de pago	Información	Físico	Impreso (Papel)	NO	SI	SI	SI	SI	SI	NO	SI
7	Notificación de morosidad	Información	Físico	Impreso (Papel)	NO	SI	SI	SI	SI	SI	NO	SI
8	Notificación al garante	Información	Físico	Impreso (Papel)	NO	SI	SI	SI	SI	SI	NO	SI
9	Compromiso de Pago	Información	Físico	Impreso (Papel)	NO	SI	SI	SI	SI	SI	NO	SI
10	Anexos de créditos vinculados	Software	Digital	Base de datos (incluye extensiones como .mdb, .sql)	NO	SI	SI	SI	SI	SI	NO	SI
11	Anexo de Depósitos a Plazo Fijo	Software	Digital	Base de datos (incluye extensiones como .mdb, .sql)	NO	SI	SI	SI	SI	SI	NO	SI
12	Anexo de Ahorros a la vista	Software	Digital	Base de datos (incluye extensiones como .mdb, .sql)	NO	SI	SI	SI	SI	SI	NO	SI
13	Base de Datos de Clientes en Mora	Software	Digital	Base de datos (incluye extensiones como .mdb, .sql)	NO	SI	SI	SI	SI	SI	NO	SI

Nota: Elaboración propia a partir de entrevistas realizadas a la entidad financiera.

Como conclusión de la matriz que organiza los activos de información, se establece la clasificación correspondiente para cada uno de ellos. Esta clasificación determina el nivel de criticidad del activo de información para la entidad financiera, y permite determinar la categoría en la que se encuentra cada activo, siguiendo los parámetros previamente establecidos. Como se puede observar en la Tabla 11.

Tabla 11.

Identificación Básica del activo de la información

IDENTIFICACIÓN BÁSICA DEL ACTIVO		PROPIEDADES DE SEGURIDAD DE INFORMACIÓN				El activo se encuentra publicado y/o disponible o ni publicado ni disponible	Lugar de consulta	Soporte Legal que establece el por qué se recibe o solicita información
No.	Nombre del Activo de Información	1. Clas. Disponibilidad (Baja, Media, Alta o Muy Alta)	2. Clas. Confidencialidad (Clasificada, Reservada, Pública de Uso Interno, Pública)	3. Clas. Integridad (Baja, Media, Alta, Crítica)	4. Nivel de Criticidad (Clasificación del Nivel de Criticidad del activo de Información para la Entidad Financiera)			
1	Reportes de Mora	Baja	Pública Clasificada	Alta	Alta	Ni disponible ni publicado	Core Financiero	
2	Cartera en mora del Asesor	Alta	Pública Clasificada	Alta	Alta	Ni disponible ni publicado	Core Financiero	
3	Hoja de seguimiento del crédito	Media	Pública Clasificada	Alta	Alta	Ni disponible ni publicado	Core Financiero	
4	Registro de Llamadas	Media	Pública Clasificada	Media	Media	Ni disponible ni publicado	Core Financiero	
5	Notificaciones gestionadas	Alta	Pública Clasificada	Alta	Alta	Ni disponible ni publicado	Core Financiero	

6	Reporte de primera notificación de pago	Media	Pública Clasificada	Alta	Alta	Ni disponible ni publicado	Core Financiero	
7	Notificación de morosidad	Media	Pública Clasificada	Alta	Alta	Ni disponible ni publicado	Core Financiero	Junta de regulación monetaria financiera
8	Notificación al garante	Media	Pública Clasificada	Alta	Alta	Ni disponible ni publicado	Core Financiero	Junta de regulación monetaria financiera
9	Compromiso de Pago	Media	Pública Clasificada	Alta	Alta	Ni disponible ni publicado	Core Financiero	Junta de regulación monetaria financiera
10	Anexos de créditos vinculados	Media	Pública Clasificada	Alta	Alta	Ni disponible ni publicado	Core Financiero	
11	Anexo de Depósitos a Plazo Fijo	Media	Pública Clasificada	Alta	Alta	Ni disponible ni publicado	Core Financiero	
12	Anexo de Ahorros a la vista	Media	Pública Clasificada	Alta	Alta	Ni disponible ni publicado	Core Financiero	
13	Base de Datos de Clientes en Mora	Media	Pública Clasificada	Alta	Alta	Ni disponible ni publicado	Core Financiero	

Nota: Elaboración propia a partir de entrevistas realizadas a la entidad financiera.

4.3. Análisis y Gestión de riesgo mediante la Metodología Magerit v3.0

En esta sección se presenta una descripción detallada del análisis y la gestión de riesgos utilizando la metodología Magerit 3.0, la cual recomienda el uso de la herramienta PILAR. Esta herramienta permite identificar los activos físicos y de información de la entidad financiera, específicamente en el proceso de recuperación operativa, mediante entrevistas con el personal involucrado en dicha área. Mediante el uso de esta herramienta, se logra identificar las amenazas a las que se enfrentan los activos más importantes y se pueden establecer las salvaguardas apropiadas.

En este procedimiento, se lleva a cabo un análisis cualitativo de los activos involucrados en el proceso de recuperación operativa, siguiendo el enfoque de la metodología Magerit y las directrices establecidas en la norma 27002:2022. Para facilitar este análisis, se utiliza la herramienta PILAR, que permite identificar y establecer las salvaguardas necesarias para proteger los activos en esa situación específica.

4.3.1. Contexto

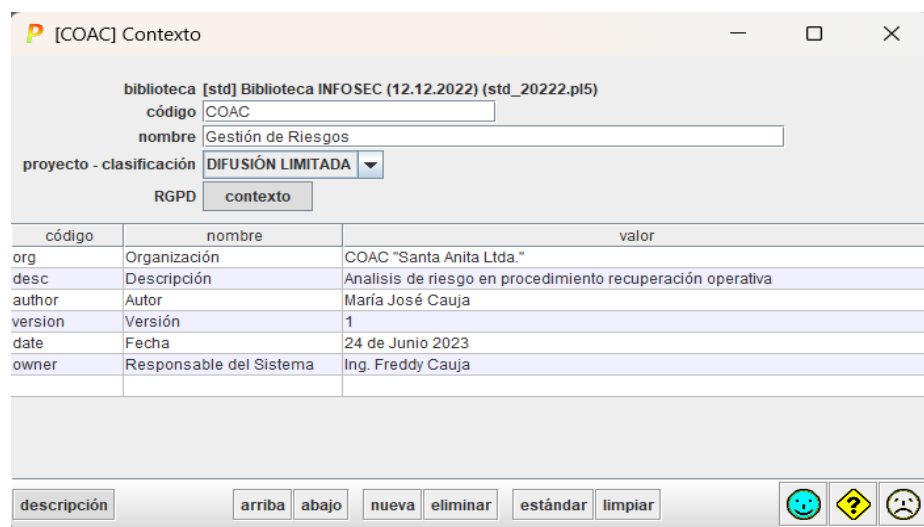
Para la gestión de riesgos en el proceso de recuperación operativa de la entidad financiera COAC "Santa Anita Ltda.", se ha elegido utilizar la versión PILAR RM (versión 1.2.2022) con una licencia de evaluación. Esta elección se debe a las amplias características que ofrece esta versión en comparación con otras disponibles.

Para facilitar el análisis de riesgos, la metodología MAGERIT cuenta con su documento complementario llamado "Catálogo de Elementos". El propósito de este catálogo es normalizar y proporcionar un conjunto de elementos más homogéneo, que incluye una lista de tipos de activos, dimensiones, criterios de valoración y tipos de amenazas para cada activo.

La herramienta utilizada también proporciona una descripción de los datos del proyecto, como se muestra en la Figura 18. Esta descripción detalla las actividades que se llevarán a cabo en el departamento de gestión de cobranza en relación al proceso de recuperación operativa.

Figura 18.

Creación del proyecto PILAR



código	nombre	valor
org	Organización	COAC "Santa Anita Ltda."
desc	Descripción	Análisis de riesgo en procedimiento recuperación operativa
author	Autor	María José Cauja
version	Versión	1
date	Fecha	24 de Junio 2023
owner	Responsable del Sistema	Ing. Freddy Cauja

Nota: Elaboración propia a partir de la experiencia en la aplicación PILAR.

4.3.2. Determinación de activos

Un activo de información se refiere a cualquier recurso o elemento que posee valor para una organización. El propósito de los activos es proteger para asegurar la operación del negocio y garantizar su continuidad.

Según la norma ISO 17799:2005, los activos se clasifican en diferentes categorías:

- **Activos de Información:** Estos activos comprenden la propia información, ya sea en forma digital o física, como datos confidenciales, documentos, registros, bases de datos, software, entre otros.
- **Activos de infraestructura tecnológica:** Estos activos incluyen los componentes de hardware y software empleados para el procesamiento, almacenamiento y transmisión de información, tales como servidores, redes, sistemas operativos, aplicaciones, entre otros.

- **Activos de Comunicación:** Se refieren a los sistemas de comunicación empleados para transmitir información, como redes de área local (LAN), redes de área amplia (WAN), Internet, sistemas de correo electrónico, entre otros
- **Activos humanos:** Hacen referencia a las personas que están involucradas en el manejo y uso de la información, tales como empleados, contratistas, usuarios finales y personal de seguridad.
- En la organización que se está evaluando, cada miembro del personal tiene la responsabilidad de manejar uno o más activos de la institución según su función. Sin embargo, todos los activos no tienen la misma relevancia dentro de la organización. Por lo tanto, la implementación de los mecanismos de seguridad dependerá de las amenazas específicas que afecten a cada activo en particular.

La Tabla 12 muestra la clasificación de activos de acuerdo al "Catálogo de Elementos", el segundo documento de la metodología MAGERIT.

Tabla 12.

Tipos de activos según Metodología Magerit

Tipo de Activo	Descripción
Datos/Información	Los datos esenciales para las funciones de la organización pueden ser tanto físicos como digitales
Servicios	Los servicios técnicos incluyen servicios de computación, servicios de mantenimiento y servicios de soporte.
Software	los sistemas de información utilizados dentro de la organización, que incluyen aplicaciones informáticas, software de sistemas, herramientas tecnológicas, bases de datos, sistemas de virtualización y correo electrónico.
Hardware	Equipo informático para brindar servicios en la organización. Esto incluye equipos tecnológicos como computadoras, servidores y equipos de red.

Redes de Comunicaciones	Las instalaciones utilizadas para los servicios de comunicaciones, que generalmente son contratados a terceros
Soporte de información	Dispositivos físicos utilizados para el almacenamiento de información a largo plazo.
Equipamiento auxiliar	Los equipos que brindan soporte a los sistemas de información, pero que no están directamente relacionados con los datos.
Instalaciones	Los espacios físicos donde están los sistemas de información. Esto puede incluir edificios, departamentos, vehículos, contenedores, entre otros.
Personal	Las personas que están involucradas con los sistemas de información, como usuarios externos, usuarios internos, operadores, administradores, desarrolladores, entre otros.

Nota. Elaboración propia de la descripción de tipos de activos.

4.3.3. Se elabora identificación de los activos de información

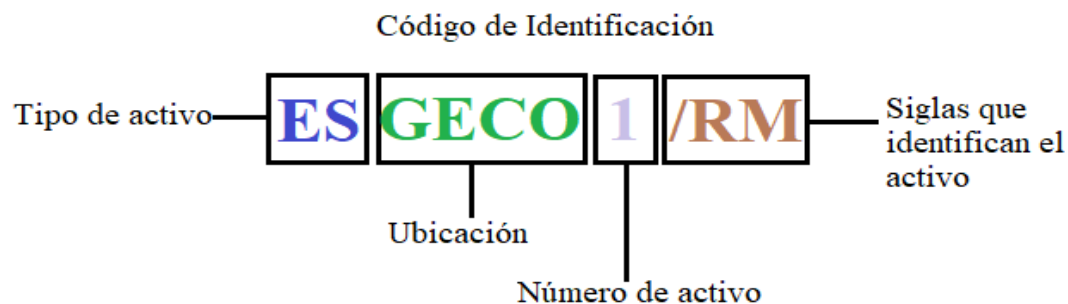
Los activos considerados en el análisis y gestión de riesgos se seleccionaron según su importancia para la entidad financiera. Siguiendo la metodología Magerit, cada activo de información debe ser identificado con un código específico. En la Figura 19 se presenta un ejemplo del código utilizado. Este código se estructura de la siguiente manera:

Tipo de activo: Las dos primeras letras del código identifican la categoría o tipo de activo al que pertenece. (Ejemplo: ES esencial, HW hardware, SW software y AUX elemento auxiliar).

- Ubicación: Las siglas representan la ubicación física del activo. (Ejemplo: GECO Gestión de Cobranzas).
- Número de activo: Este fragmento ilustra la numeración asignada a cada activo en su conjunto.
- Siglas que identifican el activo: Las siglas utilizadas representan el nombre del activo, lo que facilita su reconocimiento y comprensión

Figura 19.

Código de Identificación



Nota: Elaboración propia de nomenclatura.

La Tabla 13 presenta el listado de activos relacionados con el proceso de recuperación operativa, los cuales serán evaluados utilizando la herramienta PILAR. Estos activos han sido previamente clasificados según las recomendaciones de la metodología Magerit.

Tabla 13.

Clasificación de Activos

ACTIVOS PROCESO DE RECUPERACIÓN OPERATIVA			
[B]Activos Esenciales			
[DC] Reportes			
Código	Nombre	Detalle	
ESGECO1/RM	RM	Reportes de Mora	
ESGECO2/CMA	CMA	Cartera en mora del asesor	
ESGECO3/HSC	HSC	Hoja de seguimiento de crédito	
ESGECO4/RLL	RLL	Registro de llamadas	
ESGECO5/NG	NG	Notificaciones gestionadas	
ESGECO6/RP	RP	Reporte de la primera	
ESGECO7/NP	NP	notificación de pago	
ESGECO8/NM	NM	notificación de morosidad	
ESGECO9/NG	NG	notificación al garante	
ESGECO10/CP	CP	Compromiso de pago	
ESGECO11/ACV	ACV	Anexos de créditos vinculados	
[DB] Base de Datos			

DBGECO1/ADP	ADP	Anexo a Depósitos a Plazo fijo
DBGECO2/AAV	AAV	Anexo de Ahorro a la vista
DBGECO3/BDC	BDC	Base de Datos de clientes en mora
[IS] Servicios Internos		
ISGECO1/INT	INT	Acceso a internet
ISGECO2/PW	PW	Portal Web- Intranet
[E] Equipamiento		
<i>[HW] Equipos</i>		
HWGECO1/SBD	SBD	Servidor Base de datos
HWGECO2/PTR	PTR	Puesto de Trabajo
HWGECO3/SPW	SPW	Servidor de portal web
HWGECO4/FIR	FIR	Firewall
HWGECO5/LAN	LAN	Red Local
HWGECO6/SCF	SCF	Servidor Core Financiero
HWGECO7/DM	DM	Dispositivos Móviles
[AUX] Elementos Auxiliares		
AUXGECO1/VEH	VEH	Vehículos
AUXGECO2/EC	EC	Equipo Climatización
AUXGECO3/GE	GE	Generador Eléctrico
AUXGECO4/CF	CF	Caja Fuerte
AUXGECO5/CD	CD	Cableado de Datos
[SW] Aplicaciones		
SWGECO1/CFF	CFF	Core Financiero (Financial)
SWGECO2/OFFICE	OFFICE	Office 365
[SS] Servicios Subcontratados		
SSGECO1/ADSL	ADSL	Conexión a internet
SSGECO2/SAR	SAR	Servicio de Administración de Red
[L] Instalaciones		

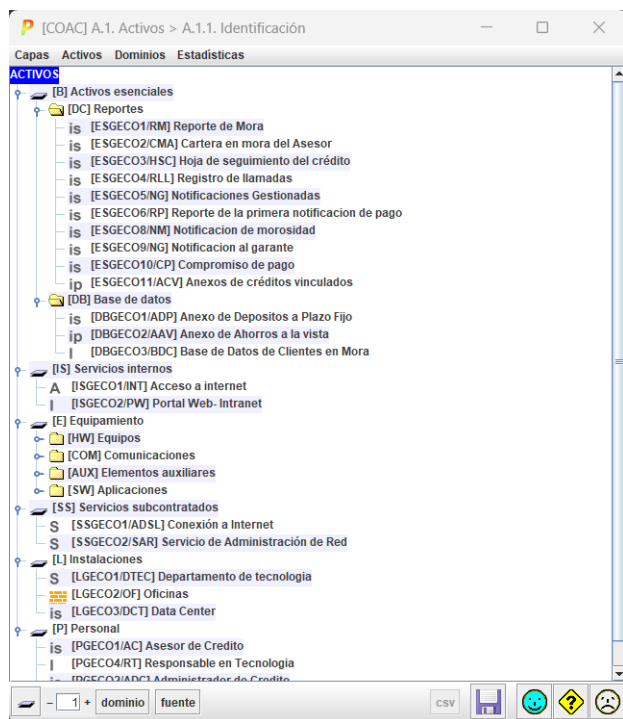
LGECO1/DTEC	DTEC	Departamento de tecnología
LGECO2/OF	OF	Oficinas
LGECO3/DCT	DCT	Data Center
[P] Personal		
PGECO1/AC	AC	Asesor de Crédito
PGECO2/ADC	ADC	Administrador de Crédito
PGECO3/ANC	ANC	Analista de Crédito
PGECO4/RT	RT	Responsable de Tecnología

Nota: Elaboración propia a partir de la nomenclatura establecida según los activos de la información

A continuación, en la Figura 20 se categorizan los activos de acuerdo a su función en el proceso de recuperación operativa.

Figura 20.

Activos del proceso de recuperación operativa



Nota: Elaboración propia a partir de la experiencia en la aplicación PILAR.

4.3.4. Dependencia entre activos

Algunos activos están interrelacionados y dependen de otros más importantes, como equipos, comunicaciones y personal, entre otros. Es fundamental identificar si existe alguna dependencia entre los activos, ya que podría darse el caso de que un activo de menor importancia se vea afectado si se materializa una amenaza en un activo más relevante. Si se detecta una dependencia entre los activos, se puede generar un árbol de dependencias para visualizar y comprender mejor estas relaciones.

La figura 21 muestra la clasificación de los activos en distintas dependencias, lo que proporciona una visualización de la cantidad de activos presentes en cada una de ellas. Además, se indica la asignación de capas para los activos de información del proceso de recuperación operativa

Figura 21.

Dependencia de activos

capa	[essential]	[arch]	[qualifier]	[D]	[keys]	[S]	[SW]	[HW]	[COM]	[Media]	[AUX]	[L]	[P]	[other]	total
B	13	0	9	12	0	8	11	9	0	1	0	9	8	0	13
IS	1	2	0	0	0	1	0	1	0	0	0	0	0	0	2
E	5	1	0	2	0	1	6	5	3	1	5	4	1	0	14
SS	2	0	0	0	0	2	0	0	0	0	0	0	0	0	2
L	2	1	0	1	0	0	1	2	1	0	0	3	3	0	3
P	4	0	0	0	0	0	4	0	0	0	0	0	4	0	4
TOTAL	27	4	9	15	0	12	22	17	4	2	5	16	16	0	38

Nota: Elaboración propia a partir de la experiencia en la aplicación PILAR.

Es importante tener en cuenta que un mismo activo puede tener múltiples clasificaciones, por lo que los totales en la tabla no siempre son la suma de las otras celdas.

4.3.5. Valoración de activos

La valoración de los activos puede realizarse de forma cuantitativa, asignando valores numéricos, o de forma cualitativa, utilizando niveles de importancia. Para lograr una valoración precisa de los activos, es necesario tener un profundo conocimiento del proceso o sistema que se

está evaluando. Esto implica revisar documentación relevante de la organización y establecer comunicación con las personas involucradas en dicho proceso.

Según la metodología Magerit, se sugiere emplear una escala del cero al diez para valorar los activos. Un valor de cero indica que el activo tiene poca importancia y su pérdida o daño no tendría un impacto significativo en las actividades de la organización. Por otro lado, un valor de diez indica que la pérdida o daño de ese activo acarrearía graves consecuencias para la organización.

La Figura 21 muestra la valoración de las propiedades de la información para cada activo, considerando los parámetros de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad. Los criterios de valoración se han establecido de manera homogénea para todos los tipos de activos, basándose en los criterios descritos en el libro "Catálogos de elementos" de la metodología Magerit

Figura 22.

Valoración de activos Software PILAR

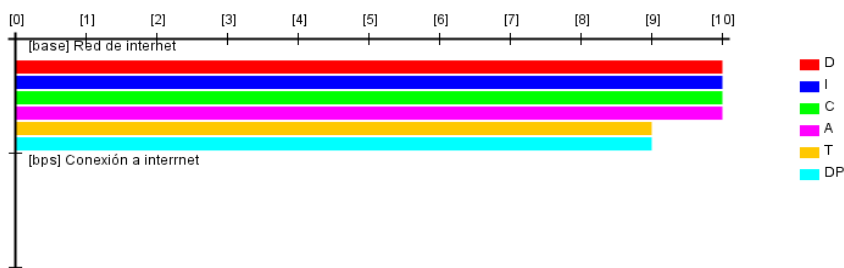
activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS						
[B] Activos esenciales						
[DC] Reportes						
is [ESGECO1RM] Reporte de Mora	[9]	[10]	[9]	[4]	[9]	[7]
is [ESGECO2CMA] Cartera en mora del Asesor	[8]	[10]	[8]	[6]	[8]	[7]
is [ESGECO3HSC] Hoja de seguimiento del crédito	[8]	[8]	[8]	[5]	[5]	[7]
is [ESGECO4RLL] Registro de llamadas	[9]	[10]	[10]	[9]	[8]	[7]
is [ESGECO5NG] Notificaciones Gestionadas	[8]	[9]	[9]	[4]	[7]	[7]
is [ESGECO6RP] Reporte de la primera notificación de pago	[9]	[9]	[8]	[7]	[7]	[7]
is [ESGECO8NM] Notificación de morosidad	[8]	[10]	[10]	[9]	[7]	[7]
is [ESGECO9NG] Notificación al garante	[7]	[10]	[10]	[6]	[8]	[7]
is [ESGECO10CP] Compromiso de pago	[10]	[10]	[10]	[10]	[7]	[7]
ip [ESGECO11ACV] Anexos de créditos vinculados	[9]	[10]	[8]	[9]	[9]	[7]
[DB] Bases de datos						
is [DBGECO1ADP] Anexo de Depositos a Plazo Fijo	[8]	[10]	[8]	[8]	[5]	[7]
ip [DBGECO2AAV] Anexo de Ahorros a la vista	[8]	[10]	[9]	[8]	[8]	[8]
l [DBGECO3BDC] Base de Datos de Clientes en Mora	[9]	[8]	[9]	[8]	[7]	[10]
[IS] Servicios internos						
A [ISGECO1INT] Acceso a internet	[9]	[9]	[9]	[9]	[9]	n.a.
l [ISGECO2PW] Portal Web- Intranet	[10]	[10]	[5]	[5]	[7]	n.a.
[E] Equipamiento						
[HW] Equipos						
l [HWGECO1SBD] Servidor Base de Datos	[10]	[10]	[10]	[8]	[9]	[8]
A [HWGECO2PTR] Puesto de trabajo	[7]	[7]	[9]	[9]	[9]	n.a.
S [HWGECO3SPW] Servidor de portal web	[10]	[10]	[9]	[8]	[9]	n.a.
is [HWGECO4FR] Firewall	[10]	[10]	[10]	[9]	[9]	[9]
S [HWGECO5SC] Servidor Core Financiero	[10]	[10]	[9]	[9]	[9]	[8]
[COM] Comunicaciones						
A [COMGECO1DM] Dispositivos Moviles	[9]	[9]	[7]	[9]	[9]	[7]
S [COMGECO2LM] Red Local	[10]	[10]	[9]	[8]	[9]	[4]
[AUX] Elementos auxiliares						
A [AUXGECO1VEH] Vehiculos	[7]	[6]	[9]	[7]	[7]	[4]
A [AUXGECO2EC] Equipo Climatizacion	[7]	[7]	[7]	[7]	[7]	n.a.
A [AUXGECO3GE] Generador Electrico	[7]	[7]	[7]	[7]	[7]	n.a.
A [AUXGECO4CF] Caja Fuerte	[7]	[7]	[7]	[7]	[7]	n.a.
A [AUXGECO5CD] Cableado de Datos	[7]	[7]	[7]	[7]	[7]	n.a.
[SW] Aplicaciones						
A [SWGECO1CF] Core Financiero (Financial)	[9]	[7]	[7]	[9]	[7]	[9]
A [SWGECO2OFFICE] OFFICE365	[9]	[7]	[7]	[7]	[7]	[7]

Nota: Elaboración propia a partir de la experiencia en la aplicación PILAR.

En la figura 21, se establece la valoración del dominio de seguridad de los activos de información en el proceso de recuperación operativa

Figura 23.

Valoración del dominio de seguridad de los activos de la información

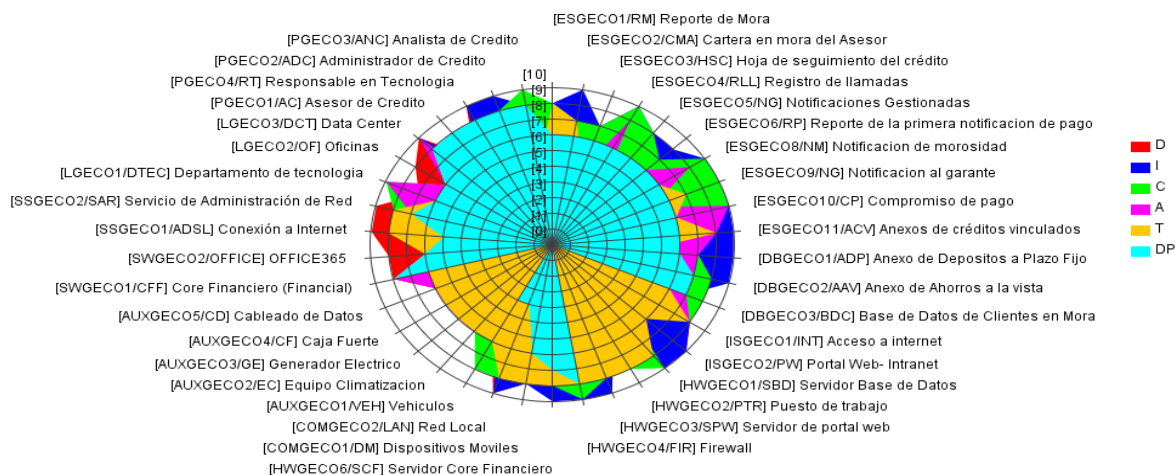


Nota: Elaboración propia a partir de la experiencia en la aplicación PILAR.

La Figura 24 muestra un gráfico que representa el valor de los activos según las dimensiones establecidas para cada uno.

Figura 24.

Valor de activos Proceso Recuperación Operativa



Nota: Elaboración propia a partir de la experiencia en la aplicación PILAR.

4.3.6. Identificación de amenazas

En el análisis de riesgo, es fundamental identificar las posibles fuentes o eventos que podrían causar incidentes o impactar los activos de información. La metodología Magerit, a través

de su "Catálogo de Elementos", ofrece una variedad de categorías de amenazas que pueden servir como referencia en este proceso.

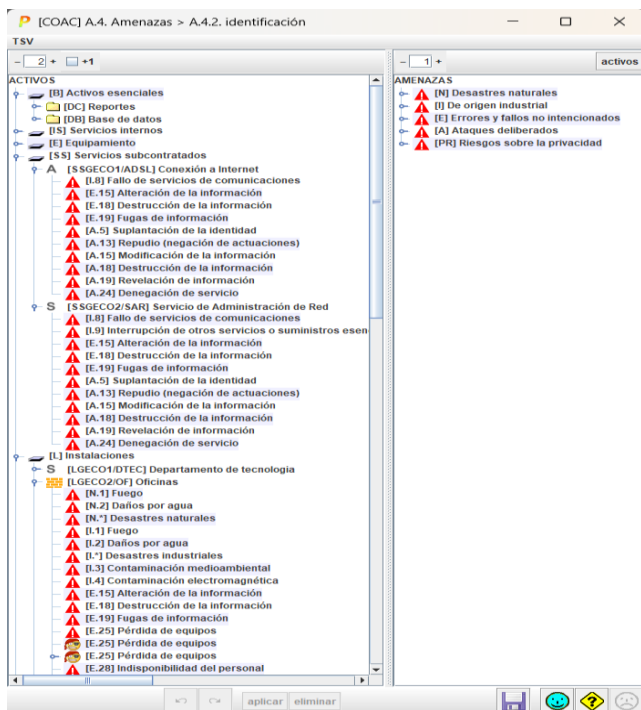
Se categorizan en cinco tipos distintos de amenazas.

- [N] Desastres Naturales
- [I] Origen Industria
- [E] Errores y Fallos no intencionados
- [A] Ataques intencionados
- [PR] Riesgo sobre la privacidad

Para cada tipo de activo, Magerit establece una relación con las amenazas potenciales que podrían afectarlo. En la figura 25 se muestra una lista de amenazas asociadas a los demás activos del proceso de recuperación operativa, tal como se mencionó anteriormente.

Figura 25.

Identificación de amenazas de los activos del proceso de recuperación operativa



Nota: Elaboración propia a partir de la experiencia en la aplicación PILAR.

4.3.7. Valoración de amenazas

En la herramienta PILAR, se realiza la evaluación y valoración de las amenazas utilizando un proceso que tiene en cuenta factores como la probabilidad de ocurrencia y el impacto potencial de cada amenaza. Esta valoración se utiliza para determinar el nivel de riesgo asociado a cada amenaza y para establecer las medidas de protección adecuadas, priorizando aquellas que sean más efectivas para mitigar los riesgos identificados.

En la tabla 14 se proporciona información sobre la probabilidad de ocurrencia de una amenaza, es decir, la posibilidad de que dicha amenaza se materialice.

Tabla 14.

Probabilidad de ocurrencia

Potencial	probabilidad	Nivel	Facilidad	Frecuencia
XL Extragrande	CS Casi seguro	MA Muy alto	F Fácil	100
L Grande	MA Muy alta	A Alto	M Medio	10
M Medio	P Posible	M Medio	D Difícil	1
S Pequeño	PP Poco posible	B Bajo	MD Muy Difícil	0.1
XS Muy pequeño	MR Muy rara	MB Muy Bajo	ED Extremadamente Difícil	0.01

En la herramienta PILAR, se utiliza el valor de amenazas para evaluar y definir el nivel o porcentaje de las cinco dimensiones que se aplican a los activos de información. Esta evaluación se representa en la figura 26, mencionada.

Figura 26.

Valoración según su nivel y porcentaje

activo	co...	nivel	[D]	[I]	[C]	[A]	[T]	[DP]
[SW] Aplicaciones								
A [SWGECO1/CFF] Core Financiero (Financial)			100%	100%	100%			
[L.5.1] Avería de origen lógico		M	50%					
[E.8] Difusión de software dañino		M	10%	10%	10%			
[E.20] Vulnerabilidades de los programas (s		M	1%	20%	20%			
[E.21] Errores de mantenimiento / actualiza		A	1%	10%	50%			
[A.8] Difusión de software dañino		M	100%	100%	100%			
[A.22] Manipulación de programas		M	50%	100%	100%			
A [SWGECO2/OFFICE] OFFICE365			100%	100%	100%			
[L.5.1] Avería de origen lógico		M	50%					
[E.8] Difusión de software dañino		M	10%	10%	10%			
[E.20] Vulnerabilidades de los programas (s		M	1%	20%	20%			
[E.21] Errores de mantenimiento / actualiza		A	1%	10%	50%			
[A.8] Difusión de software dañino		M	100%	100%	100%			
[A.22] Manipulación de programas		M	50%	100%	100%			
[SS] Servicios subcontratados								
A [SSGECO1/ADSL] Conexión a Internet			100%	100%	100%	100%	100%	
[I.8] Fallo de servicios de comunicaciones		M	100%					
[E.15] Alteración de la información		M		10%				
[E.18] Destrucción de la información		M	10%					
[E.19] Fugas de información		M			10%			
[A.5] Suplantación de la identidad		B		100%	100%	100%		
[A.13] Repudio (negación de actuaciones)		M					100%	
[A.15] Modificación de la información		M		50%				
[A.18] Destrucción de la información		M	50%					
[A.19] Revelación de información		M			50%			
[A.24] Denegación de servicio		M	50%					
S [SSGECO2/SAR] Servicio de Administración de Red			100%	100%	100%	100%	100%	
[I.8] Fallo de servicios de comunicaciones		M	100%					
[I.9] Interrupción de otros servicios o suministr		M	50%					

Nota: Elaboración propia a partir de la experiencia en la aplicación PILAR.

El Anexo G establece una evaluación de los activos de información, determinando el valor de las amenazas en función de conceptos clave como la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y datos personales.

4.3.8. Impacto acumulado

El impacto acumulado en la herramienta PILAR se refiere a la evaluación conjunta del impacto que podrían tener varias amenazas sobre un activo de información. Se calcula teniendo en cuenta tanto la probabilidad de ocurrencia de cada amenaza como su impacto potencial en el activo.

En la herramienta, es posible asignar valores de probabilidad e impacto a cada amenaza, y luego se realiza el cálculo del impacto acumulado considerando la combinación de todas las amenazas que podrían afectar al activo. Esta evaluación del impacto acumulado permite determinar la importancia relativa de los activos y facilita la toma de decisiones para implementar las medidas de protección más adecuadas.

A continuación, la Figura 27 muestra la acumulación del impacto en los activos de información del proceso de recuperación operativa

Figura 27.

Impacto acumulativo

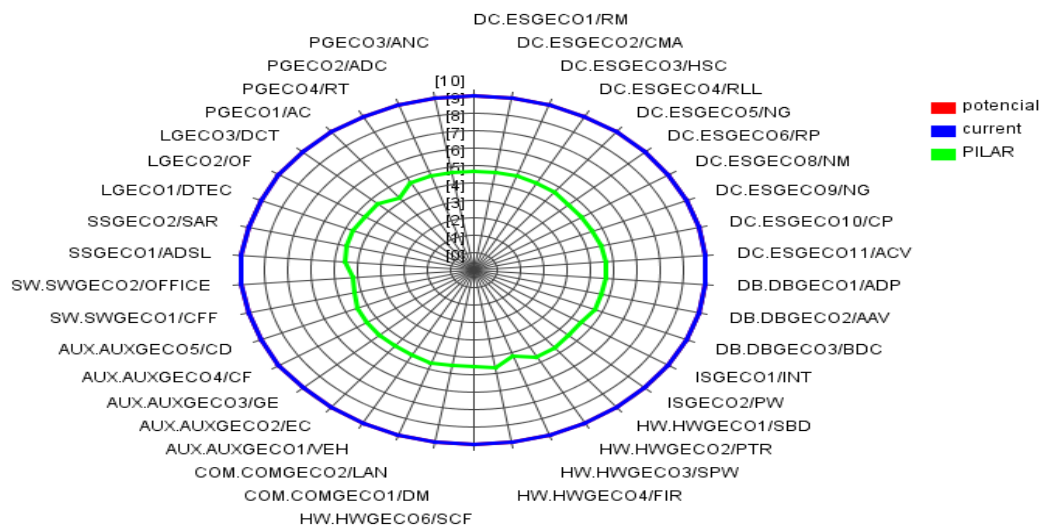
activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS	[10]	[10]	[10]	[10]	[9]	[9]
[B] Activos esenciales	[10]	[10]	[10]	[10]	[9]	[9]
[DC] Reportes	[10]	[10]	[10]	[10]	[9]	[9]
[ESGECO4/IRM] Reporte de Mora	[90]	[10]	[10]	[10]	[8]	[9]
[ESGECO2/CMA] Cartera en mora del Asesor	[8]	[10]	[10]	[10]	[9]	[9]
[ESGECO3/HSC] Hoja de seguimiento del crédito	[8]	[10]	[10]	[10]	[9]	[9]
[ESGECO4/RLL] Registro de llamadas	[9]	[10]	[10]	[10]	[9]	[9]
[ESGECO5/NG] Notificaciones Gestionadas	[8]	[10]	[10]	[10]	[9]	[9]
[ESGECO6/RP] Reporte de la primera notificación de pago	[9]	[10]	[10]	[10]	[9]	[9]
[ESGECO8/NM] Notificación de morosidad	[8]	[10]	[10]	[10]	[9]	[9]
[ESGECO9/NG] Notificación al garante	[7]	[10]	[10]	[10]	[9]	[9]
[ESGECO10/CP] Compromiso de pago	[9]	[10]	[10]	[10]	[9]	[9]
[ESGECO11/ACV] Anexos de créditos vinculados	[90]	[10]	[10]	[10]	[8]	[9]
[DB] Base de datos	[10]	[10]	[10]	[10]	[8]	[9]
[IDBGE01/ADP] Anexo de Depositos a Plazo Fijo	[10]	[10]	[10]	[10]	[8]	[9]
[IDBGE02/AAV] Anexo de Ahorros a la vista	[10]	[10]	[10]	[10]	[8]	[9]
[IDBGE03/BDC] Base de Datos de Clientes en Mora	[4]	[7]	[9]	[10]	[8]	[9]
[IS] Servicios internos	[10]	[9]	[9]	[10]	[9]	
[ISGECO1/INT] Acceso a internet	[90]	[7]	[9]			
[ISGECO2/PW] Portal Web- Intranet	[9]	[9]	[9]	[10]	[9]	
[E] Equipamiento	[10]	[10]	[10]	[10]	[9]	
[HW] Equipos						
[HWGECO1/SBD] Servidor Base de Datos	[10]	[10]	[10]	[10]	[9]	
[HWGECO2/PTR] Puesto de trabajo	[10]	[9]	[10]	[10]		
[HWGECO3/SPW] Servidor de portal web	[10]	[10]	[10]		[8]	
[HWGECO4/FIR] Firewall	[10]	[10]	[10]	[10]	[8]	
[HWGECO6/SCF] Servidor Core Financiero	[90]	[10]	[10]	[10]	[8]	
[COM] Comunicaciones	[10]	[8]	[9]	[10]		
[COMGECO1/DM] Dispositivos Moviles	[10]	[8]	[9]	[10]		
[COMGECO2/LAN] Red Local	[10]	[8]	[9]	[10]	[8]	
[AUX] Elementos auxiliares	[10]	[7]	[10]			
[SW] Aplicaciones	[10]	[10]	[10]			

Nota: Elaboración propia a partir de la experiencia en la aplicación PILAR.

La figura 28 ofrece una representación gráfica que muestra cómo el impacto de las amenazas se va acumulando en los activos a medida que ocurren. Esta visualización permite comprender la importancia de los activos y facilita la identificación de quienes necesitan mayor atención en medidas de protección y mitigación de riesgos. En la gráfica representan tanto las características de la información con respecto al proyecto y las recomendaciones por la herramienta Pilar.

Figura 28.

Impacto acumulado en el proceso de recuperación operativa



Nota: Elaboración propia a partir de la experiencia en la aplicación PILAR.

4.3.9. Riesgo Acumulado

En la metodología Magerit, el riesgo acumulado es una medida utilizada para evaluar el nivel total de riesgo asociado a un activo o sistema de información. En la herramienta PILAR, se realiza la evaluación del nivel total de riesgo que enfrentan los activos de información. El riesgo acumulado es la combinación de todas las amenazas y su impacto en los activos, lo que da una medida integral del riesgo. Esta información es crucial para priorizar las acciones de protección y tomar decisiones fundamentadas en la gestión de riesgos en el ámbito de la seguridad de la información.

En la figura 29 de PILAR, se muestra la estimación del riesgo, la cual se basa en la relación entre la probabilidad de que ocurra un riesgo y el impacto que este causaría. La figura representa el nivel de riesgo al que se enfrenta cada activo, utilizando colores que indican su nivel de criticidad.

Figura 29.

Riesgo Acumulado

[COAC] A.6.1. Valores acumulados > A.6.1.2. riesgo

Ver Exportar

potencial current PILAR

activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS	(8,0)	(8,6)	(8,6)	(8,6)	(6,9)	(7,1)
[B] Activos esenciales	(7,7)	(8,1)	(8,1)	(8,6)	(6,9)	(7,1)
[DC] Reportes	(7,7)	(8,1)	(8,1)	(8,6)	(6,9)	(7,1)
[ESGECO1/IRM] Reporte de Mora	(7,4)	(6,8)	(8,1)	(7,7)	(5,7)	(7,1)
[ESGECO2/CMA] Cartera en mora del Asesor	(6,5)	(8,1)	(8,1)	(8,6)	(6,9)	(7,1)
[ESGECO3/HSC] Hoja de seguimiento del crédito	(6,5)	(7,2)	(8,1)	(8,6)	(6,9)	(7,1)
[ESGECO4/RLL] Registro de llamadas	(7,1)	(7,2)	(8,1)	(8,6)	(6,9)	(7,1)
[ESGECO5/NG] Notificaciones Gestionadas	(6,5)	(7,2)	(8,1)	(8,6)	(6,9)	(7,1)
[ESGECO6/RP] Reporte de la primera notificación de pago	(7,1)	(7,2)	(8,1)	(8,6)	(6,9)	(7,1)
[ESGECO8/NM] Notificación de morosidad	(6,5)	(7,2)	(8,1)	(8,6)	(6,9)	(7,1)
[ESGECO9/NG] Notificación al garante	(5,9)	(7,2)	(8,1)	(8,6)	(6,9)	(7,1)
[ESGECO10/CP] Compromiso de pago	(7,7)	(7,2)	(8,1)	(8,6)	(6,9)	(7,1)
[ESGECO11/ACV] Anexos de créditos vinculados	(6,8)	(6,8)	(8,1)	(7,7)	(5,7)	(7,1)
[DB] Base de datos	(6,8)	(6,8)	(8,1)	(7,7)	(5,7)	(7,1)
[DBGECO1/ADP] Anexo de Depositos a Plazo Fijo	(6,8)	(6,8)	(8,1)	(7,7)	(5,7)	(7,1)
[DBGECO2/AAV] Anexo de Ahorros a la vista	(6,8)	(6,8)	(8,1)	(7,7)	(5,7)	(7,1)
[DBGECO3/BDC] Base de Datos de Clientes en Mora	(4,2)	(6,8)	(8,1)	(7,7)	(5,7)	(7,1)
[SI] Servicios internos	(7,2)	(7,2)	(8,1)	(8,6)	(6,9)	
[ISGECO1/INT] Acceso a internet	(7,2)	(5,1)	(6,3)			
[ISGECO2/PW] Portal Web- Intranet	(7,2)	(7,2)	(8,1)	(8,6)	(6,9)	
[E] Equipamiento	(8,0)	(8,1)	(8,1)	(7,7)	(6,9)	
[HW] Equipos	(7,7)	(8,1)	(8,1)	(7,7)	(6,9)	
[HWGECO1/SBD] Servidor Base de Datos	(7,7)	(7,2)	(7,2)	(6,8)	(6,9)	
[HWGECO2/PTR] Puesto de trabajo	(7,2)	(6,3)	(7,7)	(6,8)		
[HWGECO3/SPW] Servidor de portal web	(6,8)	(6,8)	(7,2)		(5,7)	
[HWGECO4/FIR] Firewall	(7,2)	(6,8)	(8,1)	(7,7)	(5,7)	
[HWGECO6/SCF] Servidor Core Financiero	(7,2)	(8,1)	(8,1)	(7,7)	(5,7)	
[COM] Comunicaciones	(8,0)	(5,6)	(7,4)	(6,8)	(5,7)	
[COMGECO1/DM] Dispositivos Moviles	(8,0)	(5,6)	(7,4)	(6,8)		
[COMGECO2/LAN] Red Local	(7,7)	(5,6)	(6,3)	(6,8)	(5,7)	
[AUX] Elementos auxiliares	(7,7)	(5,1)	(7,7)			
[AUXGECO1/VEH] Vehiculos	(6,8)		(7,7)			

niveles de criticidad

- (9) - catástrofe
- (8) - desastre
- (7) - extremadamente crítico
- (6) - muy crítico
- (5) - crítico
- (4) - muy alto
- (3) - alto
- (2) - medio
- (1) - bajo
- (0) - despreciable

1 + -1 dominio fuente gestionar leyenda

Nota: Elaboración propia a partir de la experiencia en la aplicación PILAR.

4.3.10. Salvaguardas

En el marco de la Metodología Magerit, en su documento titulado "Catálogo de Elementos", se hace referencia a las salvaguardas como acciones o controles que se establecen con el propósito de disminuir los riesgos identificados en un sistema de información. Se reconoce que estas salvaguardas evolucionan en concordancia con el progreso tecnológico.

Al determinar las salvaguardas, es importante considerar diversos aspectos, que incluyen el tipo de activo que se busca proteger, las amenazas que requieren protección y las alternativas de salvaguardas disponibles. Además, se ha tenido en cuenta el principio de proporcionalidad, considerando los valores de los activos y la probabilidad de ocurrencia de las amenazas.

Las salvaguardas ofrecen diferentes características para mitigar los riesgos identificados.

Las salvaguardas en MAGERIT se clasifican según el aspecto que abordan, que se identifica mediante las siguientes etiquetas: [G] para Gestión, [T] para Técnico, [F] para Seguridad Física y [P] para Gestión del Personal. Estas etiquetas indican el enfoque específico de cada salvaguarda en términos de gestión, aspectos técnicos, seguridad física o gestión del personal.

Las salvaguardas se categorizan según el tipo de protección que brindan, y esta clasificación se presenta en la siguiente Tabla 15.

Tabla 15.

Tipo de protección

Tipo de protección	Detalle
[PR] Prevención	Las medidas implementadas disminuyen las posibilidades de que ocurra un incidente.
[DR] Disuasión	Evitar que un atacante se sienta tentado a llevar a cabo un ataque.
[EL] Eliminación	Previenen la ocurrencia del incidente al evitar que se produzca.
[IM] Minimización del impacto	Limitan o reducen las repercusiones de un incidente.
[CR] Corrección	Se encargan de remediar o reparar los daños causados previamente.
[RC] Recuperación	Posibilitan la restauración al estado previo al incidente.
[AD] Administrativa	Son los elementos de seguridad del sistema.
[AW] Concienciación	La capacitación del personal involucrado con el sistema.
[DC] Detección	Pueden identificar y reportar la presencia de un ataque en curso.
[MN] Monitorización	Supervisan los incidentes ocurridos y que están ocurriendo para prever posibles incidentes.

La clasificación de las salvaguardas se realiza en función de su peso relativo o nivel de importancia, tal como se ilustra en la figura 30.

Figura 30.

Peso Relativo

	Máximo peso	Critica
	Peso alto	Muy importante
	Peso normal	Importante
	Peso bajo	Interesante
	Aseguramiento: componentes certificados	

Nota: Elaboración propia a partir de la experiencia en la aplicación PILAR.

El propósito de implementar salvaguardas es proteger los activos de información, como datos, sistemas y recursos, de amenazas potenciales y minimizar la probabilidad de que los riesgos se materialicen. En el ámbito de la seguridad y gestión de riesgos, se proponen diversas salvaguardas para abordar estos riesgos. En este caso particular, se han identificado 25 salvaguardas, que se presentan en la Figura 31.

Figura 31.

Identificación de salvaguardas para la entidad financiera COAC Santa Anita

as...	tdp	rec.	nivel	salvaguarda	dudas	fuente	base	com...	nivel	PLAN
				SALVAGUARDAS					..L3	L2-L5
G	EL	9		[A] Identificación y autenticación						L2-L4
T	EL	7		[AC] Control de acceso lógico						L2-L4
G	PR	9		[D] Protección de la Información					..L2	L2-L5
G	EL			[K] Protección de claves criptográficas [SC-12]						n.a.
G	PR	6		[S] Protección de los Servicios						L2-L4
G	PR	6		[SW] Protección de las Aplicaciones Informáticas (SW)						L2-L4
G	PR	5		[HW] Protección de los Equipos Informáticos (HW)						L2-L3
G	PR	9		[COM] Protección de las Comunicaciones						L2-L5
G	PR	6		[M] Protección de los Soportes de Información						L2-L4
G	PR	6		[AUX] Elementos Auxiliares						L2-L4
F	EL	6		[PPE] Protección física de los equipos						L2-L4
F	PR	5		[L] Protección de las Instalaciones						L2-L3
P	PR	6		[P] Gestión del Personal						L2-L4
G	CR	6		[IM] Gestión de incidentes						L2-L4
T	PR	7		[tools] Herramientas de seguridad					..L1	L2-L4
G	CR	3		[V] Gestión de vulnerabilidades						L2-L3
T	MN	4		[A] Registro y auditoría						L2-L3
G	RC	3		[BC] Continuidad del negocio						L2-L3
G	AD	5		[G] Organización						L2-L3
G	AD	5		[E] Relaciones Externas						L2-L3
G	AD	5		[NEW] Adquisición / desarrollo						L2-L3
G	PR			[PDS] Servicios potencialmente peligrosos					..L3	n.a.
G	PR	7		[PI] Sistema de protección de frontera lógica						L2-L4
F	EL	9		[PPS] Protección del perímetro físico						L2-L5
G	EL	3 (o)		[TEMPEST] Protección de emanaciones (TEMPEST) [PE-19]						L2-L3
T	PR	7		[AcB] ACCESS CONTROL [AC, ACb]						L2-L4
P	AW	2		[AT] AWARENESS AND TRAINING						L2
G	MN	3		[AU] AUDIT AND ACCOUNTABILITY						L2-L3
G	PR	3		[CA] ASSESSMENT, AUTHORIZATION, AND MONITORING						L3
G	PR	3		[CM] CONFIGURATION MANAGEMENT						L2-L3
G	PR	4		[CP] CONTINGENCY PLANNING						L3
T	EL	9		[IAB] IDENTIFICATION AND AUTHENTICATION [IA, IAb]						L3-L5
G	CR	4		[IR] INCIDENT RESPONSE						L2-L3

Nota: Elaboración propia a partir de la experiencia en la aplicación PILAR.

Si PILAR no identifica ninguna razón para aplicar una determinada salvaguarda, la celda correspondiente se muestra en color gris. Esto indica que PILAR no considera que esa salvaguarda mitigue ningún riesgo específico.

4.3.11. Valoración de Salvaguardas

En este análisis se abordan diversos aspectos relacionados con las recomendaciones proporcionadas por la herramienta PILAR. Teniendo en cuenta su evaluación en cada dimensión pertinente. Para representar estas recomendaciones, se emplea un sistema de codificación específico.

En la Figura 32 se presenta una representación de los valores de las salvaguardas y las amenazas identificadas en la herramienta PILAR. Esta representación permite determinar el nivel de criticidad para cada activo de información.

Figura 32.

Valoración de Salvaguardas

The screenshot displays the PILAR application interface. The main window shows a table with columns for 'activo', 'amenaza', 'dimensión', 'riesgo', 'current', and 'PILAR'. The 'riesgo' column is color-coded from red (high risk) to yellow (medium risk). A legend on the right side of the screen defines criticality levels from (9) - catástrofe to (0) - despreciable.

activo	amenaza	dimensión	riesgo	current	PILAR
[ISGECO2/PW] Portal Web- Intranet	[A.11] Acceso no autorizado	[A]	(8,6)	(5,5)	(5,5)
[ESGECO2/CMA] Cartera en mora del Ases...	[A.11] Acceso no autorizado	[A]	(8,6)	(5,5)	(5,3)
[LGECO1/DTEC] Departamento de tecnolo...	[A.11] Acceso no autorizado	[A]	(8,6)	(5,5)	(5,3)
[ESGECO5/NG] Notificaciones Gestionadas	[A.11] Acceso no autorizado	[A]	(8,6)	(5,5)	(5,3)
[ESGECO4/RLL] Registro de llamadas	[A.11] Acceso no autorizado	[A]	(8,6)	(5,5)	(5,3)
[ESGECO6/RP] Reporte de la primera notifi...	[A.11] Acceso no autorizado	[A]	(8,6)	(5,5)	(5,3)
[ESGECO9/NG] Notificación al garante	[A.11] Acceso no autorizado	[A]	(8,6)	(5,5)	(5,3)
[ESGECO8/NM] Notificación de morosidad	[A.11] Acceso no autorizado	[A]	(8,6)	(5,5)	(5,3)
[ESGECO10/CP] Compromiso de pago	[A.11] Acceso no autorizado	[A]	(8,6)	(5,5)	(5,3)
[ESGECO3/HSC] Hoja de seguimiento del c...	[A.11] Acceso no autorizado	[A]	(8,6)	(5,5)	(5,3)
[HWGECO6/SCF] Servidor Core Financiero	[A.3] Manipulación de los registros de acti...	[I]	(8,1)	(6,7)	(4,6)
[HWGECO6/SCF] Servidor Core Financiero	[A.11] Acceso no autorizado	[C]	(8,1)	(6,7)	(4,6)
[HWGECO4/FIR] Firewall	[A.11] Acceso no autorizado	[C]	(8,1)	(6,7)	(4,6)
[ESGECO2/CMA] Cartera en mora del Ases...	[A.3] Manipulación de los registros de acti...	[I]	(8,1)	(6,7)	(4,6)
[ESGECO11/ACV] Anexos de créditos vinc...	[A.11] Acceso no autorizado	[C]	(8,1)	(6,7)	(4,6)
[DBGECO1/ADP] Anexo de Depositos a Pla...	[A.11] Acceso no autorizado	[C]	(8,1)	(6,7)	(4,6)
[DBGECO2/AAV] Anexo de Ahorros a la vista	[A.11] Acceso no autorizado	[C]	(8,1)	(6,7)	(4,6)
[ESGECO1/RM] Reporte de Mora	[A.11] Acceso no autorizado	[C]	(8,1)	(6,7)	(4,6)
[ISGECO2/PW] Portal Web- Intranet	[A.11] Acceso no autorizado	[C]	(8,1)	(6,7)	(4,6)
[PGECO2/ADC] Administrador de Credito	[A.11] Acceso no autorizado	[C]	(8,1)	(6,7)	(4,6)
[PGECO3/ANC] Analista de Credito	[A.11] Acceso no autorizado	[C]	(8,1)	(6,7)	(4,6)
[PGECO4/RT] Responsable en Tecnologia	[A.11] Acceso no autorizado	[C]	(8,1)	(6,7)	(4,6)
[LGECO1/DTEC] Departamento de tecnolo...	[A.11] Acceso no autorizado	[C]	(8,1)	(6,7)	(4,5)
[ESGECO2/CMA] Cartera en mora del Ases...	[A.11] Acceso no autorizado	[C]	(8,1)	(6,7)	(4,5)

Legend (niveles de criticidad):

- (9) - catástrofe
- (8) - desastre
- (7) - extremadamente crítico
- (6) - muy crítico
- (5) - crítico
- (4) - muy alto
- (3) - alto
- (2) - medio
- (1) - bajo
- (0) - despreciable

Nota: Elaboración propia a partir de la experiencia en la aplicación PILAR.

4.4.Desarrollo de manual para la prevención de fuga de información

En esta sección se presenta una propuesta para desarrollar un manual de procedimientos que documente el Sistema de Gestión de Seguridad de la Información (SGSI) para la entidad financiera COAC "Santa Anita Ltda.". Este manual se alinearé con la norma ISO/IEC 27002:2022, que se basa en las mejores prácticas en seguridad de la información.

Los documentos resultantes del manual de procedimientos de fuga de información servirán como una guía para orientar las actividades relacionadas con el proceso de recuperación operativa. El enfoque estará en gestionar los controles de la documentación requeridos por la normativa, lo cual contribuirá a prevenir fugas de información.

4.4.1. Reportes de cumplimiento de la norma 27002:2022

En el Anexo G, se ha generado el informe de cumplimiento de la norma ISO/IEC 27002:2022 utilizando la herramienta PILAR. Este informe se basa en las especificaciones configuradas y el análisis de las amenazas y salvaguardas, lo que ha permitido determinar un enfoque de aplicabilidad de la norma. De esta manera, se evidencia cómo se aplica la norma en función de la información administrada.

Se ha determinado que la sección 5.2 sobre la clasificación de la información se caracteriza por tener un nivel de madurez reproducible, pero intuitivo. Esto significa que busca lograr resultados y procesos consistentes y replicables, al tiempo que se presenta de forma comprensible e intuitiva. Se siguen métodos rigurosos para garantizar la fiabilidad del manejo de la información, pero también se enfoca en hacerlo de manera clara y accesible para quienes están a cargo de cada activo de información.

En el control 8.12 sobre prevención de fuga de información, se ha establecido un nivel de madurez que corresponde a un proceso definido. Esto significa que cada etapa del proceso tiene

una descripción detallada, se asignaron roles y responsabilidades específicas, se establecieron criterios claros de entrada y salida y se identificaron los recursos necesarios para realizar todas las actividades involucradas.

La entidad financiera cuenta con una estructura organizativa que se rige por un sistema de gestión basado en procesos. Aunque se ha realizado un informe del nivel de madurez para los controles 5.12 y 8.12 de la norma ISO/IEC 27002:2022, también se debe asegurar la incorporación de las mejores prácticas basadas en dicha normativa. Esto se hará para mejorar la prevención y manejo de los activos de la información, considerando las amenazas y salvaguardas identificadas en la herramienta PILAR, según la información establecida.

4.4.2. Manual para prevención de fuga de información

En este manual se describe la estructura y funcionamiento del sistema de prevención de fuga de información, así como la identificación de los procesos y procedimientos involucrados en el proceso de recuperación operativa de la entidad financiera COAC "Santa Anita Ltda.". Estas acciones han sido diseñadas con el propósito de asegurar el cumplimiento de la Política y los Objetivos establecidos para la prevención de fuga de información, siguiendo los requisitos establecidos en la Norma ISO/IEC 27002:2022. Esta norma aborda específicamente los controles 5.12 y 8.12 relacionado con la prevención de fuga de información, y la estructura del presente documento busca asegurar la seguridad y protección de los activos de información de la empresa, evitando así que información valiosa termine en manos equivocadas.

4.4.3. Manual de Políticas y Procedimiento de Prevención de Fuga de Información

En este manual se describen los procedimientos o actividades a realizar en cada proceso definido para prevenir fuga de información. Su objetivo principal es establecer los procesos y

procedimientos específicos necesarios para prevenir, detectar y responder a posibles fugas de información confidencial o sensible en la entidad financiera.

Es importante destacar que la descripción de cómo ejecutar cada una de las actividades contenidas en este manual es una propuesta flexible y estará sujeta a ajustes a medida que se avanza en la implementación, con el propósito de perfeccionarlos y adaptarlos según las necesidades y la evolución de la entidad.

COOPERATIVA DE AHORRO Y CRÉDITO SANTA ANITA LTDA.


SISTEMA DE GESTIÓN POR PROCESOS



Santa Anita
COOPERATIVA DE AHORRO Y CRÉDITO

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN SGP-MPFI-01

MARIA JOSE CAUJA ALTAMIRANO

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información
		Versión:01
		Página: 2 de 23

SISTEMA DE GESTIÓN DE PROCESOS


MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN


Control de documentación

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre:	María José Cauja	Ing. Marlon Cevallos	Ing. Diamela Gallegos
Cargo:	Tesista	Oficial de seguridad	Gerencia
Firma:			
Fecha:	5 de enero de 2024	26 de Enero de 2024	26 de Enero de 2024

Ficha de Edición del documento

Nombre del Documento:	Manual de Prevención de Fuga de Información	
Código del Documento	SGP-MPFI-01	
Edición	01	
Fecha de Edición	27 de octubre de 2023	
Responsable de Edición	María José Cauja	
Cargo	Tesista	
Cambios Realizados	Autor de Edición	Fechas de Ediciones

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información
		Versión:01
		Página: 2 de 23

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información
		Versión:01
		Página: 2 de 23

SISTEMA DE GESTIÓN DE PROCESOS


MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN

Control de documentación

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre:	María José Cauja	Ing. Marlon Cevallos	Ing. Diamela Gallegos
Cargo:	Tesista	Oficial de seguridad	Gerencia
Firma:			
Fecha:	27 de octubre de 2023	26 de Enero de 2024	26 de Enero de 2024


Ficha de Edición del documento

Nombre del Documento:	Manual de Prevención de Fuga de Información	
Código del Documento	SGP-MPFI-01	
Edición	01	
Fecha de Edición	27 de octubre de 2023	
Responsable de Edición	María José Cauja	
Cargo	Tesista	
Cambios Realizados	Autor de Edición	Fechas de Ediciones


MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01	
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas	Versión:01
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información	

Contenido

Control de documentación	1
Ficha de Edición del documento.....	1
1. Gestión de manual prevención de fuga de información.....	5
1.1. Objetivo	5
1.2. Presentación y uso	5
1.3. Características del Manual.....	6
1.4. Control del manual	6
1.5. Referencias Normativas.....	7
1.6. Términos y Definiciones	7
2. Información del procedimiento de Recuperación Operativa	8
2.1. Misión.....	9
2.2. Visión.....	9
2.3. Análisis situacional.....	9
3. Estructura de la documentación	10
4. Roles, responsabilidades y autoridad de la entidad financiera COAC “Santa Anita Ltda.”	12
5. Requerimientos de la Ley Orgánica de Protección de Datos Personales.....	13
6. Requerimientos de la Norma ISO/IEC 27002:2022	14
6.1. Requerimientos de seguridad de la información	15
6.2. Control 5.12: Clasificación de la información.....	15
6.3. Control 8.12: Prevención de fuga de datos.....	17
7. Modelo de Operación.....	18

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información
		Versión:01
		Página: 2 de 23

7.1.	FASE 1: Planificar.....	19
7.2.	FASE 2: Hacer.....	21
7.3.	FASE 3: Verificar.....	22
7.4.	FASE 4: Plan de Contingencia	23

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01	
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas	Versión:01
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información	
		Página: 2 de 23	

1. Gestión de manual prevención de fuga de información

En este manual sobre prevención de fuga de información, se proporciona un documento público que está disponible para cualquier persona interesada en conocer los estándares de control propuestos para el procedimiento de recuperación operativa de la entidad financiera COAC "Santa Anita Ltda."


1.1.Objetivo

El propósito de este documento es establecer y describir las directrices generales del Sistema de Gestión de la Seguridad de la Información de la entidad financiera, siguiendo los requisitos establecidos en la Norma ISO 27002:2022. Este documento sirve como un modelo de mejora continua para prevenir la fuga de información en el sistema de la entidad, al proporcionar información actualizada y constante a las partes interesadas. Su objetivo es guiar las actividades y mejorar los aspectos organizacionales relacionados con la seguridad de la información.

1.2.Presentación y uso

Este Manual de Prevención de Fuga de Información engloba el alcance definido en el procedimiento de recuperación operativa de la entidad financiera COAC "Santa Anita Ltda". Incluye la Política y Objetivos de prevención de fuga de información, el organigrama, muestra los procesos establecidos en esta infraestructura, su interacción y hace referencia a los procedimientos y otros documentos que participan en el proceso.

Este manual es una herramienta de uso constante para todos los involucrados en actividades relacionadas con el procedimiento de recuperación operativa. Además, refleja la filosofía institucional de trabajo y un enfoque financiero. Es una guía esencial que muestra la

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información

visión integral de cómo se aborda la prevención de fuga de información en la entidad financiera, proporcionando una base sólida y coherente para el desarrollo de estas tareas.

1.3. Características del Manual

El Manual de Prevención de Fuga de Información proporciona una descripción detallada del Sistema de Gestión por Procesos de la entidad financiera COAC "Santa Anita". Para facilitar su comprensión, se encuentra relacionado con el documento "SGP-GA-01 Guía para Elaboración y Gestión de Documentos", que ofrece información adicional sobre ciertos aspectos.

Este documento es de acceso público y está disponible para aquellos interesados en conocer los estándares establecidos por la norma ISO/IEC 27002:2022 aplicados a la entidad financiera.


1.4. Control del manual

- **Elaboración, Revisión y Aprobación**

La autoridad competente de COAC "Santa Anita Ltda." designará a un Coordinador para el proyecto propuesto de Prevención de Fuga de Información, quien será responsable de elaborar y revisar el Manual de Prevención de Fuga de Información. Asimismo, la Alta Dirección será la encargada de aprobar dicho documento.

- **Ficha de Edición del documento**

Para gestionar las ediciones realizadas en el Manual de Prevención de Fuga de Información, se deben seguir las directrices establecidas en la "SGP-GA-01 Guía para Elaboración y Gestión de Documentos". Los registros de edición se deberán establecer en las diferentes versiones del Manual de Prevención de Fuga de Información se efectúan en la página 2 de dicho documento mencionado.

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información
		Versión:01
		Página: 2 de 23

1.5.Referencias Normativas

Las referencias normativas aplicables a este Manual son las siguientes:

- ISO/IEC 27002 Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información.
- Normativa vigente de la entidad financiera COAC “Santa Anita Ltda.”
- Manual de políticas y procedimiento de Administración de Cartera.
- Manual de Seguridad.

1.6.Términos y Definiciones


En el contexto de este Manual de Prevención de Fuga de Información, se deben considerar los términos y definiciones establecidos en las Normas ISO/IEC 27002:2022 como aplicables.

- Información confidencial: información que no está destinada a ser puesta a disposición o divulgada a personas, entidades o procesos.
- Control: medida que mantiene y/o modifica el riesgo

Nota: Los controles incluyen, entre otros, cualquier proceso, política, dispositivo, práctica u otras condiciones y/o acciones que mantienen y/o modifican el riesgo.

- No repudio: capacidad de probar la ocurrencia de un evento o acción reclamado y sus entidades de origen.
- Personal: personas que realizan un trabajo bajo la dirección de la organización

Nota: El concepto de personal incluye a los miembros de la organización, como el órgano de gobierno, la alta directivos, empleados, personal temporal, contratistas y voluntarios.

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información
		Versión:01
		Página: 2 de 23


- Política: Intenciones y dirección de una organización, expresadas formalmente por su alta dirección.’
- Procedimiento: forma especificada de llevar a cabo una actividad o un proceso
- Proceso: conjunto de actividades interrelacionadas o interactuantes que utiliza o transforma entradas para entregar un resultado.
- Información sensible: información que debe protegerse de la indisponibilidad, el acceso no autorizado, la modificación o la divulgación pública divulgación pública debido a posibles efectos adversos sobre una persona, organización, seguridad nacional o seguridad pública
- Vulnerabilidad: debilidad de un activo o control que puede ser explotada por una o más amenazas.
- Usuario: Parte interesada con acceso a los sistemas de información de la organización.

2. Información del procedimiento de Recuperación Operativa

La información proporcionada en este apartado tiene el propósito de ofrecer una comprensión detallada del entorno y las actividades realizadas en la entidad financiera COAC "Santa Anita Ltda."

Esta cooperativa de ahorro y crédito fue establecida en 2001 por iniciativa de La UNORCAC (Unión de Organizaciones Campesinas e Indígenas de Cotacachi), con el objetivo principal de respaldar el desarrollo económico y social de los sectores indígenas y campesinos en Cotacachi, provincia de Imbabura.

Los recursos financieros de la cooperativa provienen principalmente de los ahorros de sus socios, aunque también cuenta con acceso a líneas de crédito ofrecidas por prestamistas externos.

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información

En cuanto a los servicios, la cooperativa brinda tecnologías tanto individuales como grupales solidarias para satisfacer las necesidades financieras de sus clientes.

2.1.Misión

Somos una Cooperativa de Ahorro y Crédito confiable y solvente del sector financiero Popular y solidario que ofrece productos y servicios dirigidos a nuestros socios y clientes en la región sierra Norte del País, impulsando el crecimiento económico, cuidado al medio ambiente, desarrollo social e inclusión financiera de la comunidad.

2.2.Visión

Ser una Cooperativa de Ahorro y Crédito sostenible, reconocida por preservar la inclusión social, promover la calidad humana en nuestra gente, brindar productos y servicios para satisfacer las necesidades financieras de socios y clientes.

2.3.Análisis situacional

El análisis FODA en una organización permite detectar sus fortalezas y debilidades, junto con las oportunidades y amenazas que enfrenta, al considerar tanto los aspectos internos como externos que pueden afectar la efectividad de las medidas de seguridad y prevención implementadas.


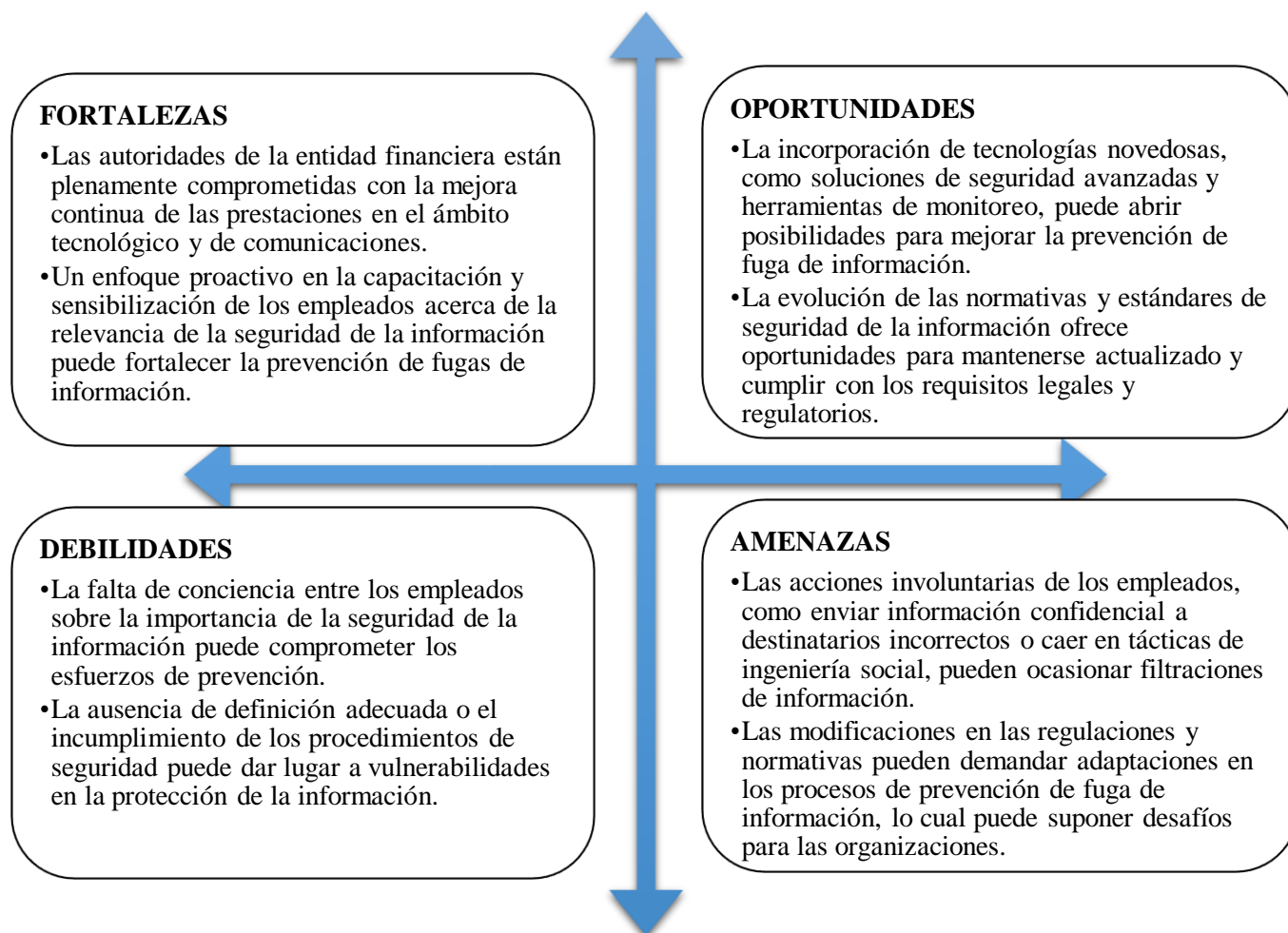
MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01	
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas	Versión:01
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información	
		Página: 2 de 23	

Figura 33.


Análisis situacional del procedimiento de recuperación operativa-FODA



Nota: Elaboración propia

3. Estructura de la documentación

Con el fin de asegurar la consistencia, mantenimiento y mejora continua del sistema de gestión por procesos, se ha establecido una estructura documental que contiene todos los documentos necesarios para facilitar su identificación, búsqueda, uso, modificación y control. En esta estructura, el presente Manual de Prevención de Fuga de Información ocupa el nivel de mayor jerarquía. La jerarquía de la documentación se muestra en la Figura 4.

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01	
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas	Versión:01
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información	
		Página: 2 de 23	

- Manual de Prevención de Fuga de Información: Este manual abarca cómo el procedimiento de recuperación operativa de la entidad financiera COAC "Santa Anita Ltda." cumple con los requisitos de la norma ISO/IEC 27002:2022. Incluye la Misión, Visión, Política de Prevención y los Objetivos que respaldan dicha política. Se basa en la metodología ISO 27001 PDCA (Planificar, Hacer, Verificar, Actuar) en el que se determina en cada sección su respectivo procedimiento
- Mapa y caracterización de procesos: El mapa de procesos proporciona una visión general de la interacción entre los diferentes procesos establecidos en la entidad financiera COAC "Santa Anita". Por otro lado, el documento de caracterización de procesos contiene información que permite identificar las condiciones y/o elementos que forman parte de cada proceso.
- Manual de políticas y procedimientos para prevención de fuga de información: Este documento describe la manera en que se lleva a cabo las políticas y procedimientos específicos para la prevención de fuga de información.
- Guías de elaboración y gestión de documentos: Este documento establecerá formatos que ayudarán a determinar ciertas características de la información necesaria para el conocimiento del proceso.


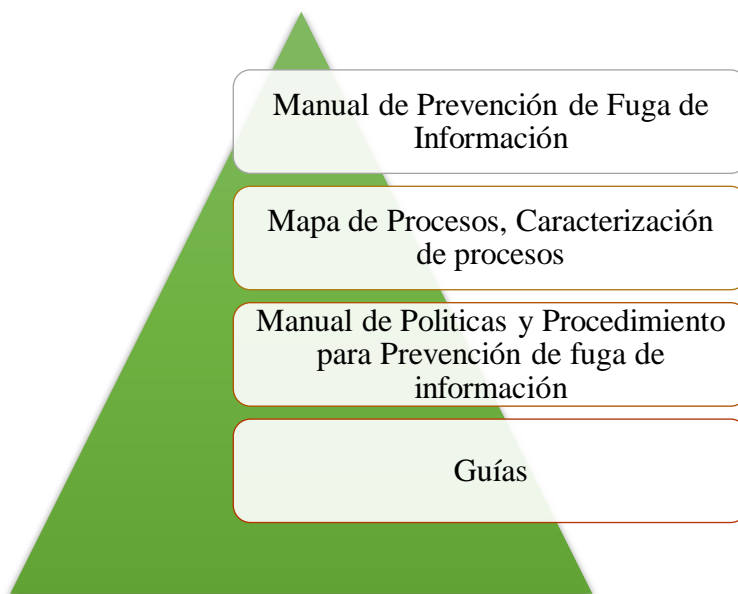
MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información

Figura 34.

Estructura documental de SGP del procedimiento de recuperación operativa




Nota: Elaboración propia estructura documental de Sistema Gestión de Procesos

4. Roles, responsabilidades y autoridad de la entidad financiera COAC “Santa Anita Ltda.”

La Alta Dirección será responsable de designar al encargado del PFI, quien tendrá la autoridad y la responsabilidad de:

- Garantizar que el Manual de Prevención de Fuga de Información, relacionado con el procedimiento de Recuperación Operativa de la entidad financiera COAC "Santa Anita Ltda.", cumple con los requisitos establecidos en la Norma ISO/IEC 27002:2022.
- Garantizar que los procedimientos se implementen de acuerdo con sus funciones y características.


MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información
		Versión:01
		Página: 2 de 23

- Informar a la Alta Dirección sobre el desempeño y funcionamiento del Manual de Prevención de Fuga de Información, y sugerir posibles acciones para mejorar su eficiencia y efectividad en caso de ser necesario.
- El responsable del PFI tendrá la función de coordinar la realización de auditorías internas al Manual de Prevención de Fuga de Información.
- El responsable del PFI se encargará de revisar los documentos que deben formar parte del Manual de Prevención de Fuga de Información y presentarlos a la Alta Dirección.
- El responsable del PFI llevará a cabo todas las funciones relacionadas con la administración, control y seguimiento del Manual de Prevención de Fuga de Información.

5. Requerimientos de la Ley Orgánica de Protección de Datos Personales

Dentro de esta metodología, se ha optado por adherirse a la legislación de protección de datos personales, la cual proporciona un marco que permite a las instituciones y empresas privadas cuyo enfoque principal son los datos (bases de datos) establecer criterios claros para determinar qué medidas tecnológicas y organizativas deben implementar. El propósito fundamental de esto es garantizar que los datos que manejan estén debidamente resguardados y utilizados de manera adecuada.

Según la (Ley Orgánica de Protección de datos personales, 2021), específicamente en su capítulo IV, titulado "Seguridad de Datos Personales," en el artículo 37, se establece que el responsable o encargado del tratamiento de datos personales, según corresponda, debe cumplir con el principio de seguridad de datos personales. Esto implica considerar diversas variables, como las categorías y el volumen de datos personales, el estado de la tecnología, las mejores prácticas de

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01	
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas	Versión:01
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información	
		Página: 2 de 23	

seguridad integral y los costos de implementación, teniendo en cuenta la naturaleza, alcance, contexto y propósitos del tratamiento, así como la identificación de posibles riesgos.


El Artículo 40 de la ley se refiere al análisis de riesgos, amenazas y vulnerabilidades. En este proceso, el responsable y el encargado del tratamiento de datos personales deben utilizar una metodología que tome en cuenta las particularidades del tratamiento, las partes involucradas y las categorías y el volumen de datos personales objeto de tratamiento.

Finalmente, el Artículo 41 establece cómo determinar las medidas de seguridad aplicables. Se deben considerar factores como los resultados del análisis de riesgos, la naturaleza de los datos personales, las características de las partes involucradas y los antecedentes relacionados con la protección de datos personales. Esto incluye la prevención de la destrucción, pérdida, alteración, divulgación o acceso no autorizado de los datos personales, ya sea de forma accidental o intencional. También se deben considerar los antecedentes de transferencia, comunicación o acceso no autorizado de estos datos.

6. Requerimientos de la Norma ISO/IEC 27002:2022

La documentación de la norma ISO/IEC 27002:2022 ha sido elaborada por el Comité Técnico Conjunto ISO/IEC JTC 1, especializado en Tecnología de la Información, y el Subcomité SC 27, dedicado a la Seguridad de la Información, Ciberseguridad y Protección de la Privacidad.

En la tercera edición de la norma ISO/IEC 27002, se han llevado a cabo varios cambios significativos. Estos cambios incluyen una nueva estructura del documento, donde los controles se presentan mediante una taxonomía simple y atributos asociados. Además, se han incorporado controles importantes para fortalecer la seguridad de la información.

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01	
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas	Versión:01
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información	

6.1.Requerimientos de seguridad de la información


Conforme a la norma ISO/IEC 27002:2022, es fundamental que una organización identifique y establezca sus requisitos de seguridad de la información. Estos requisitos pueden originarse de tres fuentes principales:

- a) La evaluación de riesgos de la organización, considerando su estrategia y objetivos generales. Esto puede incluir una evaluación específica de riesgos relacionada con la seguridad de la información. Como resultado, se deben determinar los controles necesarios para garantizar que el riesgo residual cumpla con los criterios de aceptación del riesgo establecidos por la organización.
- b) Los requisitos legales, estatutarios, reglamentarios y contractuales que afectan a la organización, así como su entorno sociocultural.
- c) El conjunto de principios, objetivos y requisitos empresariales que la organización ha desarrollado para respaldar todas las etapas del ciclo de vida de la información y que apoyan sus operaciones.

6.2.Control 5.12: Clasificación de la información

En la clasificación de la información de los activos de la entidad financiera, se hace uso de la Tabla 1 de atributos proporcionada por la normativa como punto de referencia. En esta tabla, se clasificarán los activos según sus características, las cuales están definidas de la siguiente manera:

- **Tipo de control:** Según la norma ISO/IEC 27002, la clasificación de la información se refiere a un control preventivo que es esencial en el procedimiento y está diseñado específicamente para evitar la ocurrencia de incidentes de seguridad de la información.


MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN			Código: SGP-MPFI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas	Versión:01
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información	

- **Propiedades de la seguridad de la información:** En relación con los atributos establecidos en la clasificación de confidencialidad, integridad y disponibilidad, que se detallan en el Anexo D, se determinan de acuerdo con el nivel de criticidad asignado a cada característica.
- **Conceptos Ciberseguridad:** Este procedimiento se lleva a cabo con el propósito de identificar los activos de la información, asignando a cada uno de ellos el atributo determinado según su clasificación.
- **Capacidades Operativas:** Este atributo hace referencia a las capacidades operativas de una organización o entidad, englobando sus habilidades, competencias y recursos esenciales para llevar a cabo de forma eficaz y eficiente sus actividades y operaciones. En este procedimiento, una de las capacidades destacadas es la protección de la información.
- **Dominios de Seguridad:** En este procedimiento, se abordan áreas específicas que engloban diversos aspectos de la seguridad de la información, donde se determinan los controles teniendo en cuenta las habilidades necesarias para su efectiva implementación. Estas áreas se enfocan en garantizar la protección adecuada de la información y sus activos, considerando distintos aspectos relacionados con la seguridad.

Tabla 16.

Atributos de la clasificación de la información


Tipo de control	Propiedades de seguridad de la información	Conceptos Ciberseguridad	Capacidades Operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identidad	#Proteccion_Información	#Protección #Defensa

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01	
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas	Versión:01
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información	
		Página: 2 de 23	

6.3.Control 8.12: Prevención de fuga de datos

El control 8.12, según la norma ISO/IEC 27002:2022, tiene como objetivo implementar medidas de seguridad que eviten la fuga de información desde dispositivos finales que almacenan y transmiten datos confidenciales. Su propósito es identificar y evitar accesos no autorizados y divulgaciones indebidas. La Tabla 2 describe los atributos de los activos de información involucrados en la prevención de fuga, detallando su función en el proceso.

- **Tipo de control:** El atributo que se examinará tanto como medida preventiva como detectiva está relacionado con este procedimiento y se activa después de que ha ocurrido un incidente de seguridad de la información.
- **Propiedades de seguridad de la información:** Los atributos establecidos en la clasificación de información, que se encuentran detallados en el Anexo D, se determinan en función del nivel de criticidad asignado a cada característica, y se clasifican los activos de información como confidenciales.
- **Conceptos Ciberseguridad:** Este atributo se determina de acuerdo con el control, siendo designado como preventivo y detectivo, y se describen dentro del contexto de ciberseguridad.
- **Capacidades operativas:** Este atributo, al igual que el control 5.12, se refiere a las capacidades operativas de una organización o entidad, abarcando aspectos tanto técnicos como organizativos, y desempeñan un papel fundamental en el cumplimiento de los objetivos establecidos por la entidad.

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN			Código: SGP-MPFI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas	Versión:01
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información	

- **Dominios de seguridad:** Este atributo puede abarcar categorías clave que deben ser consideradas para establecer un entorno seguro y proteger la confidencialidad de la información de cada uno de los activos descritos.

Tabla 17.

Atributos de Prevención de fuga de datos


Tipo de control	Propiedades de seguridad de la información	Conceptos Cyberseguridad	Capacidades Operativas	Dominios de seguridad
#Preventivo	#Confidencialidad	#Protector	#Protección_información	#Protección
#Detectivo		#Detector		#Defensa

Nota. Elaborado a partir de (ISO/IEC 27002, 2022b).

7. Modelo de Operación

El Manual de Prevención de Fuga de Información ha sido desarrollado aplicando el enfoque PDCA (Plan-Do-Check-Act), que involucra las etapas de Planificar, Hacer, Verificar y Actuar, con el objetivo de lograr una mejora continua en la estructura y planificación de la seguridad de la información.


- **Planificar (Plan):** El proceso consiste en definir los objetivos y procedimientos necesarios en la entidad financiera COAC "Santa Anita Ltda." para alcanzarlos. Esto implica listar o actualizar los activos de información del procedimiento de Recuperación Operativa utilizando la metodología Magerit como guía. Además, se identifican las amenazas y vulnerabilidades para realizar el Análisis de Riesgos de los activos. Con base en este análisis, se determina cómo se llevan a cabo los procesos internos de seguridad y se establece el Tratamiento de los Riesgos para mitigarlos adecuadamente.

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01	
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas	Versión:01
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información	
		Página: 2 de 23	


- **Hacer (Do):** En esta sección, se establecen los planes para la elaboración y redacción del Manual de Prevención de Fuga de Información, así como para realizar las actualizaciones o modificaciones de la Política de Seguridad de la Información. Estos planes proporcionan la justificación necesaria para la elaboración de las normativas, procedimientos y estándares que formarán parte del Manual de Prevención de Fuga de Información. Como resultado de esta fase de planificación, se obtiene una lista de la documentación que será elaborada como parte del Sistema de Gestión de Seguridad de la Información.
- **Verificar (Check):** Los mecanismos de análisis utilizados en la fase de verificación tienen como objetivo comprobar el cumplimiento de lo establecido en la Política de Seguridad de la Información y demás documentación relacionada con la Prevención de Fuga de Información. Durante esta etapa, se establecen lineamientos para el control y la recopilación de información, lo que facilita la toma de decisiones para implementar mejoras.
- **Actuar (Act):** El análisis y la implementación de mejoras en la documentación se llevan a cabo para corregir procesos débiles o insuficientes, elaborar nuevas políticas de seguridad en respuesta a cambios tecnológicos o modificaciones que afecten los servicios o activos de información. También puede implicar la revisión y ratificación de la documentación existente.

7.1.FASE 1: Planificar

Objetivo: Realizar el análisis y gestión de riesgos aplicando la metodología Magerit, con el objetivo de determinar la situación actual de la Seguridad de la Información de los activos de información.

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01	
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas	Versión:01
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información	

REGISTROS	ACTIVIDADES
Inventario de activos de información	De acuerdo con los lineamientos establecidos en la Metodología Magerit, se requiere llevar a cabo la elaboración de un inventario detallado y actualizado de los activos de información de seguridad de la entidad financiera COAC "Santa Anita Ltda." (Ver Anexo E).
Clasificación de los activos de la información	En conformidad con las directrices proporcionadas por la metodología Magerit (ver Anexo D), se debe determinar el tipo de activo correspondiente a cada uno de los activos de información, considerando el nivel de criticidad de sus propiedades, como Confidencialidad, Integridad, Disponibilidad y Autenticidad
Reconocer amenazas	Es necesario realizar la identificación de las amenazas a los activos de información, lo que implica reconocer y clasificar las diversas vulnerabilidades que podrían afectar la seguridad de la información. Este proceso se encuentra detallado en el Anexo F del documento.
Análisis de Riesgo	Con base en la identificación de amenazas, se lleva a cabo un análisis que busca determinar la probabilidad y el impacto que dichas amenazas podrían tener sobre los activos de información. Este análisis se encuentra detallado en el Anexo G del documento.
Tratamiento de Riesgo	El tratamiento de riesgo en Magerit se enfoca en la implementación de acciones y controles para reducir o mitigar los riesgos identificados. Esta fase se puede consultar en el apartado 4.3.10 del documento, donde se

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información


determinan las salvaguardas de los activos de la información. Estas salvaguardas son medidas establecidas con el propósito de disminuir los riesgos y proteger adecuadamente los activos de información.

7.2.FASE 2: Hacer

Objetivo: Elaborar la documentación sobre la prevención de fuga de información, con el fin de establecer su adecuada gestión.

Las actividades establecidas en esta sección se determinan en el manual de Políticas y procedimientos de prevención de fuga de información.

REGISTROS	ACTIVIDADES
Desarrollar/Actualizar/Modificar la Política de Prevención de la Información.	Actualizar la Política de Seguridad de la Información, la cual requiere la aprobación de las autoridades pertinentes y su posterior difusión en la entidad financiera COAC “Santa Anita Ltda.”
Procedimiento de Clasificación de la información	Determinar y asignar el nivel correspondiente a cada activo de información, teniendo en cuenta los niveles de confidencialidad, disponibilidad e integridad.
Procedimiento de Etiquetado de la Información	Consiste en asignar etiquetas o marcas específicas a los activos de información de la entidad con el fin de identificar y clasificar adecuadamente la naturaleza

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01	
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas	Versión:01
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información	


y el nivel de seguridad de la información que contienen. Estas etiquetas permiten una fácil identificación de los niveles de confidencialidad, integridad y disponibilidad asociados a cada activo, lo que facilita la aplicación de controles y restricciones de acceso apropiados para garantizar la protección y seguridad de la información en la entidad.

Procedimiento de Prevención de Fuga de información

Se implementan controles para prevenir la divulgación no autorizada de información confidencial o sensible, mediante la aplicación de directrices y acciones específicas que garantizan la protección de la confidencialidad, integridad y disponibilidad de los activos de información.

7.3.FASE 3: Verificar


Objetivo: El proceso de verificación para la prevención de fuga de información consiste en evaluar y comprobar la efectividad de los controles y medidas implementados. El objetivo es asegurarse de que estos controles funcionen adecuadamente y cumplan con los requisitos establecidos para proteger la información de divulgaciones no autorizadas.

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01	
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas	Versión:01
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información	
PÁGINA: 2 DE 23			

Registro	Actividades
Monitoreo de la prevención de fuga de información	<p>Realización de auditorías relacionadas con el modelo de seguridad, así como temas normativos y de cumplimiento de seguridad, con el propósito de verificar y evaluar su correcta implementación y cumplimiento de la información aplicables al procedimiento de Recuperación Operativa.</p> <p>Monitoreo constante de los controles de seguridad.</p> <p>Evaluar la viabilidad de adquirir soluciones de monitoreo para detectar posibles fugas de información en dispositivos finales.</p>

7.4.FASE 4: Plan de Contingencia

Objetivo: El propósito es recopilar los resultados obtenidos de la evaluación de rendimiento con el objetivo de mejorar el plan de contingencia de seguridad y privacidad de la información. Esto facilitará la implementación de las acciones correctivas identificadas, enfocándose en los controles de prevención de fuga de información. Además, es importante destacar que la entidad financiera podría aprovechar el manual de Data Loss Prevention como parte integral del plan de contingencia.

MANUAL DE PREVENCIÓN DE FUGA DE INFORMACIÓN		Código: SGP-MPFI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas
	PROCEDIMIENTO	Manual De Prevención De Fuga De Información
		Versión:01
		Página: 2 de 23

Documentación

Actividades

Manual Data Loss Prevention

Implementar mejoras en la seguridad y privacidad de la información, lo que facilitará la creación del manual de Data Loss Prevention con las acciones preventivas para la entidad financiera.

Se actualizará el Manual de Políticas de Seguridad de la Información cada vez que ocurran cambios significativos.

COOPERATIVA DE AHORRO Y CRÉDITO SANTA ANITA LTDA.


SISTEMA DE GESTIÓN POR PROCESOS



Santa Anita
COOPERATIVA DE AHORRO Y CRÉDITO

MANUAL DE POLITICAS Y PROCEDIMIENTO DE PREVENCIÓN DE SEGURIDAD DE LA INFORMACION SGP-MPPSI-01

MARIA JOSE CAUJA ALTAMIRANO

MANUAL DE POLITICAS Y PROCEDIMIENTO DE PREVENCIÓN DE FUGA DE INFORMACION		Código: SGP-MPPSI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas
	PROCEDIMIENTO	Manual De Políticas Y Procedimiento De Seguridad De La Información
		Versión: 1 Página: 2 de

SISTEMA DE GESTIÓN DE PROCESOS


MANUAL DE POLITICAS Y PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACION

Control de documentación

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre:	María José Cauja	Ing. Marlon Cevallos	Ing. Diamela Gallegos
Cargo:	Tesista	Oficial de seguridad	Gerencia
Firma:			
Fecha:	1 de agosto de 2023	26 de Enero de 2024	26 de Enero de 2024

Control de Edición del documento

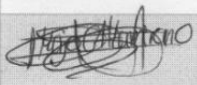
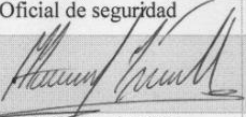
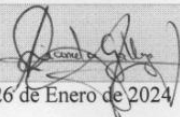
Nombre del Documento:	Manual de Políticas y Procedimiento de Seguridad de la Información	
Código del Documento	SGP-MPPSI-01	
Edición	01	
Fecha de Edición	01 de agosto de 2023	
Responsable de Edición	María José Cauja	
Cargo	Tesista	
Cambios Realizados	Autor de Edición	Fechas de Ediciones

MANUAL DE POLITICAS Y PROCEDIMIENTO DE PREVENCIÓN DE FUGA DE INFORMACION		Código: SGP-MPPSI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas
	PROCEDIMIENTO	Manual De Políticas Y Procedimiento De Seguridad De La Información
		Versión: Página: 2 de

SISTEMA DE GESTIÓN DE PROCESOS

MANUAL DE POLÍTICAS Y PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN

Control de documentación

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre:	María José Cauja	Ing. Marlon Cevallos	Ing. Diamela Gallegos
Cargo:	Tesista	Oficial de seguridad	Gerencia
Firma:			
Fecha:	1 de agosto de 2023	26 de Enero de 2024	26 de Enero de 2024

Control de Edición del documento

Nombre del Documento:	Manual de Políticas y Procedimiento de Seguridad de la Información	
Código del Documento	SGP-MPPSI-01	
Edición	01	
Fecha de Edición	01 de agosto de 2023	
Responsable de Edición	María José Cauja	
Cargo	Tesista	
Cambios Realizados	Autor de Edición	Fechas de Ediciones




MANUAL DE POLITICAS Y PROCEDIMIENTO DE PREVENCIÓN DE FUGA DE INFORMACION		Código: SGP-MPPSI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas
	PROCEDIMIENTO	Manual De Políticas Y Procedimiento De Seguridad De La Información
		Versión: Página: 2 de

Tabla de contenido

Control de documentación	1
Control de Edición del documento	1
1. Introducción	5
2. Objetivo.....	5
3. Alcance	6
4. Vigencia	6
5. Responsables.....	6
6. Referencia	7
7. Términos y Definiciones.....	8
8. Desarrollo de Políticas y Procedimientos de seguridad.....	9
8.1. Política Clasificación de la información- ISO/IEC 27022:2022- Control 5.1210	
8.1.1. Control Ficha de políticas	10
8.1.2. Objetivo.....	¡Error! Marcador no definido.
8.1.3. Alcance.....	11
8.1.5. Procedimiento.....	11
8.1.6. Disposiciones Finales	12
8.1.7. Control de Documentación.....	12
8.2. Política Prevención Fuga de información- ISO/IEC 27022:2022- Control 8.12	
12	
8.2.1. Control Ficha de políticas	13

MANUAL DE POLITICAS Y PROCEDIMIENTO DE PREVENCIÓN DE FUGA DE INFORMACION		Código: SGP-MPPSI- 01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas
	PROCEDIMIENTO	Manual De Políticas Y Procedimiento De Seguridad De La Información

8.2.2.	Objetivo	¡Error! Marcador no definido.
8.2.3.	Alcance	13
8.2.5.	Procedimiento.....	14
8.2.6.	Disposiciones Finales	15
8.2.7.	Control de Documentación.....	15

MANUAL DE POLITICAS Y PROCEDIMIENTO DE PREVENCIÓN DE FUGA DE INFORMACION		Código: SGP-MPPSI-01	
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas	Versión:
	PROCEDIMIENTO	Manual De Políticas Y Procedimiento De Seguridad De La Información	Página: 2 de

1. Introducción


Las políticas de prevención de fuga de información tienen como objetivo garantizar la seguridad y confidencialidad de los activos de información de la entidad, evitando divulgaciones no autorizadas y asegurando el cumplimiento de los requisitos legales y normativos relacionados con la protección de datos.

Estas políticas abarcarán aspectos como la clasificación de la información según su nivel de confidencialidad, integridad y disponibilidad, así como la identificación y protección de activos de información críticos.

El manual de prevención de fuga de información es un componente esencial para el éxito de estas políticas, proporcionando una guía clara y completa para su implementación y asegurando su correcto funcionamiento en la entidad. Su aplicación adecuada contribuirá significativamente a la seguridad y protección de la información en COAC "Santa Anita Ltda.", fortaleciendo su confianza y credibilidad tanto interna como externamente.

2. Objetivo

Dentro del procedimiento de Recuperación Operativa de COAC "Santa Anita Ltda.", se establecerán políticas y procedimientos orientados a asegurar la seguridad de la información de manera eficaz. Estas políticas y procedimientos serán diseñados a la medida de COAC "Santa Anita Ltda.", considerando sus particularidades y se ajustarán a las normativas y estándares de

MANUAL DE POLITICAS Y PROCEDIMIENTO DE PREVENCIÓN DE FUGA DE INFORMACION		Código: SGP-MPPSI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas
	PROCEDIMIENTO	Manual De Políticas Y Procedimiento De Seguridad De La Información

seguridad relevantes. El objetivo es garantizar un entorno seguro y protegido para la entidad, sus activos y usuarios.

3. Alcance

Este Manual de Políticas y Procedimientos se elaborará siguiendo los procesos internos de recuperación operativa, los cuales son parte integral del macro proceso de Gestión de Crédito y Cobranzas. La creación del manual estará basada en los lineamientos de la norma ISO/IEC 27002:2022 y se ajustará a la normativa institucional vigente en COAC "Santa Anita Ltda."

4. Vigencia

Este documento estará en vigencia a discreción de la entidad financiera, y su aplicación requerirá la aprobación de las autoridades responsables de la administración del procedimiento de recuperación operativa en COAC "Santa Anita Ltda." Además, se establecerá un proceso de revisión y actualización del documento para asegurar su conformidad con las leyes y normativas vigentes.

5. Responsables

De acuerdo con la Tabla 1, los responsables de la administración y gestión del procedimiento de recuperación operativa en la entidad financiera son aquellos encargados de asegurar el cumplimiento de este documento, junto con sus respectivas funciones.


MANUAL DE POLITICAS Y PROCEDIMIENTO DE PREVENCIÓN DE FUGA DE INFORMACION			Código: SGP-MPPSI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas	Versión:
	PROCEDIMIENTO	Manual De Políticas Y Procedimiento De Seguridad De La Información	Página: 2 de

Tabla 18.

Responsables y Funciones

<i>N</i>	<i>Involucrados</i>	<i>Función</i>
1	Asesores de Crédito	Individuo responsable de brindar asesoramiento a los clientes sobre las distintas alternativas de crédito disponibles, y también de apoyarlos en los diversos procedimientos relacionados tanto con el otorgamiento de créditos como con la gestión de cartera.
2	Administrador de Cartera	Es responsable de administrar y supervisar las inversiones y activos de una cartera, con el propósito de cumplir con los objetivos y limitaciones establecidos por los clientes.
3	Analista de Crédito	Su responsabilidad es analizar y evaluar la información financiera de los solicitantes, tanto internos como externos.
5	Responsable de tecnología	El responsable de tecnología es la persona encargada de supervisar la parte tecnológica y sistemas de información en la entidad financiera.

6. Referencia


Este documento se elaborará siguiendo las pautas de la norma ISO/IEC 27002:2022, que servirá como referencia para establecer las políticas, objetivos de control y controles necesarios. Se prestará especial atención a los siguientes controles específicos presentados en la mencionada norma:

5. Controles Organizacionales

5.12. Clasificación de la información

8. Controles tecnológicos

8.12. Prevención de fugas de datos

MANUAL DE POLITICAS Y PROCEDIMIENTO DE PREVENCIÓN DE FUGA DE INFORMACION		Código: SGP-MPPSI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas
	PROCEDIMIENTO	Manual De Políticas Y Procedimiento De Seguridad De La Información

7. Términos y Definiciones

En el proceso de elaboración del manual de políticas y procedimientos de prevención de fuga de información, se establecerán los términos y sus respectivas definiciones indispensables. Estas definiciones asegurarán una comprensión clara y precisa de los conceptos involucrados, facilitando así la comunicación efectiva entre todas las partes interesadas.

Tabla 19.


Términos y Definiciones

Términos	Definiciones
Manual de prevención de fuga de información	Se refiere a un conjunto de proyectos de seguridad que se llevan a cabo para poner en práctica las políticas de gestión de riesgos. Estos proyectos son implementados con el propósito de hacer efectivas las medidas necesarias para mitigar los riesgos identificados en el proceso de gestión de la seguridad.
Clasificación de la información	Es el proceso mediante el cual se identifica la clasificación de la información según los niveles establecidos en la entidad, garantizando así que reciba la protección correspondiente.
Seguridad de la información	Se definir como aquellos procedimientos, prácticas efectivas y enfoques metodológicos cuyo objetivo es salvaguardar la información y los sistemas de información contra el acceso, uso, divulgación, interrupción, alteración o eliminación no autorizados.(Vega Briceño, 2021)

Política de seguridad de la información	Se establecen con el objetivo de proteger la información, los equipos y los servicios tecnológicos que son fundamentales para la mayoría de los procesos de negocio
Confidencialidad	Característica que asegura que la información esté disponible y sea revelada únicamente a personas, entidades o procesos autorizados.(Ministerio de Tecnologías de la Información y Comunicaciones de COLOMBIA, 2016)
Disponibilidad	Característica que garantiza que la información pueda ser accedida y utilizada por una entidad autorizada cuando lo solicite.(Ministerio de Tecnologías de la Información y Comunicaciones de COLOMBIA, 2016)
Integridad	Característica que asegura la integridad y la plenitud de los activos.(Ministerio de Tecnologías de la Información y Comunicaciones de COLOMBIA, 2016)
Incidencias	Una incidencia se refiere a cualquier suceso que tenga un impacto negativo en una organización, abarcando aspectos como el personal, los productos de la organización, equipos o el entorno en el que desarrolla sus operaciones.(<i>Gestión de Incidencias</i> , 2014)

8. Desarrollo de Políticas y Procedimientos de seguridad

En esta sección, se establecen las políticas y procedimientos de seguridad que se implementarán en la entidad financiera COAC "Santa Anita Ltda." con el objetivo de asegurar la protección contra la fuga de información. Estas normativas y guías están diseñadas para abarcar distintas áreas y proporcionar directrices claras que deben seguirse para mantener un entorno seguro y protegido frente a posibles amenazas y riesgos relacionados con la seguridad de la información.

MANUAL DE POLITICAS Y PROCEDIMIENTO DE PREVENCIÓN DE FUGA DE INFORMACION			Código: SGP-MPPSI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas	Versión:
	PROCEDIMIENTO	Manual De Políticas Y Procedimiento De Seguridad De La Información	Página: 2 de

8.1. Política Clasificación de la información- ISO/IEC 27022:2022- Control 5.12


En esta sección se establecen las orientaciones y los pasos a seguir en la entidad financiera COAC “Santa Anita Ltda.”, tomando en consideración tanto los requisitos de la norma ISO/IEC 27002:2022 como la normativa actual de la organización.

8.1.1. Control Ficha de políticas

Título de Política	Política de Clasificación de la Información
<i>Código de Política</i>	PCI-001
<i>Versión</i>	1.0
<i>Fecha de aprobación</i>	
<i>Fecha de Revisión</i>	
<i>Responsable de aprobación</i>	
<i>Proceso</i>	Gestión de Cartera y Cobranzas
<i>Procedimiento</i>	Recuperación Operativa
<i>Dominio</i>	ISO/IEC 27002:2022 Sección 5. Controles Organizacionales
<i>Control</i>	5.12. Clasificación de la Información

8.1.2. Enunciado de política de clasificación de la información

Garantizar que la información reciba los niveles adecuados de protección, ajustados de acuerdo con sus características específicas y en cumplimiento con los requisitos establecidos en la norma ISO/IEC 27002:2022.

MANUAL DE POLITICAS Y PROCEDIMIENTO DE PREVENCIÓN DE FUGA DE INFORMACION			Código: SGP-MPPSI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas	Versión:
	PROCEDIMIENTO	Manual De Políticas Y Procedimiento De Seguridad De La Información	Página: 2 de

8.1.3. *Alcance*

Esta política se aplica a todos los activos de información de la entidad financiera, abarcando datos, documentos y sistemas que contengan información sensible o confidencial.

8.1.4. *Documentos Relacionados*

- ISO/IEC 27002 Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información.
- Normativa vigente de la entidad financiera COAC “Santa Anita Ltda.”
- Manual de políticas y procedimiento de Administración de Cartera.
- Manual de Seguridad
- Manual de Prevención de fuga de información
- Guía de Elaboración y Gestión de Documentos.

8.1.5. *Procedimiento*

<i>No.</i>	<i>Actividad</i>	<i>Descripción</i>
1	Identificación del inventario de Activos de Información	Se realizará la identificación exhaustiva y detallada de todos los activos de información relevantes para el funcionamiento eficiente de la entidad financiera COAC "Santa Anita Ltda.", considerando su importancia y valor para el procedimiento específico.

2	Matriz de Clasificación de la Información	Se establecerá una matriz de clasificación basada en el Anexo D de la norma ISO/IEC 27002:2022, la cual contendrá los niveles de confidencialidad, integridad y disponibilidad aplicables a cada activo de información
3	Etiquetado y Control de Acceso	Los activos de información que hayan sido clasificados serán adecuadamente etiquetados con su nivel de clasificación para facilitar su identificación. Además, se implementarán controles de acceso adecuados para garantizar que solo las personas autorizadas tengan acceso a la información clasificada.
4	Revisión Periódica	Se establecerá un proceso de revisión periódica para asegurar que la clasificación de la información se mantenga actualizada y refleje los cambios que puedan ocurrir en los activos o en los requerimientos de seguridad.

8.1.6. *Disposiciones Finales*


La actual política será objeto de revisión anualmente o en caso de modificaciones importantes en los activos de información o en los requisitos de seguridad. Cualquier violación de esta política estará sujeta a las consecuencias disciplinarias apropiadas.

8.1.7. *Control de Documentación*

Control de Documentos		
N	Código	Nombre del Documento
1	SGP-GA-01	Guía de elaboración y gestión de documentos
2	SGP-MPFI-01	Manual de Prevención de fuga de información

8.2. Política Prevención Fuga de información- ISO/IEC 27022:2022- Control 8.12

La prevención de la fuga de información se fundamenta en la seguridad de la información, asegurando la confidencialidad, disponibilidad e integridad de los datos, evitando

MANUAL DE POLITICAS Y PROCEDIMIENTO DE PREVENCIÓN DE FUGA DE INFORMACION			Código: SGP-MPPSI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas	Versión:
	PROCEDIMIENTO	Manual De Políticas Y Procedimiento De Seguridad De La Información	Página: 2 de

cualquier acción no autorizada, como su uso, divulgación, alteración, manipulación, investigación o destrucción.

8.2.1. *Control Ficha de políticas*


Título de Política	Política de Prevención de Fuga de Información
<i>Código de Política</i>	PFI-001
<i>Versión</i>	1.0
<i>Fecha de aprobación</i>	
<i>Fecha de Revisión</i>	
<i>Responsable de aprobación</i>	
<i>Proceso</i>	Gestión de Cartera y Cobranzas
<i>Procedimiento</i>	Recuperación Operativa
<i>Dominio</i>	ISO/IEC 27002:2022 Sección 8. Controles Tecnológicos
<i>Control</i>	8.12revención de fuga de información

8.2.2. *Enunciado de política de prevención de fuga de información*

El propósito de esta política es implementar las medidas de seguridad requeridas para evitar la filtración de información desde dispositivos finales que almacenan y transmiten datos confidenciales en la entidad financiera COAC "Santa Anita Ltda."

8.2.3. *Alcance*

Esta política se extiende a los recursos de información pertenecientes a la institución financiera "COAC Santa Anita Ltda.", abarcando datos, documentos y sistemas que alberguen información confidencial o sensible.

MANUAL DE POLITICAS Y PROCEDIMIENTO DE PREVENCIÓN DE FUGA DE INFORMACION			Código: SGP-MPPSI-01
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Gestión de crédito y cobranzas	Versión:
	PROCEDIMIENTO	Manual De Políticas Y Procedimiento De Seguridad De La Información	Página: 2 de

8.2.4. *Documentos Relacionados*

- ISO/IEC 27002 Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información.
- Normativa vigente de la entidad financiera COAC “Santa Anita Ltda.”
- Manual de políticas y procedimiento de Administración de Cartera.
- Manual de Seguridad
- Manual de Prevención de fuga de información
- Guía de Elaboración y Gestión de Documentos.

8.2.5. *Procedimiento*

<i>N.</i>	<i>Actividad</i>	<i>Descripción</i>
1	Clasificación de información	Los activos de información se clasifican según los niveles de confidencialidad definidos en los procedimientos de la política de clasificación de información.
2	Acceso y control de datos	Implementar un sistema que restrinja los activos de información de acuerdo con los roles y niveles de acceso correspondientes a sus funciones respectivas
4	Seguridad dispositivos finales	Una acción crucial para mitigar el riesgo de pérdida de datos consiste en supervisar los medios por los cuales la información podría filtrarse, como el correo electrónico, la transferencia de archivos, dispositivos móviles y unidades de almacenamiento portátiles.
5	Seguridad en base de datos	Evitar que los usuarios realicen acciones o transmitan datos a través de la red que puedan comprometer información confidencial, por ejemplo,

		bloqueando la copia de datos de bases de datos a hojas de cálculo u otras acciones que puedan exponer la información.
6	Monitorear y auditoria	Implementar sistemas de seguimiento para supervisar el acceso y la utilización de información sensible, además de llevar a cabo auditorías regulares para garantizar el cumplimiento de las políticas y detectar posibles fallos en la seguridad.

8.2.6. *Disposiciones Finales*

- Detallar las repercusiones que los empleados enfrentarán en caso de violar la política de prevención de fuga de información. Estas consecuencias pueden abarcar medidas disciplinarias, acciones legales o cualquier otra sanción establecida por la organización.
- Garantizar la confidencialidad y no divulgación de la política como información reservada, prohibiendo su compartición con personas no autorizadas. Además, instar a los empleados a informar sobre cualquier inquietud o sugerencia para mejorar la política.
- Establecer la fecha de aprobación y la fecha de inicio de vigencia de la política. Asimismo, es esencial determinar los métodos de comunicación para que los empleados conozcan la política y asegurar que la comprendan y cumplan adecuadamente.

8.2.7. *Control de Documentación*

Control de Documentos		
N	Código	Nombre del Documento
1	SGP-GA-01	Guía de elaboración y gestión de documentos
2	SGP-MPFI-01	Manual de Prevención de fuga de información

5. CAPITULO V

HERRAMIENTA DATA LOSS PREVENTION

5.1.Requerimientos para la herramienta Data Loss Prevention

A partir de la evaluación realizada en el proyecto y la recopilación de información para implementar políticas de seguridad en una herramienta de prevención de pérdida de datos (DLP), podemos identificar los elementos necesarios que satisfacen las necesidades detectadas. Siguiendo las pautas establecidas por la norma IEEE 29148, se evalúan los requerimientos de Usuario, requerimientos del Sistema y requerimientos de Arquitectura con el objetivo de lograr este propósito.

En la tabla 20 se presenta la nomenclatura que se utilizará para facilitar la comprensión y simplificación de los requisitos principales para el desarrollo del proyecto.

Tabla 20.

Requerimientos

<i>Requerimiento</i>	<i>Nomenclatura</i>
<i>Stakeholder</i>	StSR
<i>Sistema</i>	SySR
<i>Arquitectura</i>	SRSH

5.1.1. Stakeholders

Los Stakeholders serán determinados teniendo en cuenta las necesidades de los usuarios en el entorno específico, quienes participan de manera directa o indirecta en el desarrollo del proyecto y evalúan todas las características que pueden surgir en el mismo. La Tabla 21 presenta la lista de los stakeholders identificados.

Tabla 21.

Abreviatura de Stakeholders

<i>N</i>	<i>Involucrados</i>	<i>Función</i>
1	Usuarios Directos	Asesores de Crédito, Administrador de Cartera y Analista de Crédito
2	Usuarios Indirectos	Abogado
3	Administrador	Responsable de tecnología
4	Director del trabajo de titulación	MSc. Mauricio Domínguez
5	Asesor de trabajo de titulación	MSc. Fabian Cuzme
6	Desarrollador	María José Cauja

5.1.2. *Requerimientos de Stakeholders*

El propósito de emplear los requerimientos de los Stakeholders se vincula con los criterios del sistema, los cuales se fundamentan en una encuesta llevada a cabo en la institución financiera. Cada requerimiento refleja las necesidades y expectativas individuales de cada Stakeholder en relación a la prevención de la fuga de datos y protección de la información confidencial de la organización. En consecuencia, en la tabla 22 se realizará la evaluación de los requerimientos operacionales y de los usuarios.

Tabla 22.

Requerimientos de Stakeholder

StSR (Requerimientos Stakeholder)				
Requerimientos Operacionales				
#	Requerimiento	Prioridad		
		Alta	Media	Baja
StSR1	Es necesario que la plataforma cumpla con las normativas de privacidad y protección de información.	X		

StSR2	La herramienta debe ser compatible con las versiones de sistemas operativos Windows.	X		
StSR3	La herramienta debe poder clasificar y etiquetar datos confidenciales.	X		
StSR4	La plataforma debe contar con características que permitan identificar y evitar la transferencia no autorizada de información confidencial.	X		
StSR5	La herramienta debe generar registros de actividades, incluyendo auditorías de conformidad y revisiones de políticas de seguridad.	X		
Requerimientos de Usuario				
StSR6	La herramienta debe tener una implementación y administración sencillas, como opciones de configuración claras.	X		
StSR7	La herramienta debe ser transparente para los usuarios, sin comprometer su productividad o rendimiento en las tareas.		X	
StSR8	La herramienta debe recibir actualizaciones periódicas, parches de seguridad y contar con un soporte continuo	X		
StSR9	La herramienta debe poder identificar y prevenir la filtración de información.	X		

5.1.3. *Requerimientos del sistema*

En este apartado se consideran los requerimientos del sistema según los Stakeholders, los cuales incluirán requisitos relacionados con el uso, la interfaz, el modo/estado, el rendimiento y los aspectos físicos. Estos requisitos son cruciales para alcanzar un equilibrio entre las diversas necesidades y expectativas, dándole prioridad a aquellos que son más críticos o estratégicos para el éxito del sistema. En la tabla 23, se encuentran detallados los requerimientos del sistema para su visualización.

Tabla 23.

Requerimiento de sistema

StSR (Requerimientos Stakeholder)				
Requerimientos de Interfaz				
#	Requerimiento	Prioridad		
		Alta	Media	Baja
SySR1	La interfaz debe ser fácil de usar y amigable, permitiendo que los usuarios utilicen la herramienta sin dificultad	X		
SySR2	La interfaz debe mostrar las alertas y eventos relacionados con la detección de pérdida de datos.	X		
SySR3	Deberá contar con opciones de filtrado y búsqueda para facilitar la ubicación de información en la interfaz.		X	
SySR4	La interfaz debe generar informes y mostrar estadísticas detalladas sobre los incidentes de pérdida de datos y las medidas de prevención implementadas.		X	
SySR5	La interfaz debe incluir autenticación para administradores y usuarios que realicen el monitoreo.	X		
Requerimientos de Uso				
SySR6	Debe poder integrarse con los sistemas y aplicaciones existentes en la infraestructura de la entidad financiera.	X		
SySR7	La herramienta debe brindar la opción de crear y personalizar políticas de prevención de pérdida de datos	X		
SySR8	Es necesario que la plataforma permita un acceso y control específico, definiendo quiénes pueden acceder, modificar o compartir dicha información.	X		
SySR9	La herramienta debe tener la capacidad de detectar y monitorear en tiempo real las actividades.		X	
SySR10	La herramienta debe poder enviar notificaciones y alertas personalizables a los usuarios cuando se detecte una fuga de datos.	X		

Requerimientos de Performance				
SySR11	La herramienta debe aprovechar de manera eficiente los recursos del sistema para reducir la carga y garantizar un rendimiento óptimo.	X		
SySR12	La herramienta debe evitar la generación de falsos positivos al detectar posibles fugas de datos de manera eficiente.		X	
SySR13	Debe adaptarse al crecimiento de la organización.	X		
Requerimientos de Modo/Estado				
SySR14	La herramienta debe operar tanto en modo activo como pasivo, dependiendo de las necesidades y preferencias de la organización.	X		
SySR15	En el modo activo, la herramienta aplicará políticas de prevención de pérdida de datos y tomará medidas proactivas.	X		
SySR16	En el modo pasivo, la herramienta solo se limitará a monitorear y generar informes sin tomar acciones preventivas.	X		
SySR17	El modo de configuración y administración de la herramienta debe restringirse solo a usuarios autorizados con acceso privilegiado.	X		
Requerimientos Físico				
SySR18	La herramienta de DLP necesita un hardware adecuado para su operatividad, el cual debe cumplir con los requisitos de capacidad, rendimiento y escalabilidad.	X		
SySR19	Para prevenir el acceso no autorizado a la infraestructura de la herramienta, es necesario implementar medidas de seguridad física, tales como cámaras de vigilancia, controles de acceso, cerraduras y sistemas de alarma.	X		
SySR20	Es necesario ubicar la herramienta en un entorno físico seguro y controlado para prevenir el acceso no autorizado, daños físicos o pérdida de datos.	X		

SySR21	Se requiere un programa de mantenimiento regular y soporte técnico para asegurar el correcto funcionamiento del hardware físico de la herramienta.	X		
--------	--	---	--	--

5.1.4. *Requerimientos de Arquitectura*

La sección de Requerimientos de Arquitectura es fundamental en el desarrollo de software, ya que define las especificaciones y restricciones que orientarán el diseño y la construcción de la herramienta de prevención de pérdida de datos, con el objetivo de satisfacer las necesidades y metas del proyecto. En la tabla 24, se pueden observar los requisitos que abarcan aspectos como el diseño, el hardware, el software y los aspectos eléctricos.

Tabla 24.

Requerimientos de Arquitectura

SRSR (Requerimientos Arquitectura)				
Requerimientos de Hardware				
SRSR5	La herramienta debe tener interfaces de red adecuadas, como puertos Ethernet, para permitir la comunicación entre los dispositivos en la infraestructura de la red.	X		
SRSR6	Se necesitan tarjetas de red con una velocidad mínima de 1GBPS que cumplan con los estándares de conectividad y velocidad para el tráfico de datos.	X		
SRSR7	La herramienta necesita un procesador con capacidad de procesamiento mínimo 2.4GHz para realizar operaciones en tiempo real de detección y prevención de pérdida de datos.	X		
SRSR8	Es necesario contar con una memoria RAM mínimo de 8GB para asegurar un rendimiento óptimo de la herramienta, especialmente al manejar grandes volúmenes de datos.	X		

Requerimientos de Software				
SRSH9	La herramienta debe contar con un navegador web para acceder a su interfaz de administración y configuración, y debe ser compatible con diferentes navegadores.	X		
SRSH10	La herramienta deberá ser compatible con las versiones de Windows	X		
SRSH11	Es necesario contar con conectividad de red para permitir la comunicación con otros sistemas, dispositivos y agentes de seguridad en la red.	X		
SRSH12	Puede ser necesario instalar frameworks o bibliotecas adicionales, como .NET Framework o Java Runtime Environment (JRE).	X		

5.2.Comparativa de Herramientas de análisis

Según los requerimientos esenciales establecidos por la entidad para la elección de la herramienta de prevención de pérdida de datos, se analizaron las distintas características de las herramientas detalladas en la tabla, con el objetivo de seleccionar la más apropiada en concordancia con los requisitos específicos de la entidad financiera.

Tabla 25.

Cuadro comparativo de herramientas Data Loss Prevention

Características	FileCloud DLP	Safetica DLP	ManageEngine Datasecurity Plus
Plataformas compatibles	Enfocado principalmente en Windows y macOS	Enfocado principalmente en Windows	Compatibilidad robusta con Windows, macOS y Linux
Detección de datos confidenciales	Enfocado en la detección, pero puede carecer de	Detección basada en políticas y patrones	Sistema avanzado de detección que emplea análisis de comportamiento y precisión en

	ciertas características de clasificación de información		la detección, con características de clasificación de información.
Control de acceso y políticas	Definición de políticas basadas en roles y jerarquías	Políticas granulares basadas en roles	Establecimiento fácil de políticas mediante una estructura de lista de control de acceso que posibilita la especificación de permisos y restricciones, ofreciendo un control de acceso intuitivo.
Prevención de fuga de datos en tiempo real	SI	SI	Prevención de fuga de datos eficiente dependiendo a la clasificación de información,
Encriptación de datos	Sí (encriptación de datos sensibles)	Sí (encriptación de datos sensibles)	Encriptación sólida de datos sensibles con opciones configuración de políticas
Informes y auditorías	Informes detallados y auditorías	Informes detallados de actividad y auditorías	Informes detallados, auditorías exhaustivas y análisis predictivo, tanto como monitoreo, como para restricciones
Costo	Varía según el plan y las funcionalidades seleccionadas	Dependiendo del plan y del número de usuarios	Escalado flexible, costos competitivos y retorno de inversión rápido.

Nota. Elaborado a partir de las características de las herramientas, las cuales han sido analizadas en comparación con otras herramientas.

5.3.Herramienta ManageEngine DataSecurity Plus

(ManageEngine DataSecurity Plus, 2023), posibilita salvaguardar la red de ataques cibernéticos y amenazas internas. Monitoriza y analiza datos de seguridad generados por

dispositivos en tiempo real, alertándote oportunamente sobre vulnerabilidades, indicadores de compromiso y cualquier actividad sospechosa.

5.3.1. Arquitectura LAN

La arquitectura de red de Data Loss Prevention (DLP) consiste en una combinación de componentes y ajustes diseñados para desplegar y mantener una solución DLP en una red empresarial. Su propósito fundamental es salvaguardar los datos confidenciales y prevenir su filtración, compartición o acceso no autorizado.

En la Figura 35 se presenta un diagrama de arquitectura donde se muestra cómo Endpoint DLP Plus está integrado en los dispositivos finales, lo que le permite desplegar sus funcionalidades con niveles de flexibilidad en diferentes escalas. De esta manera, Endpoint DLP Plus se adapta a los requisitos específicos de cualquier tipo de empresa.

Figura 35.

Arquitectura LAN dispositivos finales



Nota. Elaborado a partir de (*ManageEngine Browser Security Plus*, 2023)

Los responsables de tecnología de la información o los equipos de seguridad de red requieren los siguientes elementos para llevar a cabo la prevención de pérdida de datos (DLP) en los endpoints de su organización:

- **Servidor Endpoint DLP Plus:** Este servidor simplifica la ejecución de las políticas establecidas para Endpoint DLP Plus en la detección y clasificación de datos, además de

fijar los umbrales requeridos para la protección de datos. En este contexto, se detalla en la Tabla 28 los puertos utilizados para la comunicación entre los distintos dispositivos.

Tabla 26.

Puertos de servidor

Puerto	Propósito	Tipo	Conexión
8020	Para la comunicación entre el agente y el servidor Endpoint DLP Plus	HTTP	Vinculado al servidor
8383	Para la comunicación entre el agente y el servidor Endpoint DLP Plus	HTTPS	Vinculado al servidor
8027	Comunicación agente-servidor	TCP	Vinculado al servidor

Nota. Elaborado a partir de (*ManageEngine Browser Security Plus*, 2023)

- **Agente:** es instalado de manera automática en las computadoras de una red local (LAN) y colabora en conjunto con el servidor de Endpoint DLP Plus. Su objetivo es llevar a cabo varias tareas que son iniciadas desde el servidor. Por ejemplo, en situaciones donde es necesario añadir o excluir una aplicación en una lista particular en un conjunto de computadoras dentro de la red, estos ajustes se efectúan en el servidor de Endpoint DLP Plus.
- **Web Console:** Proporciona una ubicación central desde la cual un administrador puede monitorear todas las aplicaciones que están en ejecución en los sistemas bajo su administración.
- **Active Directory:** Dentro de una configuración de dominio fundamentada en Active Directory, el servidor de Endpoint DLP Plus adquiere información proveniente de Active Directory con el fin de producir informes relativos a los siguientes aspectos: Sitios, Dominios, Grupos y Computadoras.

5.3.2. *Detalles de la licencia*

DataSecurity Plus está disponible en una única descarga y ofrece tres ediciones: gratuita, de prueba y profesional. Esto significa que puedes descargar el mismo instalador y luego seleccionar la edición que desees utilizar, ya sea la gratuita, la de prueba o la profesional.

- **Edición Trial**

Al descargar DataSecurity Plus por primera vez, los usuarios tendrán acceso a la edición de prueba completamente funcional durante 30 días. Durante este período, podrán evaluar todas las características y módulos que ofrece el producto. Los usuarios de esta edición también recibirán soporte técnico gratuito de lunes a viernes durante las 24 horas del día.

La versión de prueba de DataSecurity Plus cuenta con las siguientes limitaciones:

- En el módulo de Evaluación de Riesgo de Datos, solo se permite configurar 500GB de datos para el descubrimiento de datos.
- En el módulo de Endpoint DLP, se pueden configurar solo 300 estaciones de trabajo para la auditoría.
- En el módulo de Auditoría de Archivos, solo se pueden configurar 5 servidores para la auditoría.
- En el módulo de Análisis de Archivos, se pueden configurar 5 TB de datos para el análisis.

- **Edición Professional**

La edición Professional con licencia completa de DataSecurity Plus ofrece las siguientes capacidades:

- Realizar auditoría, generar informes y recibir alertas sobre todos los accesos a archivos, modificaciones, movimientos y cambios de permisos en servidores de archivos Windows.

- Analizar datos de auditoría históricos y en tiempo real para proporcionar información sobre las tendencias de acceso a archivos.
- Realizar análisis del almacenamiento de archivos y ofrecer representaciones visuales sobre la propiedad de los archivos, la seguridad de los archivos, el uso del disco, etc.
- Detectar e interrumpir la filtración de archivos confidenciales a través de dispositivos USB y del correo electrónico de Outlook.
- Identificar y clasificar archivos que contengan datos personales (PII/ePHI) almacenados en servidores de archivos Windows y clústeres de conmutación por error.

5.3.3. Cotización de precio de la herramienta ManageEngine

(ManageEngine DataSecurity Plus , 2023) es una solución especializada en seguridad y visibilidad de datos que se enfoca en la prevención de fugas de datos, auditoría de servidores de archivos y descubrimiento de datos. Ofrece seguimiento y alertas para modificaciones y movimientos críticos de archivos entre servidores de archivos, estaciones de trabajo y dispositivos USB. La cotización de la herramienta se determina según sus funciones, que pueden variar dependiendo del número de servidores, estaciones de trabajo, capacidad de análisis de datos, entre otros aspectos.

- **DataSecurity Plus Professional Edition: auditoría de servidores de archivos (suscripción anual)**

La tarifa para la auditoría de servidores de archivos suele estar directamente relacionada con la cantidad de servidores que se analizarán en la arquitectura de red. Esta medida proporciona una base para determinar el alcance del servicio y, por ende, su costo asociado, por lo que se puede evidenciar en la Tabla el valor que proporciona la herramienta

Tabla 27.

Cotización según la auditoría de servidores de archivos

Productos	Tarifa de Licencia
2 File Server	US\$ 745
10 File Server	US\$2.995
20 File Server	US\$ 4.795

Nota. Elaborado a partir de (*ManageEngine DataSecurity Plus Store*, n.d.)

- **DataSecurity Plus Professional Edition: Prevención de fuga de datos (suscripción anual)**

La cantidad de estaciones de trabajo tiene un impacto importante en la complejidad y alcance de la implementación, lo cual incide directamente en el costo del servicio. Por ende, se definen los valores correspondientes en la Tabla para esta característica.

Tabla 28.

Cotización por Prevención de fuga de datos

Productos	Tarifa de Licencia
100 estaciones de trabajo	US\$ 345
500 estaciones de trabajo	US\$ 1.195
1000 estaciones de trabajo	US\$ 2.095

Nota. Elaborado a partir de (*ManageEngine DataSecurity Plus Store*, n.d.)

- **DataSecurity Plus Professional Edition: Evaluación de riesgo de datos (suscripción anual)**

La evaluación de riesgo de datos define la capacidad para analizar información que pueda suponer un riesgo. Este detalle se refleja en la tabla que contiene la cotización para la evaluación de riesgos de datos.

Tabla 29.

Cotización de Evaluación de riesgo de datos

Productos	Tarifa de Licencia
2 TB	US\$ 395
10 TB	US\$ 1.495
20 TB	US\$ 2.295
50 TB	US\$ 4.995

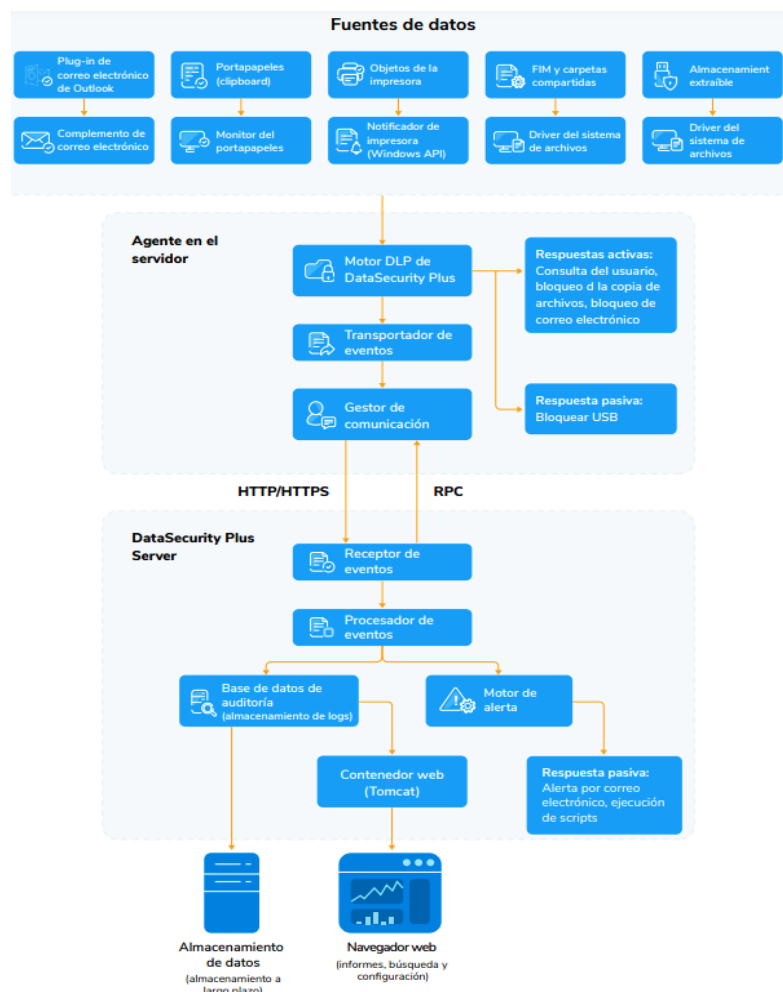
Nota. Elaborado a partir de (*ManageEngine DataSecurity Plus Store*, n.d.)

5.3.4. Módulo de prevención de pérdida de datos

Define una solución completa de ciberseguridad diseñada para salvaguardar la información sensible y evitar su divulgación no autorizada, tal como se ilustra en la Figura 36. En esta representación, se detallan las funciones específicas de los módulos y cómo operan en cada uno de ellos.

Figura 36.

Módulos de prevención de pérdida de datos



Nota. Autoría de (ManageEngine DataSecurity Plus, 2023)

En esta representación, los elementos están organizados de acuerdo con los distintos módulos de prevención de pérdida de datos, que son los siguientes:

- **Motor de alerta:** Con base en las reglas que se hayan establecido, el motor de alertas lleva a cabo respuestas tanto activas, como mostrar notificaciones al usuario o bloquear dispositivos USB, como respuestas pasivas, que abarcan enviar notificaciones por correo electrónico, ejecutar scripts por lotes, eliminar archivos o moverlos a ubicaciones específicas.

- **Base de datos de auditoría:** En DataSecurity Plus se incorpora una base de datos PostgreSQL que guarda los datos de eventos en su forma original y normalizada, provenientes de las fuentes configuradas.
- **Agente DataSecurity Plus:** El software implementa un agente liviano en cada computadora monitoreada. El agente utiliza un controlador de minifiltro de Windows para auditar las actividades de los archivos y la API de Windows para analizar las propiedades de los archivos. También permite a los usuarios finales categorizar archivos manualmente en las computadoras.
- **Motor DLP de DataSecurity Plus:** El motor de prevención de pérdida de datos procesa todos los datos entrantes de las fuentes de datos configuradas y los compara con un repositorio de políticas de DLP, que incluye tanto políticas integradas como aquellas definidas por el usuario.

5.3.5. Manual de configuración herramienta ManageEngine Data Loss Prevention

Este manual tiene como objetivo establecer las configuraciones requeridas para llevar a cabo las políticas delineadas en el apartado 4.4.3 correspondiente a Manual de Procedimientos de Políticas de Seguridad de la Información. Su propósito fundamental radica en brindar una guía detallada y estructurada que facilite a los usuarios y administradores la implementación efectiva de las políticas de seguridad de la información en un entorno tecnológico.

Este manual ofrecerá instrucciones claras y coherentes acerca de cómo configurar y aplicar políticas de DLP. Esto asegurará que los usuarios comprendan de manera completa los pasos necesarios para cumplir con las regulaciones de seguridad específicas de la organización, enfocadas en proteger datos confidenciales y prevenir la fuga de información.

COOPERATIVA DE AHORRO Y CRÉDITO SANTA ANITA LTDA.

SISTEMA DE GESTIÓN POR PROCESOS



Santa Anita
COOPERATIVA DE AHORRO Y CRÉDITO

GUIA DE CONFIGURACIÓN HERRAMIENTA MANAGEENGINE DATA LOSS PREVENTION

SGP-DLP-01

SISTEMA DE GESTIÓN DE PROCESOS

MANUAL GUIA DE CONFIGURACIÓN HERRAMIENTA

MANAGEENGINE DATA LOSS PREVENTION

Control de documentación

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre:	María José Cauja	Ing. Marlon Cevallos	Ing. Diamela Gallegos
Cargo:	Tesista	Oficial de seguridad	Gerencia
Firma:			
Fecha:	5 de enero de 2024	26 de Enero de 2024	26 de Enero de 2024

Ficha de Edición del documento


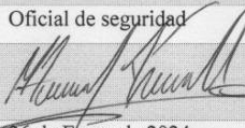
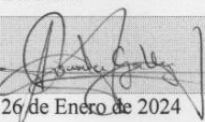
Nombre del Documento:	Guía de Configuración Herramienta Manageengine Data Loss Prevention	
Código del Documento	SGP-HME-01	
Edición	01	
Fecha de Edición	5 de enero de 2024	
Responsable de Edición	María José Cauja	
Cargo	Tesista	
Cambios Realizados	Autor de Edición	Fechas de Ediciones

SISTEMA DE GESTIÓN DE PROCESOS

MANUAL GUÍA DE CONFIGURACIÓN HERRAMIENTA

MANAGEENGINE DATA LOSS PREVENTION

Control de documentación

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre:	María José Cauja	Ing. Marlon Cevallos	Ing. Diamela Gallegos
Cargo:	Tesista	Oficial de seguridad	Gerencia
Firma:			
Fecha:	5 de enero de 2024	26 de Enero de 2024	26 de Enero de 2024

Ficha de Edición del documento

Nombre del Documento:	Guía de Configuración Herramienta Manageengine Data Loss Prevention	
Código del Documento	SGP-HME-01	
Edición	01	
Fecha de Edición	5 de enero de 2024	
Responsable de Edición	María José Cauja	
Cargo	Tesista	
Cambios Realizados	Autor de Edición	Fechas de Ediciones

1. Tabla de contenido

Control de documentación	1
Ficha de Edición del documento	1
1. Introducción	5
2. Objetivo.....	5
3. Alcance	5
4. Herramienta ManageEngine DataSecurity Plus.....	5
4.1. Requisitos de instalación	6
4.1.1. Requisitos de Hardware	6
4.1.2. Requisitos de Software	7
4.1.3. Guía de configuración de puertos	7
4.2. Diagrama de Red.....	9
4.3. Instalación de la herramienta.....	10
4.3.1. Configuración de servidor Windows 2019 como controlador de dominio... ..	10
4.3.2. Configuración de la maquina cliente	13
4.4. Configuraciones de la Herramienta.....	14
4.4.1. Admin Console	14
4.4.2. File Audit	16
4.4.3. File Analysis	18
4.4.4. Risk Analysis	20

	4
4.4.5. Endpoint DLP	23
4.5. Configuraciones según las políticas de prevención de fuga de información	24
4.5.1. Clasificación de información	24
4.5.2. Acceso y control de datos	25
4.5.3. Seguridad dispositivos finales.....	29
4.5.4. Seguridad en base de datos	45
5. Lista de verificación de las acciones de acuerdo con la política de prevención de la fuga de información.	49

2. Introducción

La norma ISO/IEC 27002:2022 ha proporcionado directrices en relación a las mejores prácticas concernientes a evitar la fuga de información. Este manual servirá para configurar la herramienta de Prevención de Pérdida de Datos (DLP) conforme a los controles específicos de prevención de filtración de información, lo cual permitirá prevenir la divulgación de datos confidenciales.

3. Objetivo

Describir las configuraciones aplicados en la herramienta de Data Loss Prevention basados en las directrices establecidas en los manuales elaborados, los cuales se fundamentan en los controles 5.12 y 8.12 de la norma ISO/IEC 27002:2022.

4. Alcance

El propósito de elaborar una guía de configuración dirigida a la herramienta de Prevención de Pérdida de Datos (DLP) consiste en suministrar un conjunto organizado de directrices y sugerencias que faciliten la implementación y el uso eficaz de la herramienta DLP en la institución financiera COAC "Santa Anita Ltda". Esta guía tomará como base las políticas de prevención de filtración de información establecidas en el Manual de prevención de fuga de información, y a través de ella se definirán las configuraciones correspondientes para lograr este objetivo.

5. Herramienta ManageEngine DataSecurity Plus

La plataforma ManageEngine DataSecurity Plus es una herramienta que posibilita la prevención de la filtración de datos, y es de fácil configuración, funcionando en la red. Tiene la capacidad de examinar, vigilar y evitar la pérdida de información. Esta herramienta permite

establecer directrices que definen la detección, supervisión y salvaguardia de información confidencial, sin importar dónde se encuentre almacenada o utilizada.

5.1.Requisitos de instalación

Los requisitos de instalación se utilizan para comprobar las condiciones y especificaciones necesarias para instalar y ejecutar de manera adecuada la herramienta de Prevención de Pérdida de Datos (DLP).

5.1.1. Requisitos de Hardware

Los requisitos mencionados son establecidos por el fabricante del software DataSecurity Plus y contienen las especificaciones de hardware y software necesarias para asegurar el correcto funcionamiento del programa.

Tabla 30.

Requisitos de Hardware

Hardware	Mínimo	Recomendado
Procesador	2.4 GHz	3GHz
Core	4	6 o mas
RAM	8GB	16GB o mas
Espacio de Disco	50GB	100GB*

Los requisitos de hardware para los servidores de (*ManageEngine Browser Security Plus*, 2023), pueden variar según la cantidad de servidores configurados para la auditoría y la evaluación del riesgo de los datos.

Tabla 31.

Servidores Browser Security Plus

Cant. de equipos	Información del procesador	Tamaño de RAM	Espacio en disco duro
1 a 250	Intel Core i3 (2 core/4 thread) 2.0 Ghz 3 MB cache	2 GB	5 GB

251 a 500	Intel Core i3 (2 core/4 thread) 2.4 Ghz 3 MB cache	4 GB	10 GB
1001 a 3000	Intel Core i5 (4 core/4 thread) 2.3 GHz. 6 MB cache	8 GB	30 GB
3001 a 5000	Intel Core i7 (6 core/12 thread) 3.2 GHz. 12 MB cache	8 GB	40 GB

5.1.2. Requisitos de Software

En esta sección, se proporciona información acerca de los requisitos de software para los servidores y agentes de Browser Security Plus.

- **Navegadores:** Internet Explorer 9 y superiores, Mozilla Firefox, Google Chrome (recomendado) y Microsoft Edge.
- **Sistemas operativos:** En esta sección se especifican los sistemas operativos y versiones que son soportados por el software

Windows OS	Windows Server OS
Windows 10	Windows server 2016
Windows 8.1	Windows server 2012 R2
Windows 8	Windows server 2012
Windows 7	Windows server 2008 R2
	Windows server 2008
	Windows server 2003 R2

- **Resolución de pantalla preferida:** 1280 x 800 píxeles o superior.
- **Práctica recomendada:** Le recomendamos que disponga de un ordenador dedicado para instalar DataSecurity Plus

5.1.3. Guía de configuración de puertos

A continuación, se describen los puertos que deben estar abiertos para que DataSecurity Plus funcione correctamente de manera habitual.

- **Puertos del producto**

En la siguiente tabla 3 se enumeran los puertos predeterminados utilizados por DataSecurity Plus. Estos pueden modificarse durante o después de la instalación.

Tabla 32.

Puertos del producto

Puertos	Protocolo	Propósito
8800	HTTP	Comunicación servidor web/agente del producto
9163	HTTPS	Comunicación servidor web/agente del producto

- **Sistemas de Puertos**

En la tabla 4 siguiente se presentan los puertos de los ordenadores de destino que DataSecurity Plus utiliza. Estos puertos pueden ser abiertos en Windows o en cortafuegos de terceros.

Tabla 33.

Sistema de Puertos

Puertos	Protocolo	Destino	Servicio	Objetivo	Dirección
135	TCP	Ordenadores vigilados	RPC	Comunicación con los agentes	Outbound
445	TCP y UDP	Ordenadores vigilados	RPC	Para listar los archivos compartidos	Outbound
389	TCP y UDP	Controladores de dominio	LDAP	Para sincronizar objetos AD con DataSecurity Plus	Outbound
636	TCP	Controladores de dominio	LDAP over SSL	Para sincronizar objetos AD con DataSecurity Plus	Outbound
3269	TCP	Controladores de dominio	Global catalog over SSL	Para sincronizar objetos AD con DataSecurity Plus	Outbound
25	TCP	SMTP servers	SMTP	Para enviar correos electrónicos	Outbound
465	TCP	SMTP servers	SSL	Para enviar correos electrónicos	Outbound

587	TCP	SMTP servers	TLS	Para enviar correos electrónicos	Outbound
49152 - 65535	TCP	Ordenadores vigilados	RPC asigna aleatoriamente puertos TCP elevados	Para la comunicación con los agentes y la configuración del cluster	Outbound

Nota: Para monitorizar el estado del agente DataSecurity Plus, es necesario que los servicios de registro remoto estén activos en todos los equipos que tengan instalado el agente. Si se utiliza el Firewall de Windows, se pueden abrir los puertos dinámicos del 49152 al 65535 en los equipos monitorizados habilitando las siguientes reglas de salida.

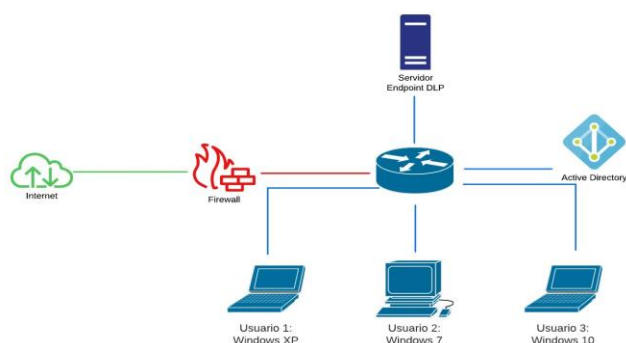
- Gestión remota de registros de eventos (NP-In)
- Gestión remota de registros de sucesos (RPC)

5.2.Diagrama de Red

Para llevar a cabo la instalación, es necesario decidir el método de implementación, el cual se ilustra en la Figura 1. A través de esta implementación, la solución tendrá la capacidad de identificar y prevenir la filtración de datos, lo que nos permitirá establecer cómo se configurará este proceso.

Figura 37.

Implementación de la red



Nota: Elaboración propia basada en la arquitectura de red.

5.3.Instalación de la herramienta

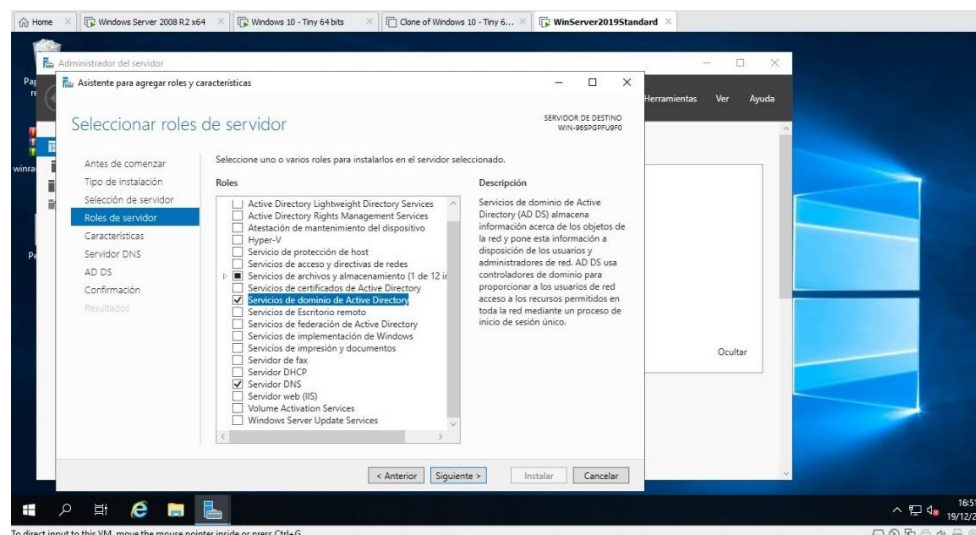
La implementación de Windows Server 2019 con la configuración de servicios de directorio, como Active Directory Domain Services (AD DS), establece los procedimientos para guardar información de directorio y ofrecer acceso a esta información a los usuarios y gestores de la red.

5.3.1. Configuración de servidor Windows 2019 como controlador de dominio

Paso 1: Desde el administrador del servidor abrir el Asistente para agregar características, en la sección de Roles de Servidor seleccionar: Servicios de dominio de Active Directory y Servidor DNS, luego continuar por defecto con el resto de opciones. Como se puede observar en la Figura 2.

Figura 38.

Servicios de dominio de Active Directory

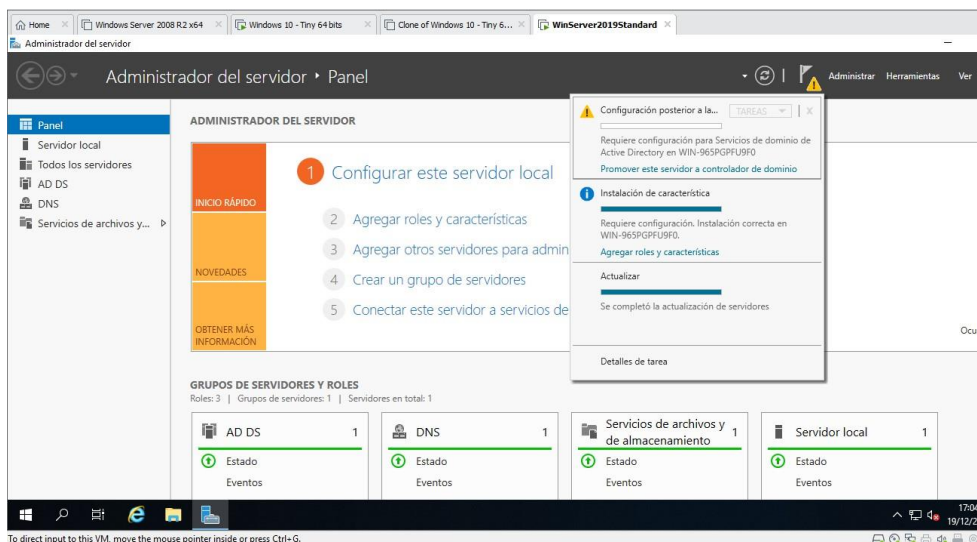


Nota: Elaboración propia basada en las configuraciones del Windows server 2019

Paso 2: Después de completar el paso anterior, el Administrador del servidor mostrará una advertencia; en este punto, seleccionar la opción de Promover el servidor. Se puede observar en la Figura 3.

Figura 39.

Administrador del servidor

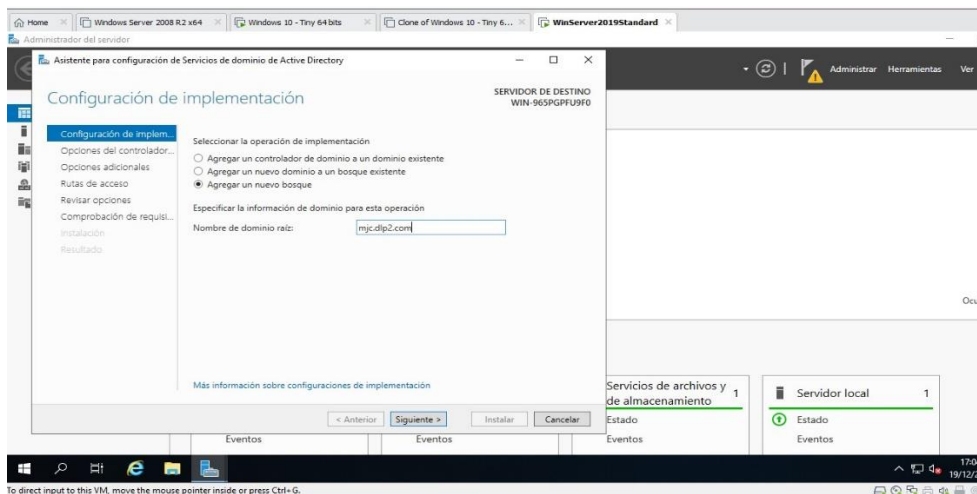


Nota: Elaboración propia basada en las configuraciones del Windows server 2019

Paso 3: En la Figura 4, se puede ver dentro del asistente que se despliega, ingresar el nuevo dominio que manejará el servidor, en este caso será `mjc.dlp2.com`. Luego continuar.

Figura 40.

Agregar un nuevo dominio

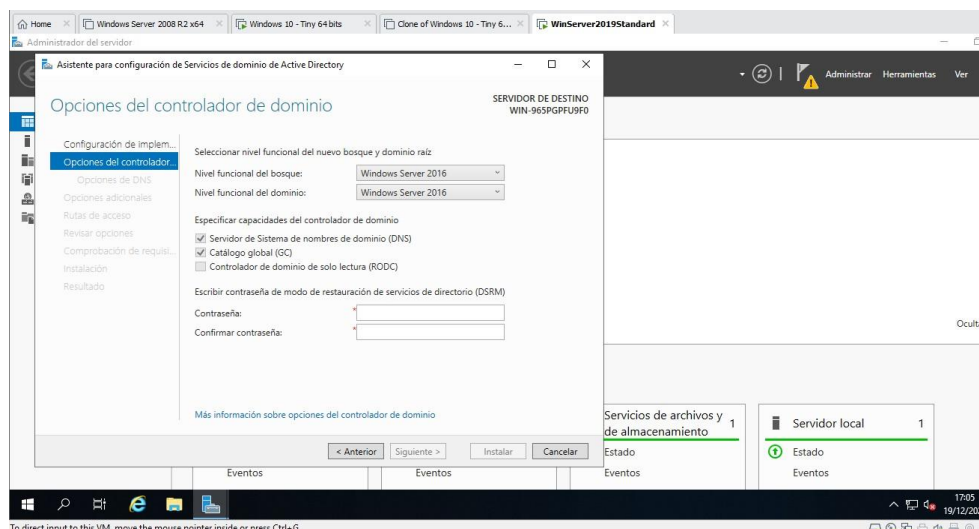


Nota: Elaboración propia basada en las configuraciones del Windows server 2019

Paso 4: Se pedirá una contraseña para restaurar servicios, es la misma del usuario local (123456).

Figura 41.

Agregar contraseña al usuario

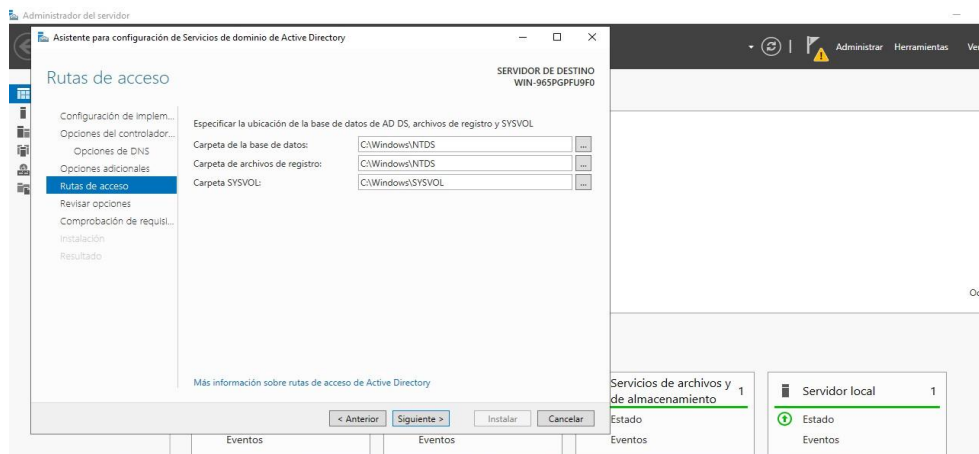


Nota: Elaboración propia basada en las configuraciones del Windows server 2019

Paso 6: En la figura 6, se verifica la configuración de las vías de acceso a la base de datos del Active Directory y otros archivos de registro, asegurando así la posibilidad de realizar registros de acceso.

Figura 42.

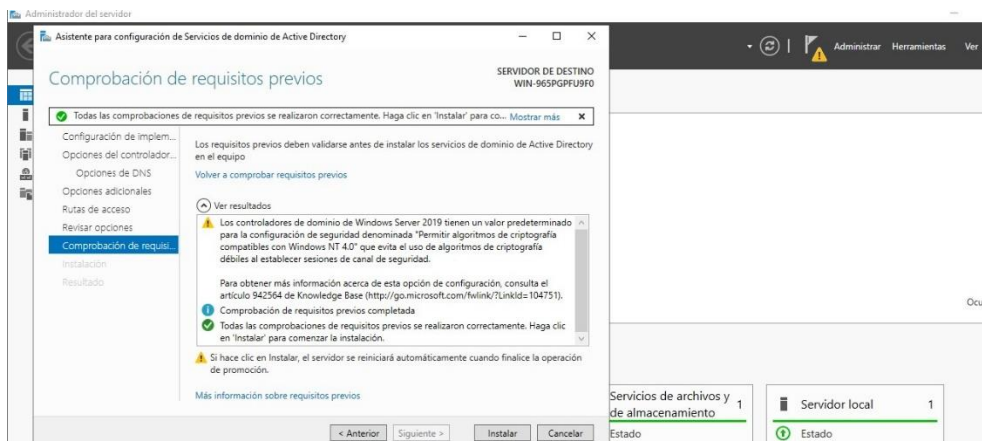
Rutas de Acceso



Nota: Elaboración propia basada en las configuraciones del Windows server 2019

Paso 7: Examinar la figura 7 para confirmar el cumplimiento de los requisitos fundamentales para la instalación; en este contexto, se presentan advertencias informativas que no afectan la continuidad de los servicios.

Figura 43.

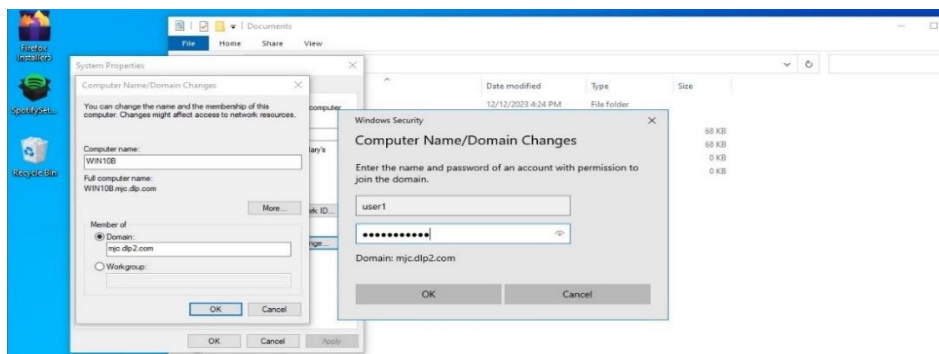
Requisitos previos

Nota: Elaboración propia basada en las configuraciones del Windows server 2019

5.3.2. Configuración de la maquina cliente

Paso 1: La máquina que actuará como cliente es una réplica temprana de la máquina que alberga la herramienta; su configuración DNS se dirige al servidor Windows 2019 y forma parte del nuevo dominio, así como se observa en la Figura 8.

Figura 44.

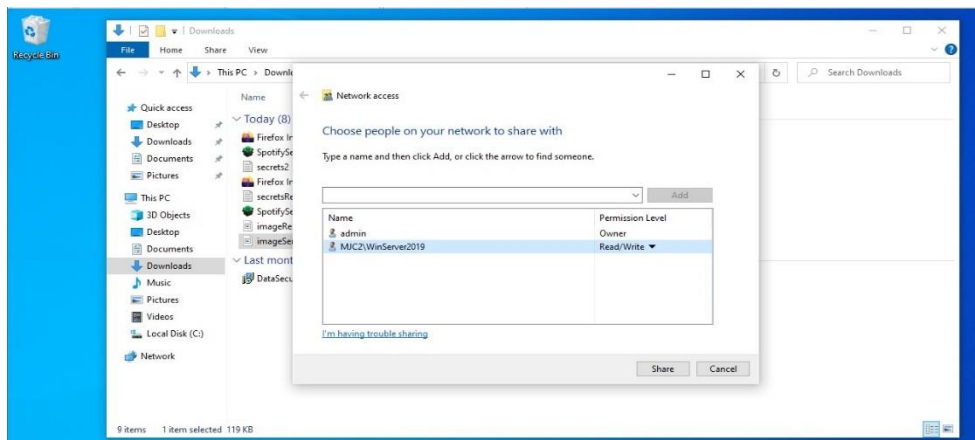
Configuración de dominio de Windows 10

Nota: Elaboración propia basada en configuraciones de Windows 10

Paso 2: Se ha ajustado la configuración de la carpeta de descargas en la máquina cliente para posibilitar el acceso compartido dentro de la red local, tal como se evidencia en la Figura 9.

Figura 45.

Configuración de compartido de la red local



Nota: Elaboración propia basada en configuraciones de Windows 10

5.4. Configuraciones de la Herramienta

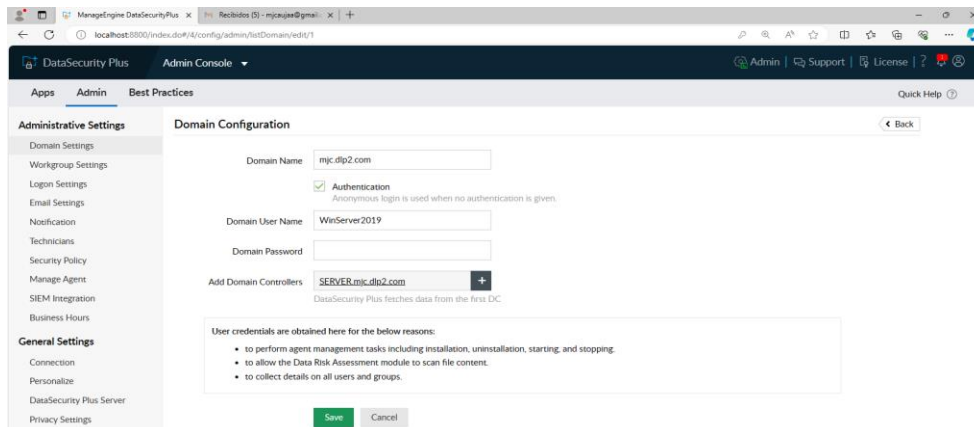
En esta sección, es posible definir las configuraciones fundamentales necesarias para la interconexión de los hosts de administración, servidores y endpoints. Estas configuraciones serán esenciales para asegurar su adecuada comunicación y funcionamiento.

5.4.1. Admin Console

La consola de administración posibilitará llevar a cabo ajustes que habiliten la gestión y control de los diferentes elementos de la herramienta, en la cual se definen las siguientes configuraciones:

Paso 1: Tras finalizar la instalación de las características del controlador de dominio en el servidor, proceda a cambiar a la máquina encargada de administrar la herramienta y agregar el nuevo dominio en la configuración del administrador, como se ilustra en la Figura 10.

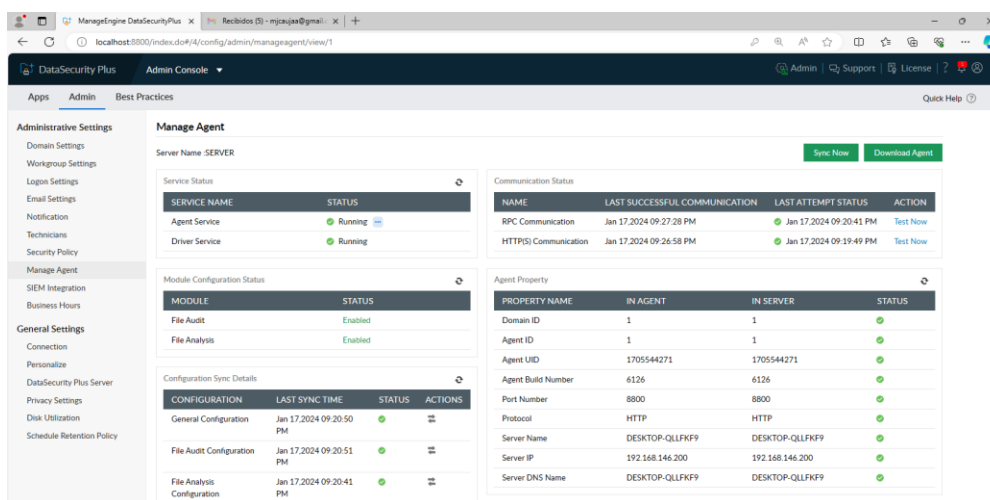
Figura 46.

Configuración de Dominio

Nota: Elaboración propia basada en la experiencia con ManageEngine.

Paso 2: Llevar a cabo la instalación del agente en la máquina del servidor siguiendo el proceso estándar. Luego, comprobar en el panel de agentes que todos los ajustes estén configurados de manera adecuada. En caso de que alguna conexión falle, actualizar la sección correspondiente mediante el ícono de refresco o realizar una sincronización nuevamente desde la parte superior de la ventana, tal y como se muestra en la Figura 11.

Figura 47.

Instalación del agente

Nota: Elaboración propia basada en la experiencia con ManageEngine.

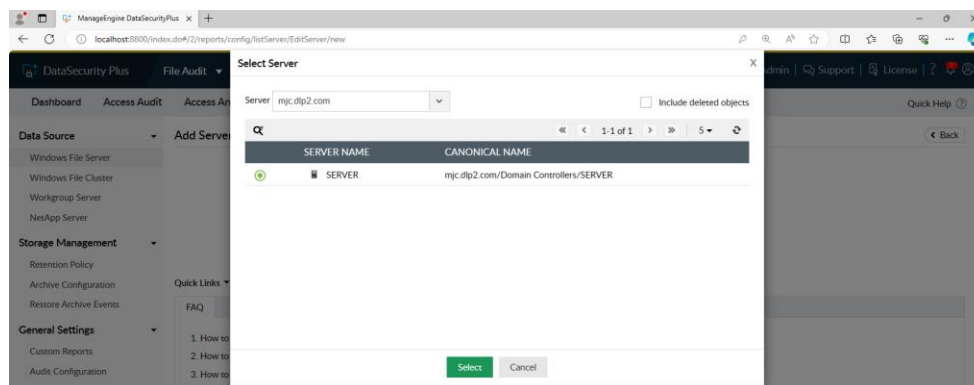
5.4.2. File Audit

Esta funcionalidad se refiere a la auditoría de archivo, que consiste en supervisar y documentar las acciones vinculadas a archivos o documentos almacenados en los servidores. También incluye la identificación de las categorías de datos personales que su organización maneja.

Paso 1: Solamente será necesario hacer clic en el botón "Add Server" o "Click here to configure server" para que este aparezca en el listado, como se puede ver en la Figura 12.

Figura 48.

Agregar servidor SERVER

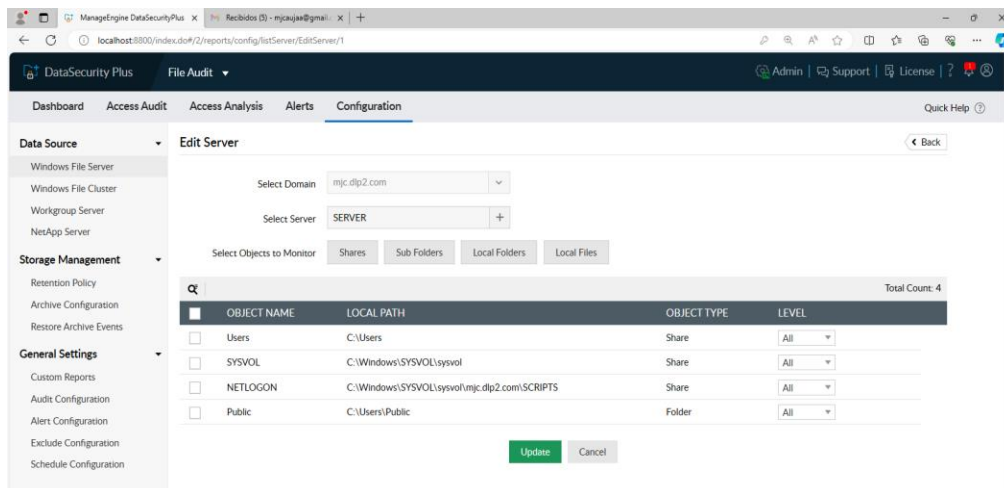


Nota: Elaboración propia basada en la experiencia con ManageEngine.

Paso 2: A continuación, seleccionar los elementos que se desean supervisar en el equipo local, tales como directorios y archivos. Estas elecciones pueden abarcar desde ubicaciones generales hasta carpetas específicas o archivos particulares, según se muestra en la Figura 13.

Figura 49.

Agregar carpetas de análisis

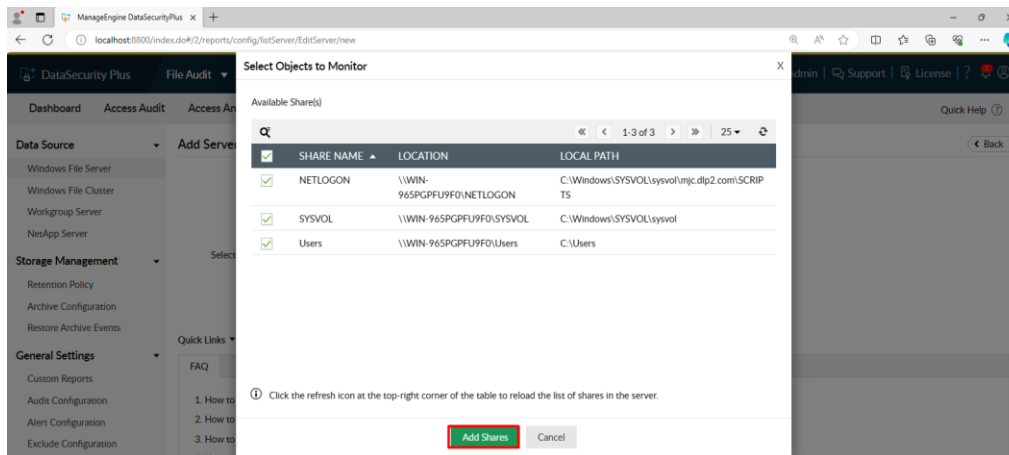


Nota: Elaboración propia basada en la experiencia con ManageEngine.

Paso 3: La Figura 14 muestra cómo se reconocen automáticamente varias de las rutas que pueden ser monitoreadas.

Figura 50.

Rutas automáticas.

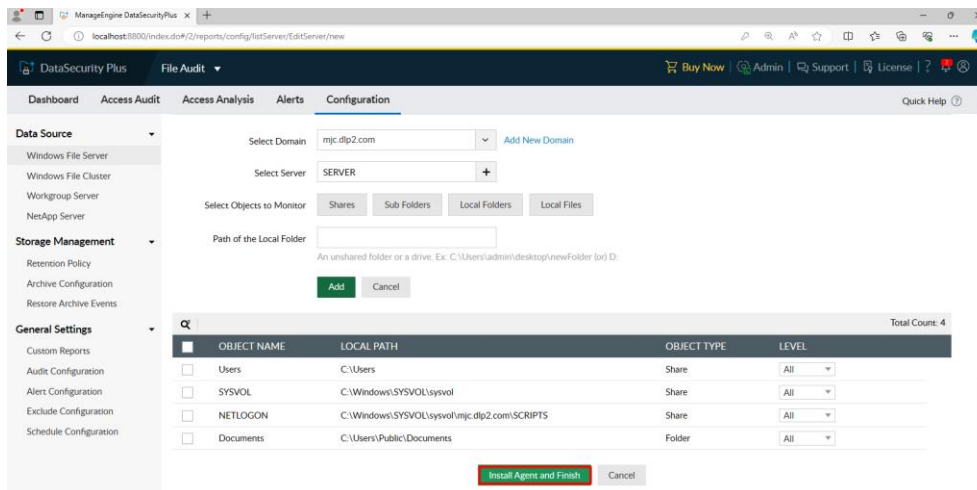


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 4: En la Figura 15, se aprecia que, si el agente ha sido instalado en el servidor, la opción estará disponible.

Figura 51.

Instalar Agente para Archivo de auditoria

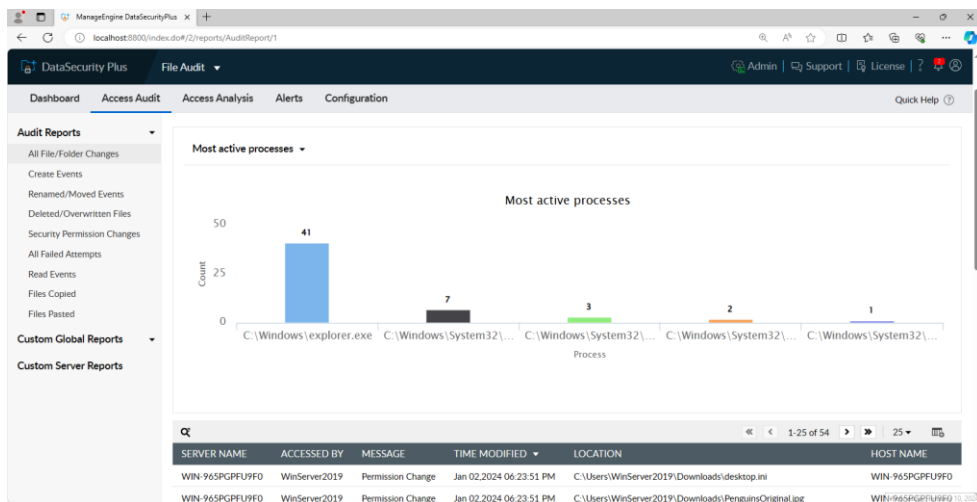


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 5: En la Figura 16, se puede notar cómo la herramienta comenzará a recopilar diversos datos que serán disponibles para su revisión en las distintas secciones de informes.

Figura 52.

Reporte de información



Nota: Elaboración propia basada en la experiencia con ManageEngine

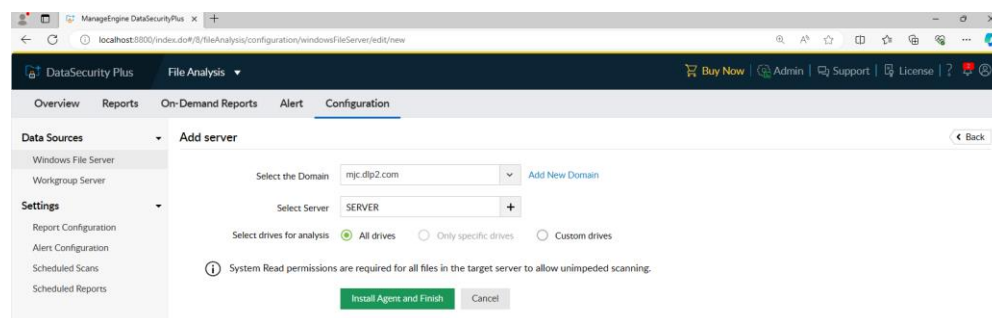
5.4.3. File Analysis

Identifica y administra los datos más vulnerables a las amenazas de seguridad y mejora la postura de seguridad de una entidad financiera.

Paso 1: Para ajustar la configuración en la herramienta de análisis, se requiere proceder a la pestaña de configuración, donde se ingresará el dominio en uso y se elegirá el servidor junto con los discos (unidades) correspondientes, tal como se ilustra en la Figura 17.

Figura 53.

Configuración de archivo de análisis

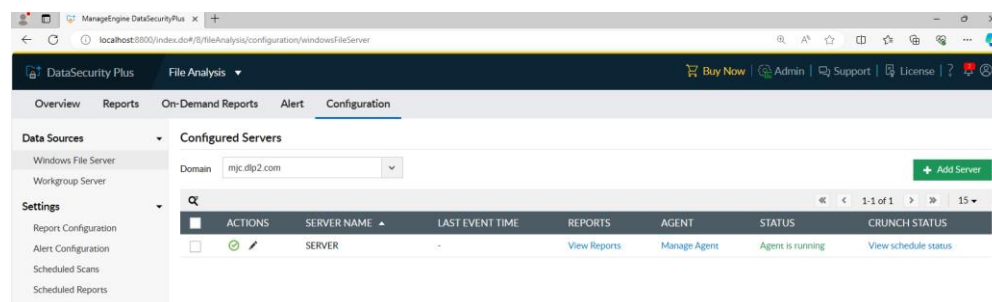


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 2: La Figura 18 brinda la oportunidad de visualizar la incorporación del servidor, además de proporcionar detalles adicionales relacionados con el agente y su conexión.

Figura 54.

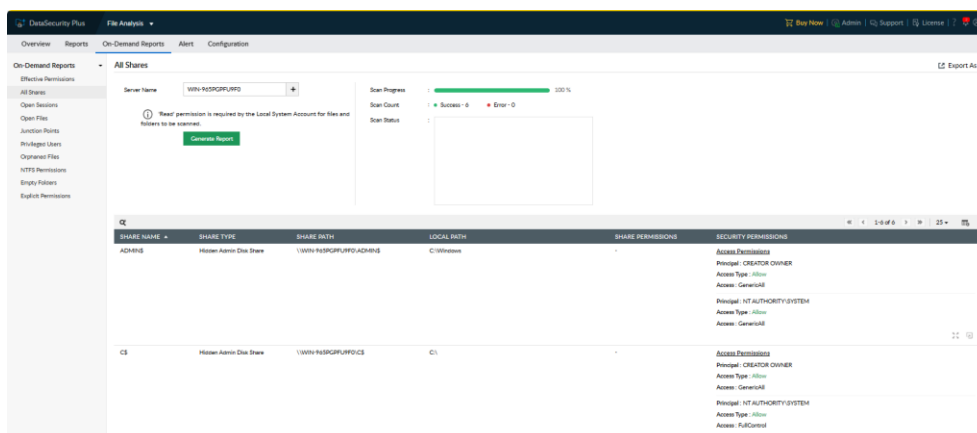
Configuración Windows File Server



Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 3: Luego, se debe seleccionar los informes, algunos de los cuales podrían no generar resultados si no detectan el tamaño de los archivos, mientras que otros funcionarán según lo programado. Esto es especialmente relevante para el informe que abarca todas las carpetas compartidas, como se muestra en la Figura 19.

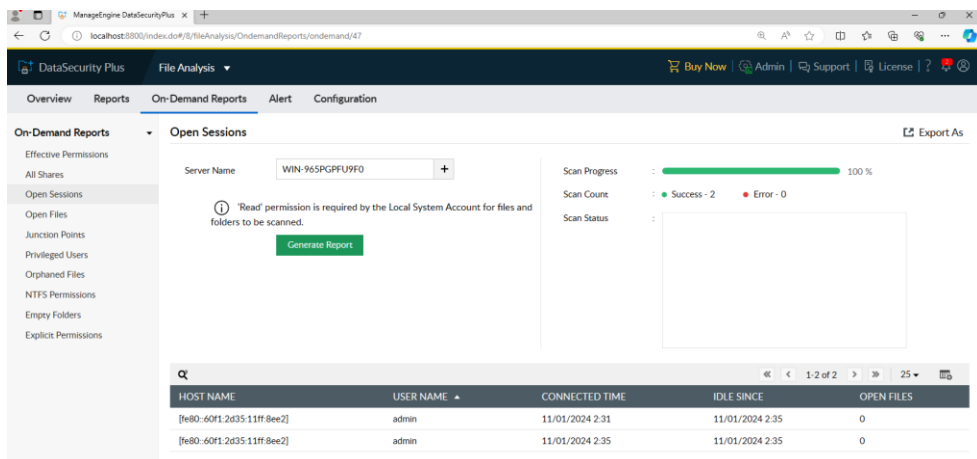
Figura 55.

Análisis On Demand Reports

Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 4: En lo que respecta a la sección de "Open Sessions", posibilita la supervisión de los usuarios que acceden al servidor. Esta funcionalidad se ilustra en la Figura 20, donde se puede observar el ingreso al servidor administrador.

Figura 56.

Monitoreo de ingreso al servidor administrador

Nota: Elaboración propia basada en la experiencia con ManageEngine

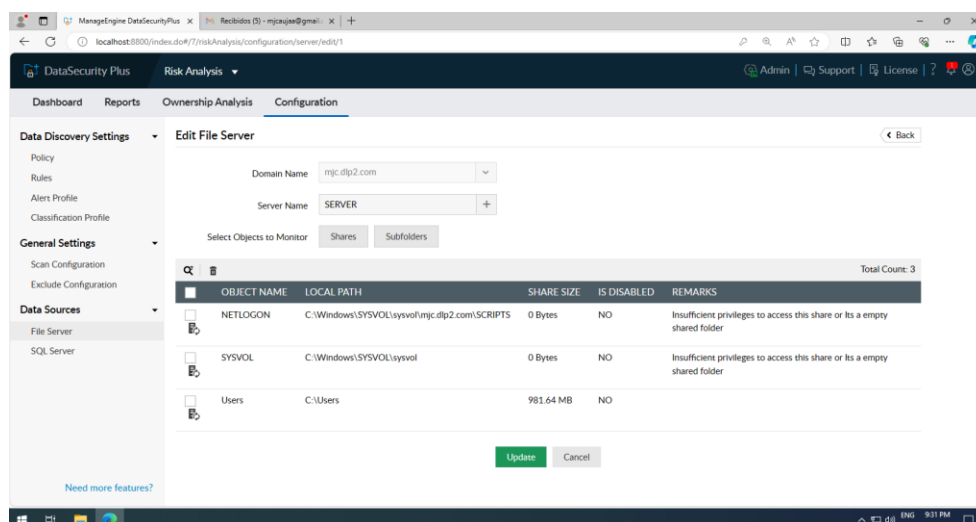
5.4.4. Risk Analysis

El análisis de riesgo de ManageEngine se refiere a la evaluación y comprensión de los riesgos asociados a la utilización de las soluciones y herramientas proporcionadas por ManageEngine, una empresa que ofrece software de gestión y seguridad de TI.

Paso 1: Para utilizar la herramienta de análisis, es necesario agregar el servidor que se va a analizar. En el caso de un servidor de Windows, se sugiere configurar inicialmente los siguientes aspectos, siendo fundamental la selección de las carpetas compartidas y las rutas de las subcarpetas que serán objeto de análisis. Se incluye una imagen de referencia en la Figura 21 para facilitar la comprensión.

Figura 57.

Editor de servidor de archivos

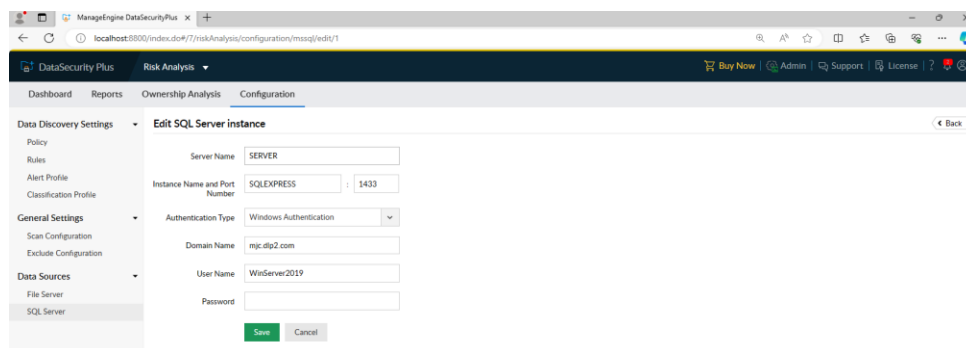


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 2: El paso subsiguiente consiste en agregar el servidor SQL, y los detalles introducidos aquí deben corresponder a las configuraciones previamente establecidas, como se muestra en la Figura 22.

Figura 58.

Configuración de SQL Server

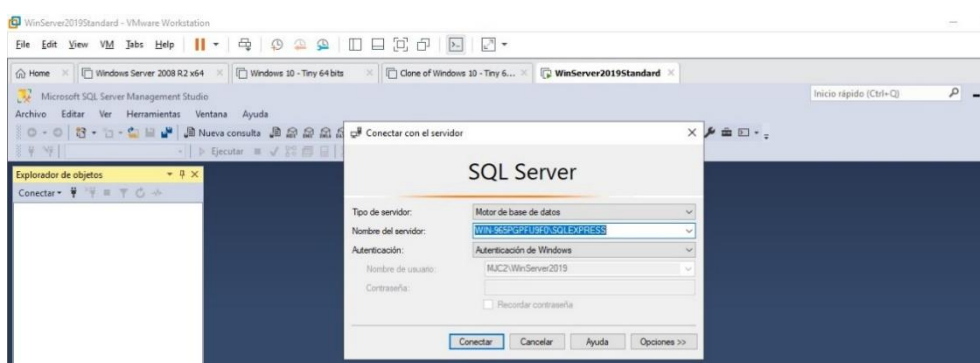


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 3: Además, se ha instalado el administrador SQL, cuya función principal es simplificar la creación, manipulación y administración de bases de datos, así como la gestión de la información almacenada en ellas. En la Figura 23 se realiza la conexión al servidor instalado en la misma máquina es prácticamente automática utilizando una de las cuentas especificadas durante la instalación.

Figura 59.

Instalación de administrador SQL

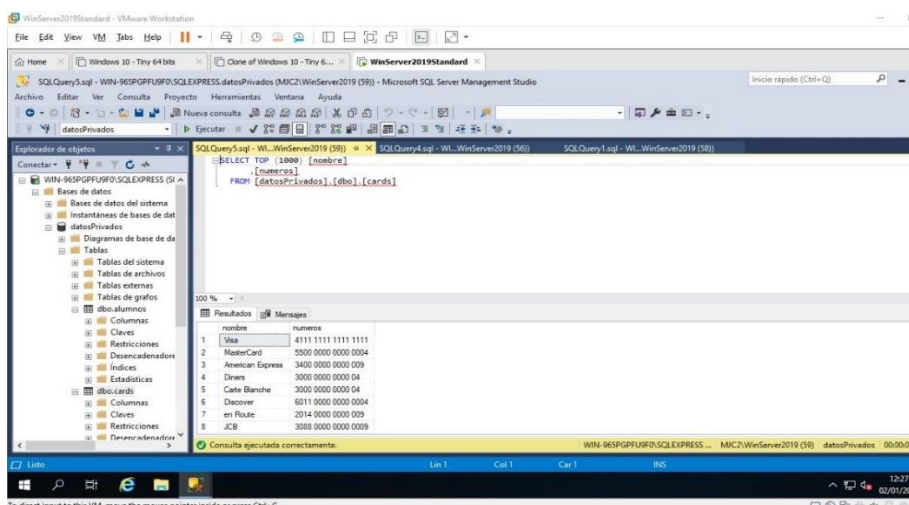


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 4: En la base de datos, se ha creado una entidad llamada "datosPrivados" con dos tablas, siendo que una de ellas incluye de manera predeterminada varios números de tarjetas de crédito, como se puede apreciar en la Figura 24.

Figura 60.

Base de datos



Nota: Elaboración propia basada en la experiencia con ManageEngine

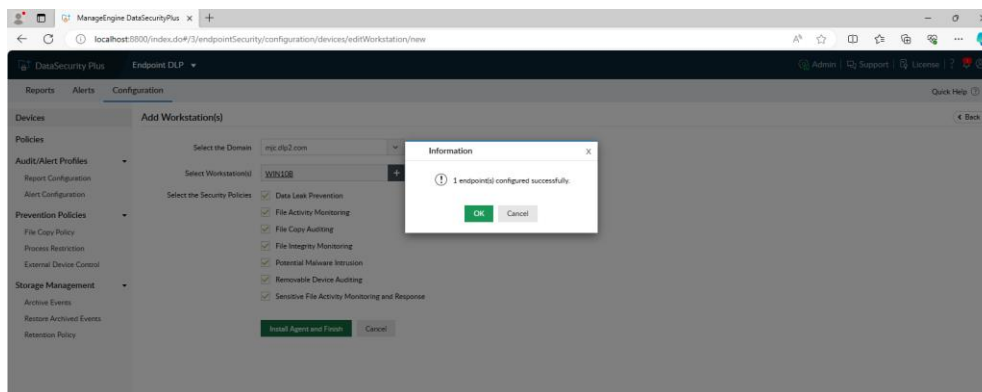
5.4.5. *Endpoint DLP*

Refuerza la seguridad de sus puntos finales contra amenazas internas y dispositivos no permitidos mediante la encriptación, categorización y resguardo de datos esenciales para su empresa.

- **Paso 1:** Una vez que el equipo haya sido registrado, en un corto período de tiempo, ME reconocerá la adición de la nueva máquina al dominio y permitirá su selección como estación de trabajo (Workstation) para su configuración. En este punto, existe la posibilidad de elegir las políticas por defecto que se aplicarán en esta máquina. La configuración adoptada se encuentra ilustrada en la Figura 25.

Figura 61.

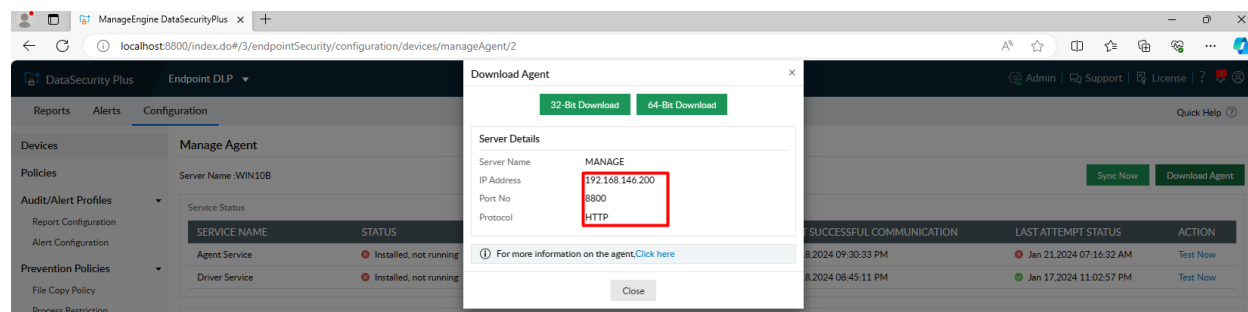
Configuración exitosa de Usuario



Nota: Elaboración propia basada en la experiencia con ManageEngine

- **Paso 2:** Cuando instale el agente DataSecurity, deberá proporcionar el nombre o la dirección IP del servidor de ManageEngine y configurar el puerto de comunicación en el número 8800. Además, se utiliza el protocolo HTTP para la comunicación al como se muestra en la figura correspondiente, tal como se observa en la figura 26.

Figura 62.

Configuración de agente

Nota: Elaboración propia basada en la experiencia con ManageEngine

5.5. Configuraciones según las políticas de prevención de fuga de información

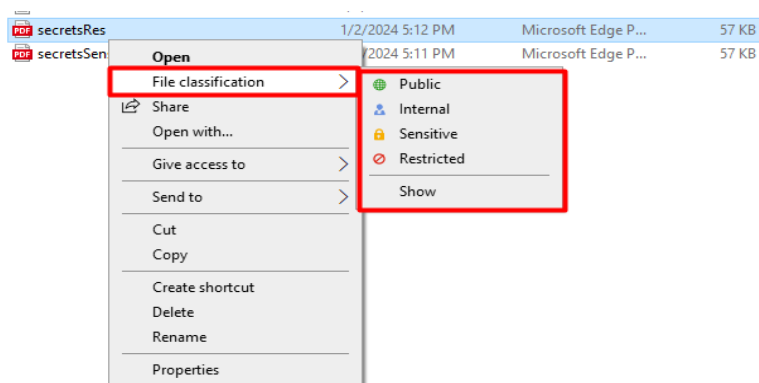
Basándose en el manual de políticas de prevención de fuga de información, se llevan a cabo configuraciones que se detallarán en las políticas de la herramienta y podrán ajustarse según las actividades, describiendo cómo se implementan en acciones específicas.

5.5.1. Clasificación de información

En el proceso de clasificación de información, se considera la acción de ordenar y agrupar documentos y datos en categorías particulares basadas en criterios definidos en el manual de Prevención de Fuga de Información. A través de este proceso, se identifican y determinan los activos de información.

- **Paso 1:** Tras la instalación del agente DataSecurity Plus, se activa la posibilidad de incorporar la funcionalidad de clasificación de información en los dispositivos finales. Esta característica faculta la visualización de "File Classification" al efectuar un clic izquierdo en los archivos. La elección de la clasificación pertinente se realiza de acuerdo con las categorías definidas, tal como se presenta en la figura 27 correspondiente.

Figura 63.

File Classification

Nota: Elaboración propia basada en la experiencia con ManageEngine

- **Paso 2:** En la sección de Reportes, más precisamente en File Classification Report > Data Classification Report, se encuentra información que rastrea el dispositivo utilizado para realizar cambios, el momento en que se efectuaron las modificaciones, el nombre del usuario que inició sesión para llevar a cabo la alteración y la clasificación que se asignó al archivo. Estos detalles están representados en la Figura 28.

Figura 64.

Reporte de Clasificación de información

The image shows a screenshot of the 'Data Classification Report' in the ManageEngine DataSecurity Plus interface. The report displays a table with the following columns: ENDPOINT NAME, TIME GENERATED, USER NAME, CLASSIFICATION VALUE, LOCATION, FILE SIZE, and FILETYPE EXTENSION. The first row is highlighted with a red box.

ENDPOINT NAME	TIME GENERATED	USER NAME	CLASSIFICATION VALUE	LOCATION	FILE SIZE	FILETYPE EXTENSION
WIN10B	Jan 02, 2024 05:11:24 PM	MJC2\admin	Restricted	C:\Users\admin\Downloads\secrets - Copy.txt	920	txt
WIN10B	Jan 02, 2024 05:10:44 PM	MJC2\admin	Sensitive	C:\Users\admin\Downloads\secrets.txt	920	txt
WIN10B	Jan 02, 2024 05:10:37 PM	MJC2\admin	Restricted	C:\Users\admin\Downloads\SpotifySetup21.exe	932824	exe
WIN10B	Jan 02, 2024 05:10:29 PM	MJC2\admin	Sensitive	C:\Users\admin\Downloads\Firefox Installer5.exe	398784	exe

Nota: Elaboración propia basada en la experiencia con ManageEngine

5.5.2. Acceso y control de datos

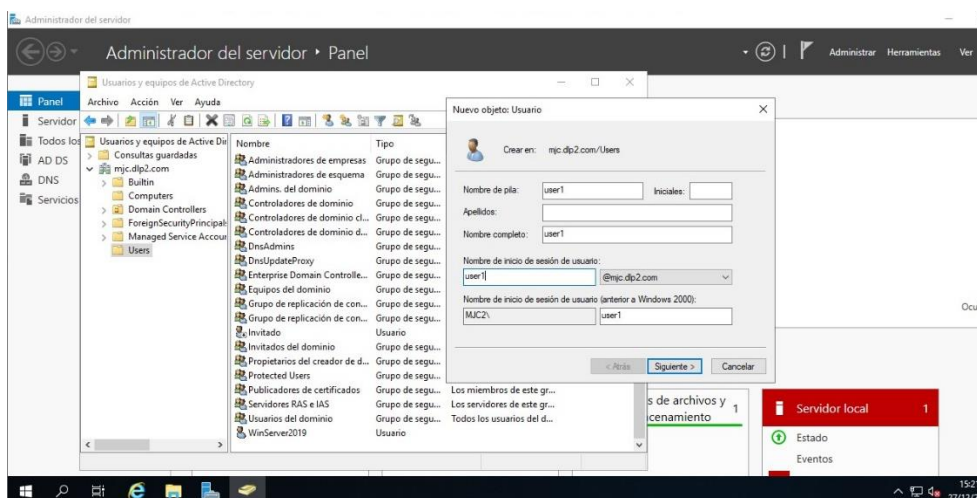
El acceso y control de datos permite una implementación efectiva de estas medidas contribuye a garantizar la seguridad y la privacidad de los datos almacenados en los dispositivos

finales como parte de las políticas de prevención de fuga de información, por lo que al configurar una Active Directory permite la gestión y autenticación de los usuarios.

Paso 1: Para añadir nuevos usuarios, abrir la herramienta de Usuarios y Equipos de Active Directory. Posterior, expandir el dominio y seleccionar el archivo de Usuarios.

Figura 65.

Agregar usuarios Active Directory

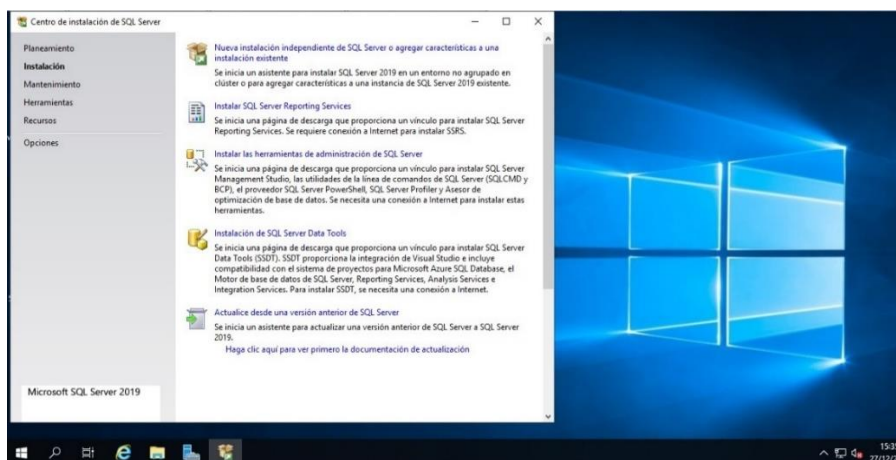


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 2: La instalación de la base de datos se realizó mediante el asistente de SQL EXPRESS. Al ejecutarlo, se eligió la primera opción que es la "Instalación de SQL Server".

Figura 66.

Instalación de la base de datos



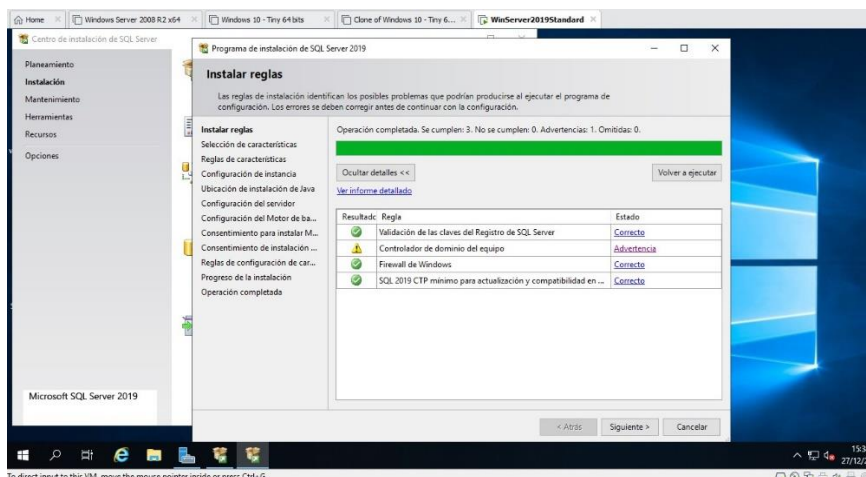
Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 3: Asegurarse de que se cumplan con los requisitos principales para la instalación.

Se ha observado una advertencia, posiblemente relacionada con el servidor que también funciona como controladora, generando una alerta de buenas prácticas, como se observa en la Figura 31.

Figura 67.

Instalación de reglas



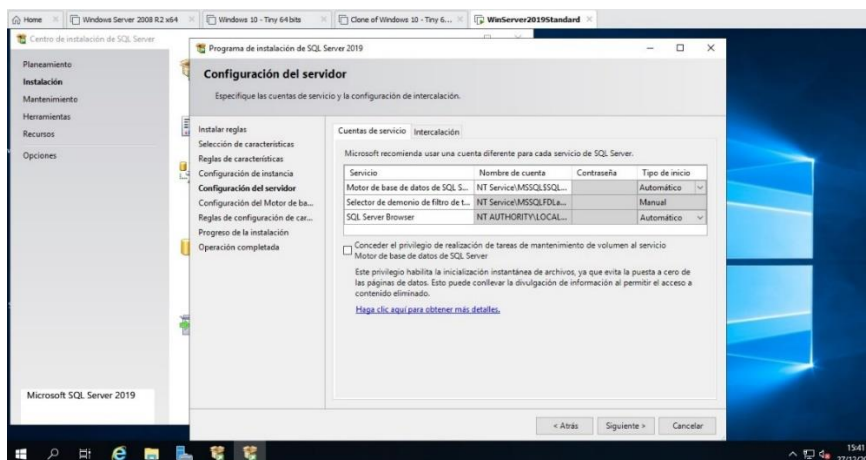
Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 4: Asegurarse de que, dentro de la configuración del servidor, el servicio SQL Server

Browser se inicie automáticamente. Como se puede observar en la Figura 32.

Figura 68.

Configuración del servidor

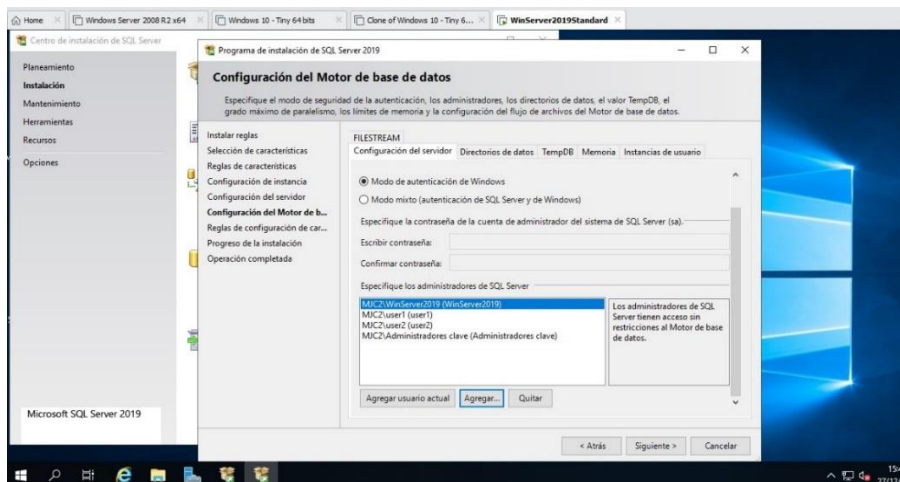


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 5: La autenticación utilizada para acceder a la base de datos será la de Windows, lo que implica utilizar el nombre de usuario y la contraseña registrados en Active Directory. Se indicarán los usuarios con los permisos necesarios para administrar la base de datos.

Figura 69.

Configuración del Motor de base de datos

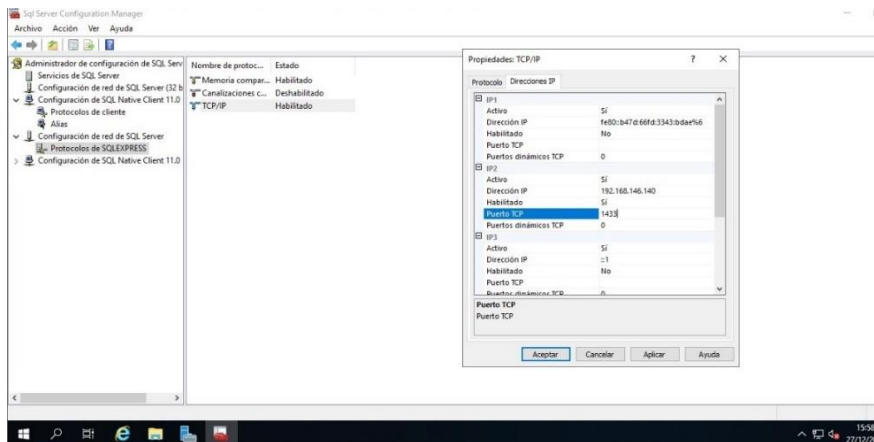


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 6: Para permitir la conexión de equipos a la base de datos, abrir el SQL Server Configuration Manager. En la configuración de red, seleccionar los protocolos de la instancia y habilitar TCP/IP. Posteriormente, en las propiedades de este protocolo, activar el correspondiente a IPv4 e introducir 1433 como puerto predeterminado. Como se puede ver en la Figura 34.

Figura 70.

SQL Server Configuration Manager



Nota: Elaboración propia basada en la experiencia con ManageEngine

5.5.3. Seguridad dispositivos de almacenamiento

Garantizar la seguridad de los dispositivos de almacenamiento es esencial para resguardar la información confidencial de una entidad. La Prevención de Pérdida de Datos se centra en prevenir la fuga de información sensible, y a continuación se presentan algunas consideraciones particulares para fortalecer la seguridad de estos dispositivos.

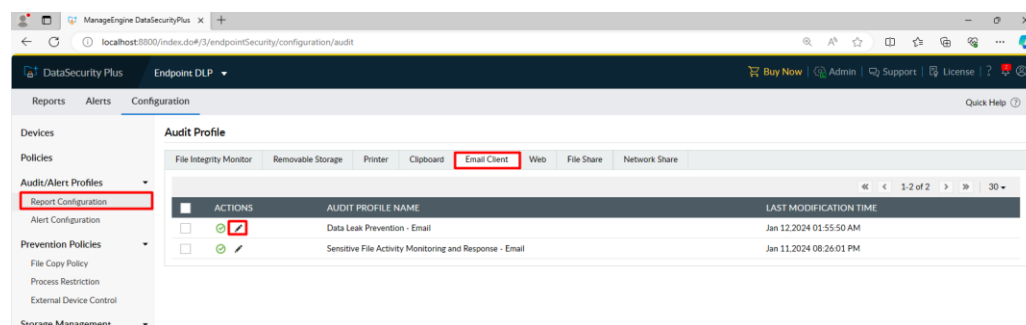
Configuración de restricción de correo electrónico.

La seguridad y la confiabilidad de la comunicación por correo electrónico en un ámbito empresarial son primordiales. Esto se logra a través de la configuración de bloqueo de correo electrónico, que posibilita la definición y gestión de reglas o políticas que determinan qué correos electrónicos deben ser bloqueados o restringidos en su plataforma de administración de correo electrónico de ManageEngine.

Paso 1: En la Figura 35, se puede apreciar la sección de configuración de auditoría (Audit Configuration), donde es posible ajustar los perfiles vinculados a distintos tipos de análisis. No obstante, solamente se permitirá editar los perfiles ya existentes, sin la posibilidad de añadir nuevos perfiles.

Figura 71.

Audit Configuration - Endpoint DLP

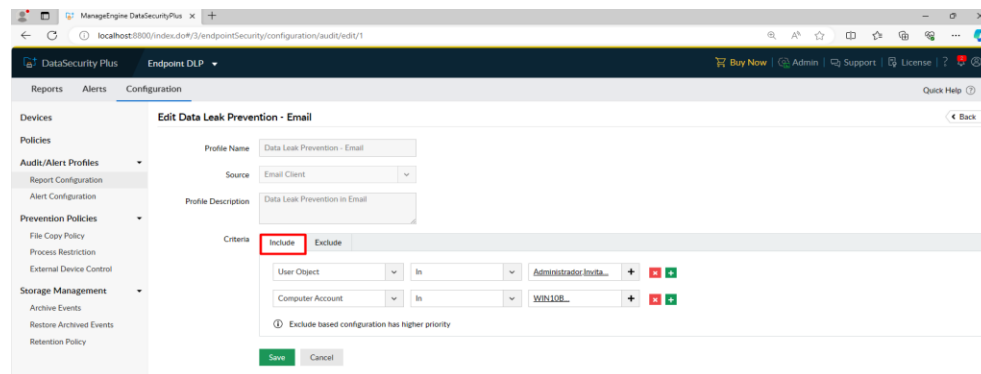


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 2: Dentro de la sección de **Criteria**, seleccionar las "reglas" que el archivo debe satisfacer para que se genere la alerta o el informe correspondiente, tal como se muestra en la representación presentada en la Figura 36.

Figura 72.

Configuración de perfiles de sistemas

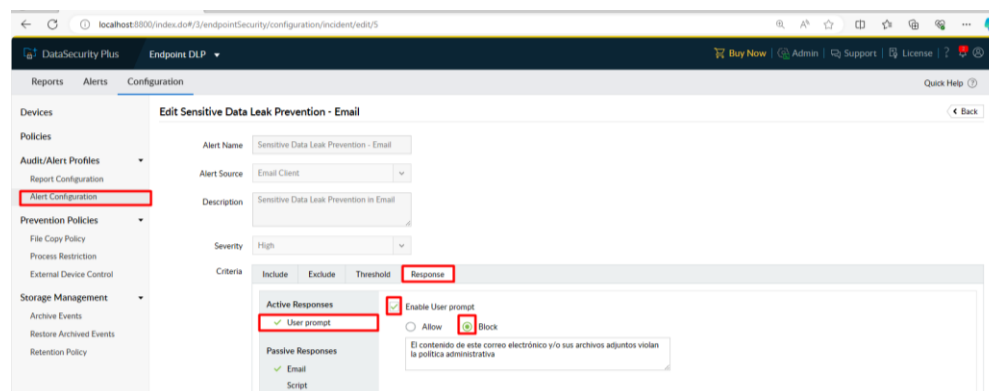


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 3: Cuando se trata de las alertas, se emplea un enfoque similar de configuración, tal como se observa en la Figura 37. Estas respuestas pueden ser en forma de mensajes que aparecerán en la pantalla, ofreciendo la alternativa de permitir o bloquear la acción correspondiente.

Figura 73.

Configuración de alertas según la política

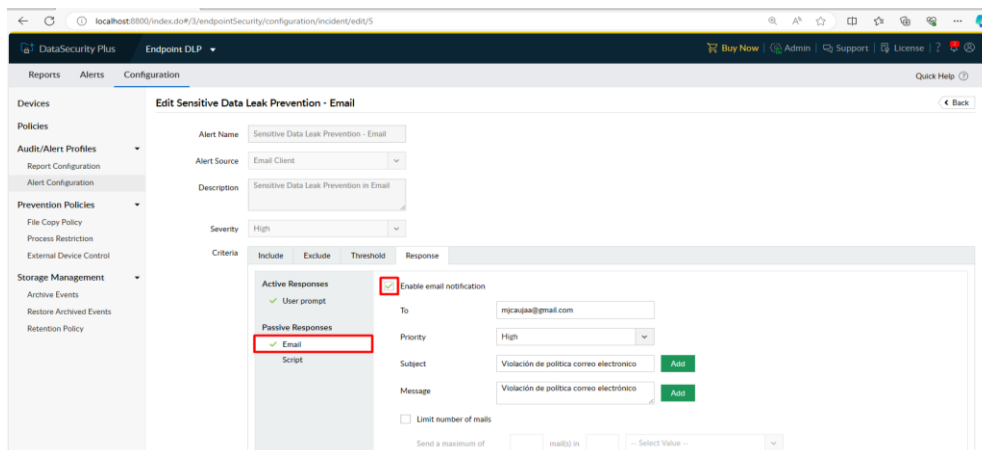


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 4: La herramienta enviará notificaciones por correo electrónico, la información detallada que se enviará por correo se definirá a través de las variables o metadatos de los

eventos. Es importante que se haya configurado previamente el servidor de correo, en este caso, Gmail. Como se observa en la figura 38.

Figura 74. Configuración de email para alertas

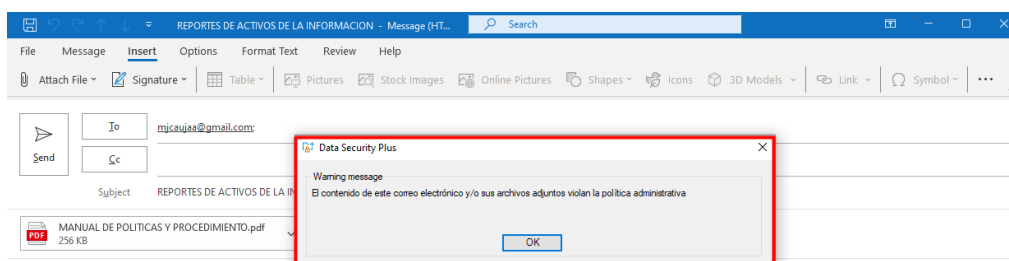


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 5: En la figura 39, se muestra lo que ocurrirá cuando se intente enviar un correo después de haber configurado la función de alerta en pantalla para el usuario, se presentará el mensaje de alerta “El contenido de este correo electrónico y/o sus archivos adjuntos violan la política administrativa”

Figura 75.

Restricción de envío de correo de archivos restringidos

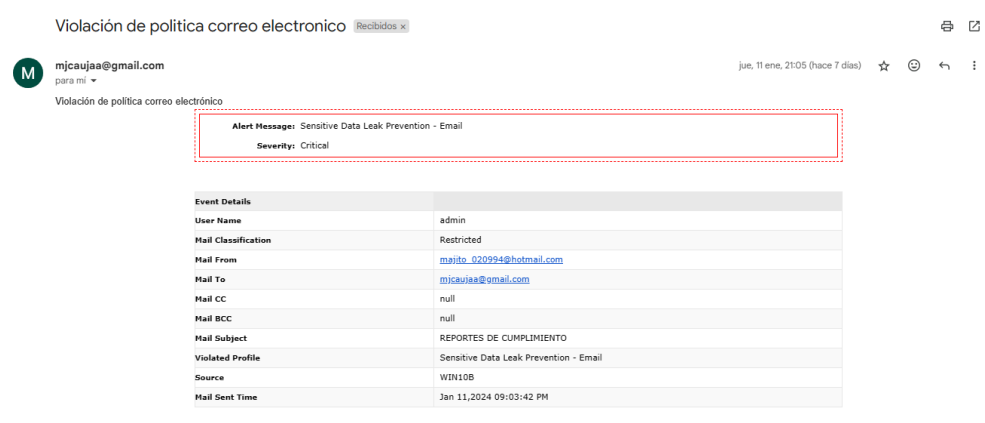


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 6: En la Figura 40, se puede observar la recepción de correos después de haberlos configurado de acuerdo con las opciones previamente explicadas.

Figura 76.

Correo de alerta de correo



Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 7: De manera similar, la pestaña de alertas ofrecerá un resumen de los detalles del evento, tal como se puede apreciar en la Figura 41.

Figura 77.

Alertas de la herramienta DLP

VIOLATED PROFILE	VIOLATED BY	SOURCE	INCIDENT TIME	SEVERITY	MAIL FROM	MAIL TO	MAIL CC	MAIL SUBJECT	MAIL SENT TIME	MAIL CLASSIFICATION
Sensitive File Activity Monitoring and Response - Email	admin	WIN10B	Jan 11, 2024 09:03:42 PM	Medium	majito_020994@hotmail.com	mjcaujaa@gmail.com	-	REPORTES DE CUMPLIMIENTO	Jan 11, 2024 09:03:42 PM	Restricted
Sensitive Data Leak Prevention - Email	admin	WIN10B	Jan 11, 2024 09:03:42 PM	High	majito_020994@hotmail.com	mjcaujaa@gmail.com	-	REPORTES DE CUMPLIMIENTO	Jan 11, 2024 09:03:42 PM	Restricted
Sensitive File Activity Monitoring and Response - Email	admin	WIN10B	Jan 11, 2024 08:47:04 PM	Medium	majito_020994@hotmail.com	mjcaujaa@gmail.com	-	REPORTES DE ACTIVOS DE LA INFORMACION	Jan 11, 2024 08:47:04 PM	Restricted
Sensitive Data Leak Prevention - Email	admin	WIN10B	Jan 11, 2024 08:47:04 PM	High	majito_020994@hotmail.com	mjcaujaa@gmail.com	-	REPORTES DE ACTIVOS DE LA INFORMACION	Jan 11, 2024 08:47:04 PM	Restricted

Nota: Elaboración propia basada en la experiencia con ManageEngine

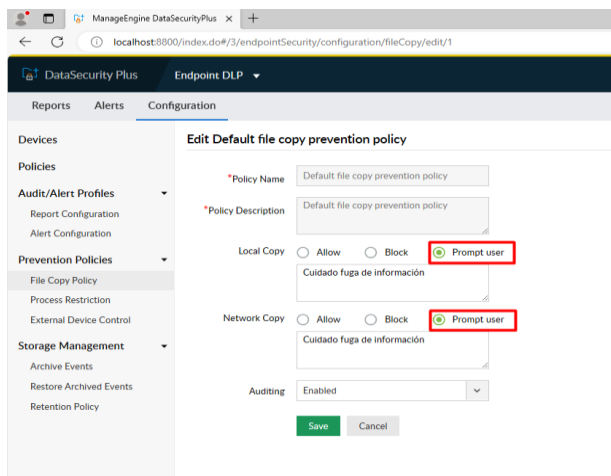
Configuración de prevención de copias de archivos

Dentro de la sección de políticas de prevención de fuga de información, específicamente en la política relacionada con la copia de archivos, se establece cómo se debe actuar cuando se copian archivos localmente o dentro de la red de trabajo.

Paso 1: Las opciones disponibles al activar este evento son similares a las mencionadas anteriormente, lo que significa que se puede permitir, bloquear o mostrar un mensaje específico en pantalla. En la Figura 42 se detallan las configuraciones pertinentes que activarán esta restricción en los archivos.

Figura 78.

Política de Prevención de archivos copiados

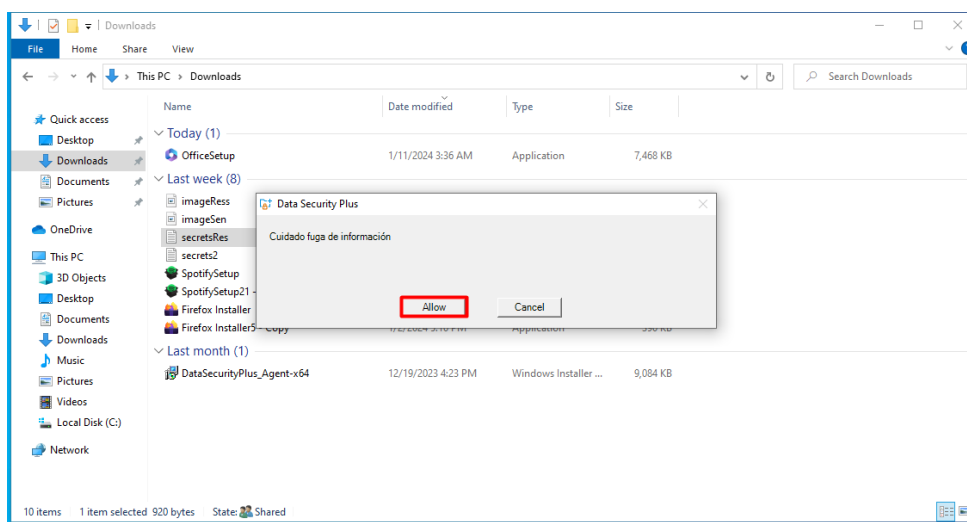


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 2: Cuando se intenta copiar cualquier archivo, aparecerá un mensaje de alerta que dice " Cuidado con la filtración de información", tal como se muestra en la Figura 43.

Figura 79.

Alerta emitida durante la copia de archivos.



Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 3: En la Figura 44, se muestra el informe de seguimiento de la copia de archivos, donde se pueden identificar el dispositivo final que está incumpliendo la política, la fecha y la hora de la acción, el usuario que intentó realizarla, el mensaje de alerta generado y la ubicación del archivo que se está copiando.

Figura 80.

Reporte de incumplimiento de la política de copia de archivos

ENDPOINT NAME	TIME GENERATED	ACCESSED BY	MESSAGE	COPIED FROM	PROCESS NAME	CLIENT HOST	IS NETWORK COPY
WIN108	Jan 12, 2024 02:04:41 AM	user1	File Copied	E:\3DP_Net_v2101.exe	C:\Windows\Explorer.EXE	WIN108	false
WIN108	Jan 12, 2024 02:04:23 AM	user1	File Copied	C:\Users\user1\Documents\REPORTES DE GESTION DE RIESGO\GESTIONRIESGO-NORMAZ7002-2013.pdf	C:\Windows\Explorer.EXE	WIN108	false
WIN108	Jan 12, 2024 02:03:00 AM	user1	File Copied	C:\Users\user1\Documents\REPORTES DE GESTION DE RIESGO\GESTIONRIESGOS_CUMPLIMIENTO27701.pdf	C:\Windows\Explorer.EXE	WIN108	false
WIN108	Jan 11, 2024 10:07:43 PM	user1	File Copied	E:\REPORTES DE GESTION DE RIESGO	C:\Windows\Explorer.EXE	WIN108	false
WIN108	Jan 11, 2024 10:07:43 PM	user1	File Copied	E:\MANUALES Y GUIAS	C:\Windows\Explorer.EXE	WIN108	false
WIN108	Jan 11, 2024 10:07:43 PM	user1	File Copied	E:\REFERENCIA	C:\Windows\Explorer.EXE	WIN108	false

Nota: Elaboración propia basada en la experiencia con ManageEngine

Configuración para controlar la actividad de dispositivos USB

Dentro de las opciones que ofrece la herramienta de ManageEngine, es posible establecer restricciones para la actividad de los dispositivos USB. Esto implica la capacidad de activar o desactivar dispositivos USB, configurar permisos de lectura y escritura, y establecer políticas de seguridad. Es fundamental realizar pruebas y supervisar la eficacia de estas restricciones USB para asegurarse de que estén alineadas con los estándares de seguridad que se requieran.

Paso 1: Para establecer la configuración de bloqueo de dispositivos USB, se llevan a cabo diversos ajustes en la sección "Endpoint DLP > Configuration > Audit Configuration > Removable Storage". Aquí, es posible revisar las múltiples acciones que pueden ser auditadas, como se muestra en la Figura 45.

Figura 81.

Configuración de Audit Configuration

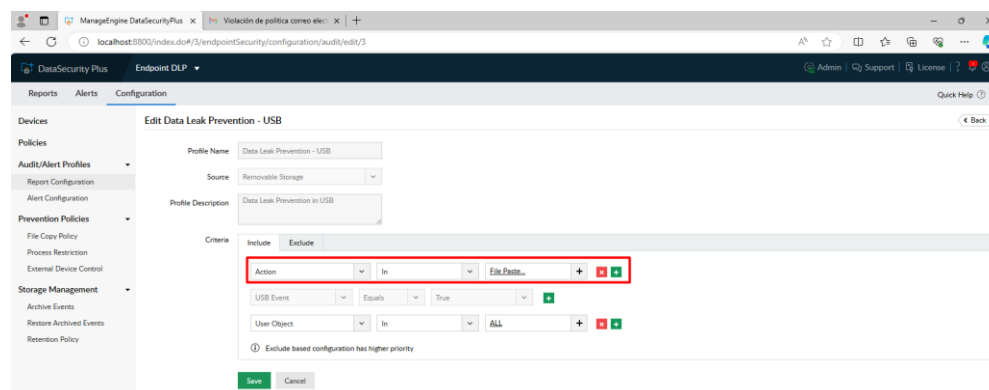
ACTIONS	AUDIT PROFILE NAME	LAST MODIFICATION TIME
<input type="checkbox"/>	Data Leak Prevention - USB	May 01, 2019 10:33:10 AM
<input type="checkbox"/>	Removable Device Auditing	May 01, 2019 10:33:10 AM
<input type="checkbox"/>	Sensitive File Activity Monitoring and Response - USB	May 01, 2019 10:33:10 AM

Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 2: Para modificar la configuración de Prevención de Pérdida de Datos (Data Leak Prevention) relacionada con dispositivos USB, es posible examinar las acciones disponibles que determinarán qué actividades serán capturadas y auditadas en los dispositivos finales. Estas configuraciones se llevan a cabo como se muestra en la Figura 46.

Figura 82.

Configuraciones de Data Leak Prevention- USB

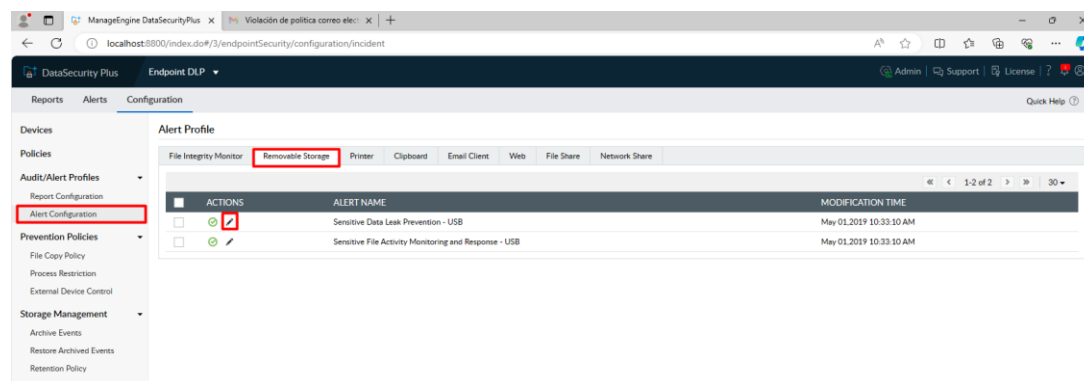


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 3: Para configurar alertas relacionadas con el bloqueo de actividades USB, es necesario ingresar a la sección "Alert Configuration > Removable Storage > Sensitive Data Leak Prevention- USB", como se muestra en la figura 47.

Figura 83.

Configuración de alerta de actividad USB



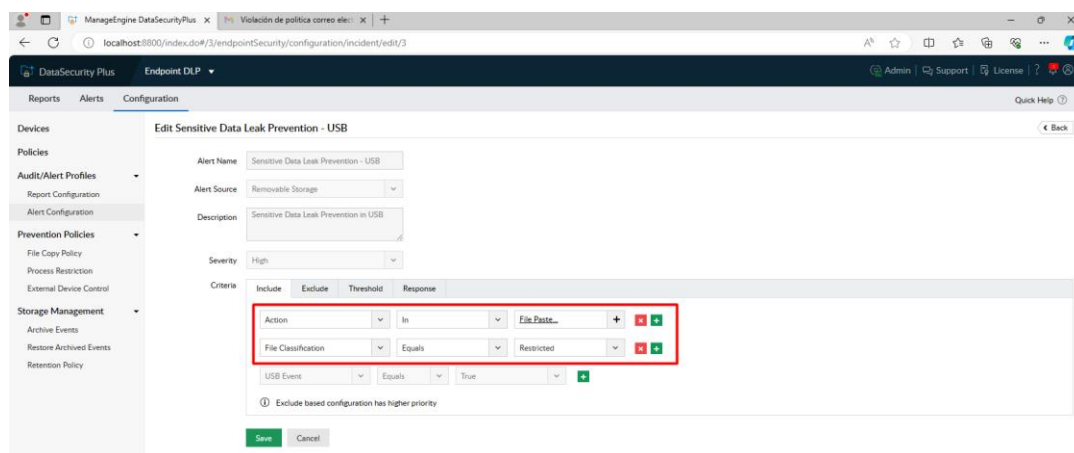
Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 4: Dentro de la sección de Configuración de Alertas, se realiza la configuración de la función Sensitive Data Leak Prevention – USB relacionada con dispositivos USB. En esta

configuración, se detallan las acciones que se incluirán, y se especifican los archivos que serán clasificados, como se muestra en la figura 48.

Figura 84.

Acciones incluidas en la política de alerta USB

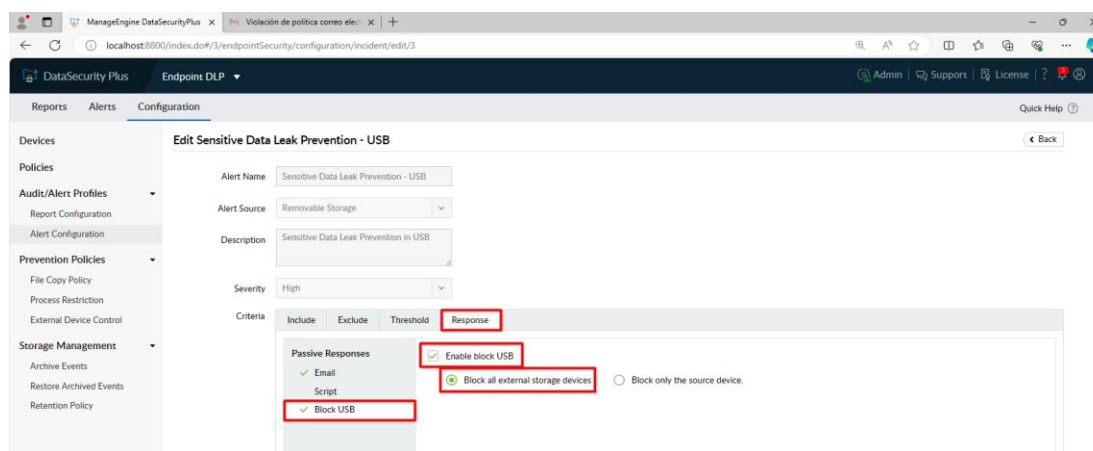


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 5: La opción "Response" permite implementar respuestas pasivas que posibilitan el bloqueo de dispositivos USB. Esto se ilustra en la figura 49 al seleccionar "Response > Block USB > Enable block USB > Block external storage devices".

Figura 85.

Activar bloqueo USB

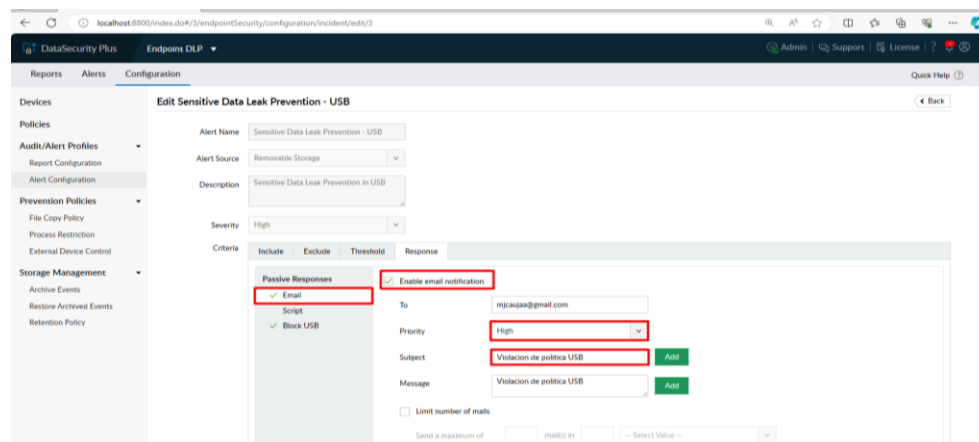


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 6: Para habilitar la alerta por correo electrónico, se puede observar en la figura 50 cómo realizar la configuración, que se describe de la siguiente manera: "Response > Email > Enable email notification".

Figura 86.

Alerta por correo electrónico



Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 7: Cuando se registra que una acción de la política está en curso, esto se refleja en la sección "Reports > Removable Storage File Activity", tal como se muestra en la Figura 51.

Aquí, se pueden visualizar detalles como:

- "Endpoint Name", indica el dispositivo desde el cual se está llevando a cabo la actividad.
- "Time Generated", establece la fecha y hora en que ocurrió la actividad.
- "Accessed By", identifica al usuario que está realizando la actividad.
- "Message", describe la acción que se está realizando en los archivos.
- "Location", señala la ubicación del archivo a través del cual se está ejecutando en el dispositivo final.

Figura 87.

Reporte de actividad de dispositivo USB

Endpoint Name	Time Generated	Accessed By	Message	Location	Process Name	Client Host
WIN10B	Jan 18, 2024 07:50:06 PM	admin	Read	E:\Arenas\Bicoreas.xlsx	C:\Windows\explorer.exe	WIN10B

Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 8: También es posible notar como parte del informe de incumplimiento de políticas, se encuentra en la sección "USB Security Response" que demuestra que el dispositivo fue bloqueado. En la figura 52, se pueden observar las siguientes acciones:

- "Action", indica si el dispositivo ha sido bloqueado.
- "Endpoint Name", identifica el dispositivo desde el cual se está ejecutando la actividad.
- "USB Status", establece el tipo de bloqueo aplicado, que es para todos los dispositivos de almacenamiento externo.
- "Client Host", determina el usuario que realizó la actividad.
- "Device Name", especifica el nombre del dispositivo que está siendo bloqueado.
- "Device Instance Path", proporciona la ruta de instancia del dispositivo bloqueado

Figura 88.

Informe de incumplimiento de políticas USB

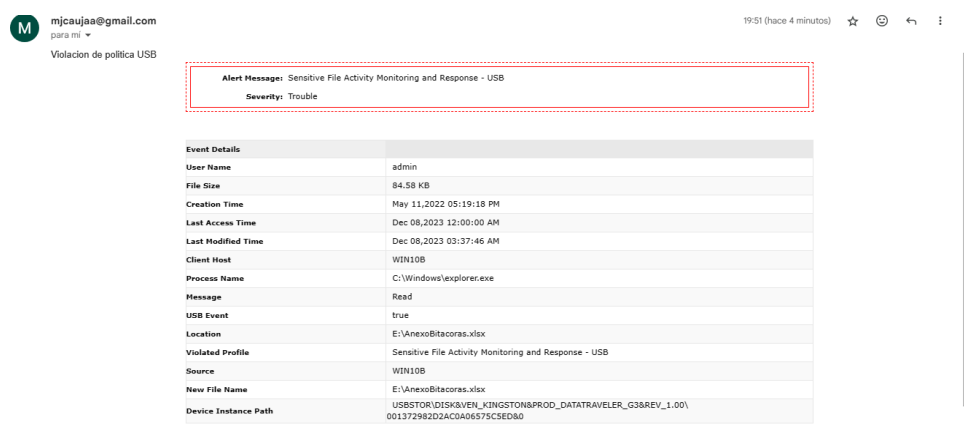
ACTION	ENDPOINT NAME	USB STATUS	UNBLOCKED BY	UNBLOCKED TIME	UNBLOCKED STATUS	CLIENT HOST	DEVICE NAME	DEVICE INSTANCE PATH
UNBLOCK	USER2	All external storage devices blocked.	-	-	-	User2	Kingston DataTraveler G3 USB Device	USBSTOR:DISK&VEN_KINGSTON&PROD_DATATRAVELER_G3&REV_1.00\001372982D2AC0A06579C5ED60
UNBLOCKED	USER2	All external storage devices blocked.	admin	Sep 20, 2023 12:23:58 PM	All external storage devices are unblocked.	User2	Kingston DataTraveler G3 USB Device	USBSTOR:DISK&VEN_KINGSTON&PROD_DATATRAVELER_G3&REV_1.00\001372982D2AC0A06579C5ED60

Paso 9: Otra de las alertas relacionadas con la violación de la política de USB se notifica a través del correo electrónico, como se muestra en la figura 53. Esta alerta proporciona detalles importantes que incluyen:

- "File Name", es el nombre del archivo en el que se ha producido la infracción de la política.
- "Process Name", indica la fuente desde la que se está ejecutando el proceso.
- "Message", especifica el tipo de acción que se está llevando a cabo en el archivo.

Figura 89.

Alerta de correo electrónico de USB



Nota: Elaboración propia basada en la experiencia con ManageEngine

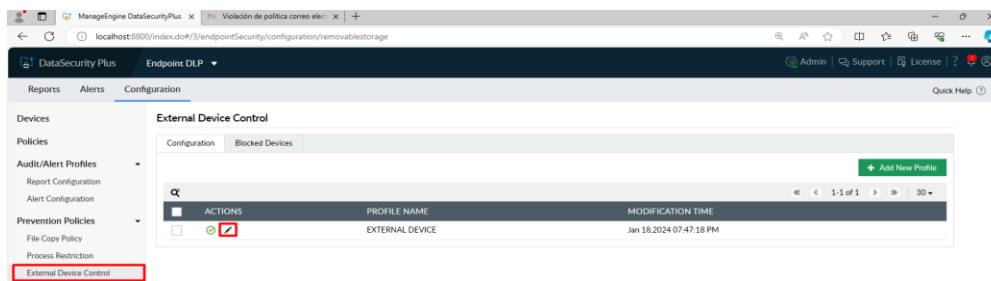
Gestionar la autorización para el uso de dispositivos externos

La configuración para restringir quién tiene la capacidad de emplear hardware externo, como unidades USB, discos duros, cámaras, teclados y mouse, en una red, por lo general se efectúa con el propósito de salvaguardar la seguridad y ejercer control de acceso.

Paso 1: La siguiente sección posibilita el bloqueo del acceso mediante dispositivos externos. Se aconseja que las reglas se configuren en "deshabilitar" y solo se activen para pruebas, con el fin de evitar posibles confusiones en el funcionamiento de la herramienta.

Figura 90.

Configuración de bloqueo externo

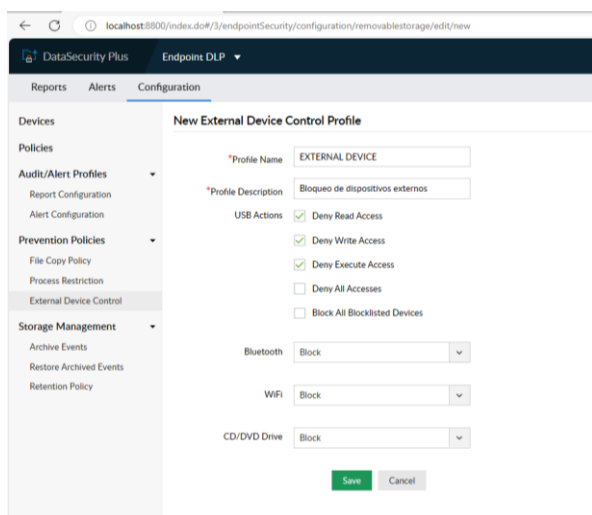


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 2: Para crear una regla en esta sección, tendrá la capacidad de elegir las acciones que se ejecutarán durante un evento USB. Además, tiene la opción de bloquear la transferencia de archivos hacia dispositivos conectados mediante Bluetooth, WiFi o CD, tal como se muestra en la figura 55.

Figura 91.

Configuraciones de bloqueo de dispositivos externos.

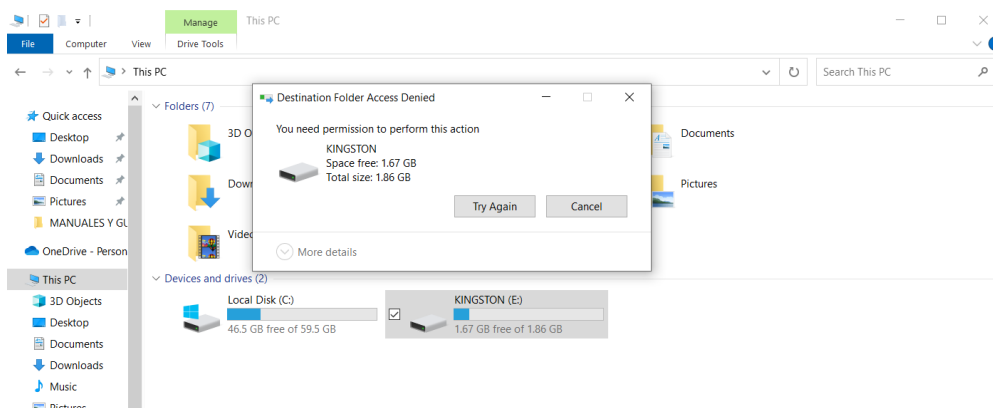


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 3: Cuando se prohíbe la copia de archivos hacia un dispositivo USB, la figura 56 representa la acción de transferencia de documentos en curso.

Figura 92.

Acceso denegado de transferencia de archivos

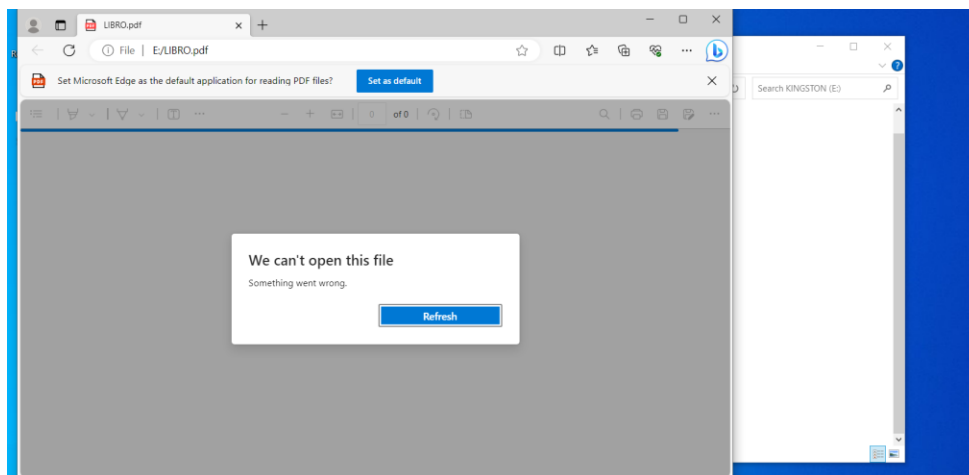


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 4: Cuando se aplican políticas de restricción de lectura en el dispositivo USB, se evidencia en la figura 57 que el archivo no puede ser abierto.

Figura 93.

Restricción de lectura del dispositivo USB

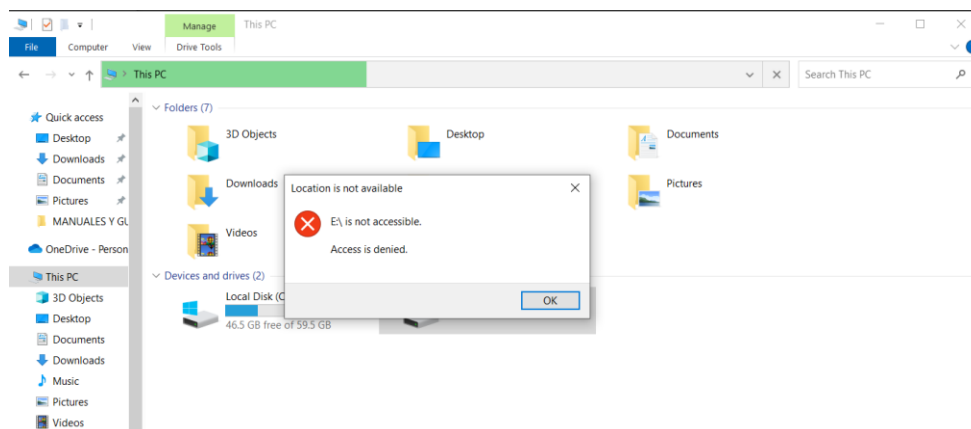


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 5: Dentro de las acciones relacionadas con dispositivos externos, es posible negar el acceso a cualquier dispositivo externo. Al realizar este procedimiento, se mostrará la siguiente notificación cuando se intente acceder, tal como se ilustra en la figura 58.

Figura 94.

Denegar acceso a dispositivos externos



Nota: Elaboración propia basada en la experiencia con ManageEngine

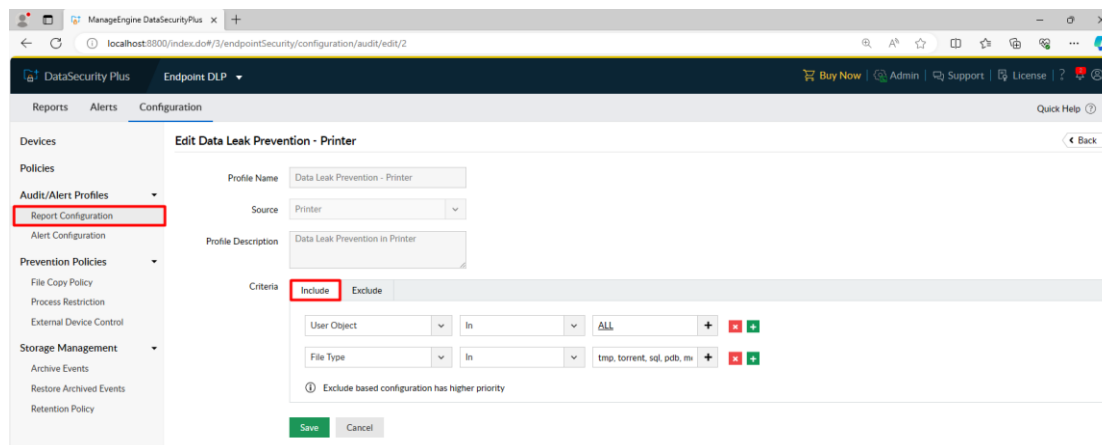
Gestión y monitoreo de impresión

Esta solución se enfoca de manera especial en la administración y vigilancia de las actividades de impresión, permitiéndote supervisar las impresiones, establecer límites de impresión y crear informes exhaustivos, entre otras funcionalidades adicionales.

Paso 1: La sección permite llevar un seguimiento de los archivos que se imprimen. Para configurar esta función, a través de la ruta "Audit Configuration > Printer". Puede establecer los criterios que se incorporan en la política, y es esencial especificar el tipo de archivos que se utilizarán para configurar la auditoría, como se muestra en la figura 59.

Figura 95.

Criterios de política

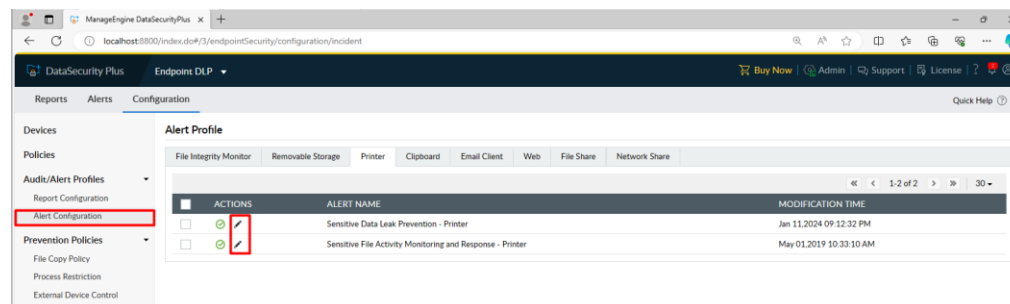


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 2: Para configurar las opciones de alerta, puede acceder a través de la selección "Alert Configuration > Printer", donde encontrará las alertas que pueden ser configuradas, como se muestra en la figura 60.

Figura 96.

Configuración de alertas Printer

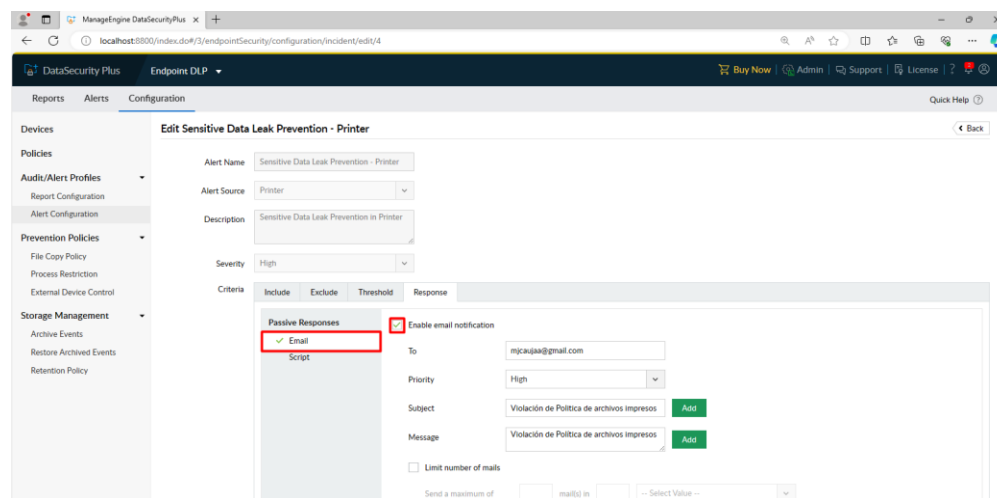


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 3: Se puede incluir los accesos que tendrán en cuenta en relación a las acciones de la política. Puede definir las alertas que se activarán en la sección Response > email al habilitar Enable email notification, y esta configuración se realizará como se muestra en la figura 61.

Figura 97.

Habilitar configuración de email para políticas Printer



Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 4: Dentro de la sección "Alerts", se pueden detectar la violación de la política, tal como se muestra en la figura 62, en la que se proporcionan detalles sobre varias características que también se enviarán por correo electrónico.

Figura 98.

Alerta de violación de política Printer

FILE NAME	PRINTER NAME	ENDPOINT NAME	USER NAME	TIME GENERATED	TOTAL PAGES	FILE SIZE
GUIA_PARA_ELABORACION_DE_DOCUMENTOS.pdf	Microsoft Print to PDF	WIN10B	mjc.dlp2.com/user1	Jan 11, 2024 10:11:17 PM	21	2168043
GUIA_PARA_ELABORACION_DE_DOCUMENTOS.pdf	Microsoft Print to PDF	WIN10B	mjc.dlp2.com/admin	Jan 11, 2024 09:13:45 PM	21	2168043
MANUAL DE POLITICAS Y PROCEDIMIENTO.pdf	Microsoft Print to PDF	WIN10B	mjc.dlp2.com/admin	Jan 11, 2024 09:10:04 PM	14	1749256
secretsRes - Notepad	Microsoft Print to PDF	WIN10B	mjc.dlp2.com/admin	Jan 02, 2024 05:12:00 PM	3	60057
secret2 - Notepad	Microsoft Print to PDF	WIN10B	mjc.dlp2.com/admin	Jan 02, 2024 05:11:48 PM	3	60065

Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 5: En el correo electrónico configurado, como se puede apreciar en la figura 63, se detallan las características que indican la infracción de la política, que son las siguientes:

- Notify Name: muestra el nombre del usuario que llevó a cabo esta acción.
- Printer Name: indica el nombre del dispositivo de impresión instalado.
- File Name: establece el nombre del documento que se imprimió sin autorización y que ha sido identificado como un archivo restringido.
- Violated policy: Sensitive Data Leak Prevention- Printer: esto identifica el tipo de alerta asociada a esta violación.
- Source: especifica el dispositivo final en el que se llevó a cabo esta acción.

Figura 99.

Notificación vía correo electrónico

Violación de Política de archivos impresos Recibidos x

mjcaujaa@gmail.com para mí jue, 11 ene, 22:13 (hace 11 días)

Violación de Política de archivos impresos

Alert Message: Sensitive Data Leak Prevention - Printer
Severity: Critical

Event Details	
File Size	2.07 MB
Creation Time	Jan 11, 2024 10:11:17 PM
Notify Name	user1
Total Pages	21
Printer Name	Microsoft Print to PDF
File Name	GUIA_PARA_ELABORACION_DE_DOCUMENTOS.pdf
Violated Profile	Sensitive Data Leak Prevention - Printer
Source	WIN10B

Nota: Elaboración propia basada en la experiencia con ManageEngine

5.5.4. Seguridad en base de datos

La protección de información confidencial almacenada en bases de datos en relación con la Prevención de Pérdida de Datos (DLP) requiere la aplicación de medidas específicas de seguridad.

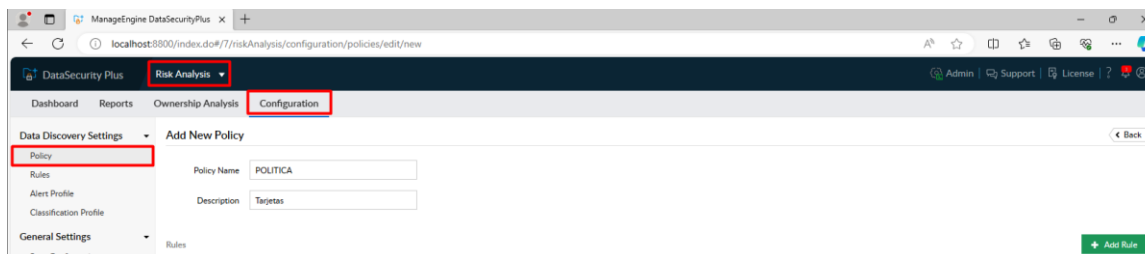
Desarrollo de políticas de archivos en el servidor.

Entre las configuraciones fundamentales que esta herramienta puede ajustar, se incluyen opciones que posibilitan la implementación de políticas de restricción de archivos en el servidor, lo que permitirá evaluar la sensibilidad de los archivos.

Paso 1: Para crear políticas de datos, se inicia el proceso en la sección de Risk Analysis > Policy, donde es posible cambiar el nombre y proporcionar una descripción a la política que se está configurando, tal como se muestra en la Figura 64.

Figura 100.

Creación de política de datos

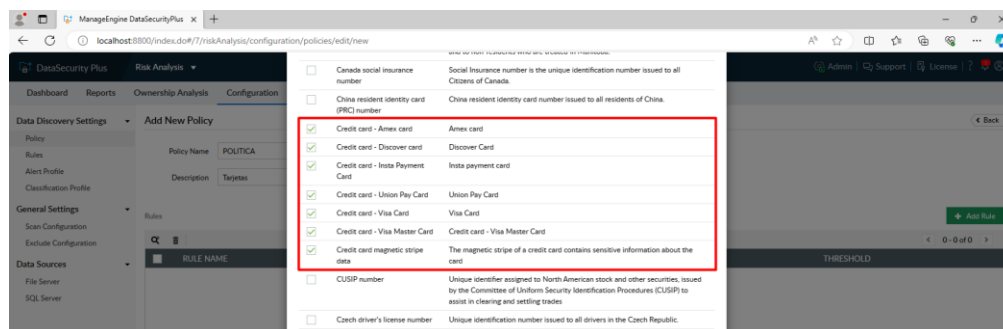


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 2: Luego, se procede haciendo clic en (Add Rule), donde se pueden elegir diversas características de acuerdo con las reglas definidas para analizar archivos de datos. La configuración específica para el análisis de datos se puede visualizar en la Figura 65.

Figura 101.

Agregar reglas



Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 3: Puede confirmarse la ejecución exitosa del análisis en la sección de Reports, donde se presenta en la figura 66. Aquí, se detallan los archivos que fueron objeto de análisis, la política a la que están vinculados, la cantidad de incidentes detectados y el nivel de riesgo asociado a los archivos examinados.

Figura 102.

Reportes de análisis de datos

NAME	LOCATION	SOURCE	SOURCE TYPE	SCAN START TIME	POLICY MATCHED	NO. OF OCCURRENCES	RISK SCORE	CLASSIFICATION LABEL
tarjeta1.txt	\\SERVER\NETLOGON	SERVER	File Server	Sep 04, 2023 04:13:01 PM	GDPR Policy	20	29	-
tarjeta1.txt	\\SERVER\NETLOGON	SERVER	File Server	Sep 04, 2023 04:13:01 PM	POLITICA	20	22	-
secrets1.txt	\\SERVER\NETLOGON	SERVER	File Server	Sep 04, 2023 04:13:01 PM	GDPR Policy	20	29	-
secrets1.txt	\\SERVER\NETLOGON	SERVER	File Server	Sep 04, 2023 04:13:01 PM	POLITICA	20	22	-
secrets1.txt	\\SERVER\SYSVOL\myc.dlp.com\scripts	SERVER	File Server	Sep 04, 2023 04:13:01 PM	GDPR Policy	20	29	-
secrets1.txt	\\SERVER\SYSVOL\myc.dlp.com\scripts	SERVER	File Server	Sep 04, 2023 04:13:01 PM	POLITICA	20	22	-
tarjeta1.txt	\\SERVER\SYSVOL\myc.dlp.com\scripts	SERVER	File Server	Sep 04, 2023 04:13:01 PM	GDPR Policy	20	29	-
tarjeta1.txt	\\SERVER\SYSVOL\myc.dlp.com\scripts	SERVER	File Server	Sep 04, 2023 04:13:01 PM	POLITICA	20	22	-

Nota: Elaboración propia basada en la experiencia con ManageEngine

Una vez que se haya completado el proceso de análisis de riesgos de los archivos inspeccionados, se procede a revisar los datos y los informes generados como resultado de este proceso. En la figura 67 se presentan los siguientes conjuntos de información:

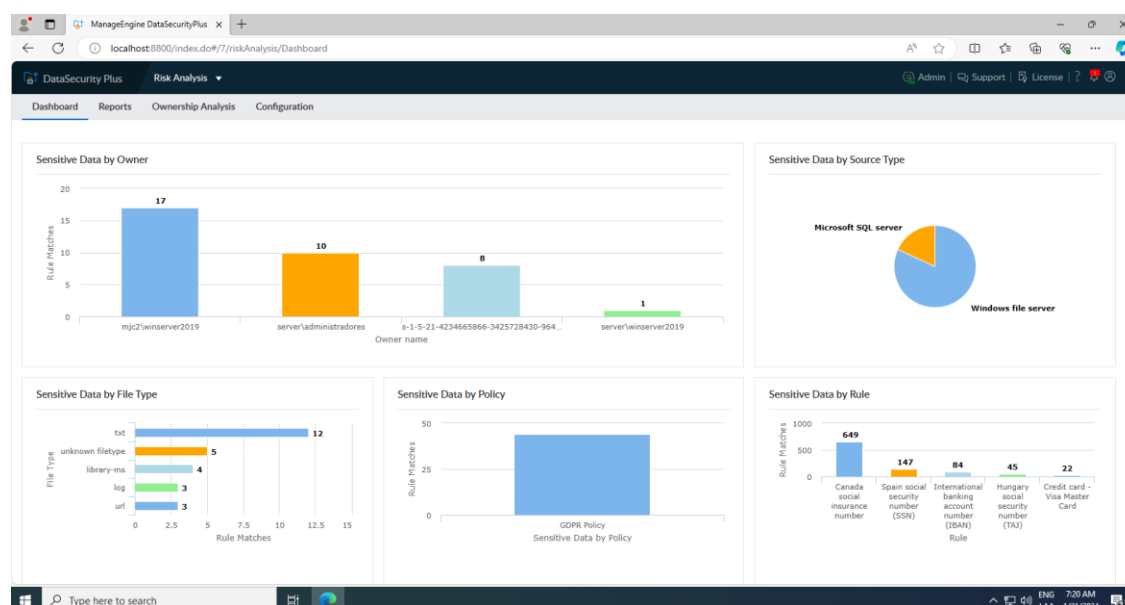
- La gráfica denominada "Sensitive Data by Owner" muestra el análisis de los usuarios en su servidor y la cantidad de archivos que han sido examinados.

- En la sección "Sensitive Data by Policy" se detallan las políticas que se aplicarán al análisis de los archivos sensibles.
- También se encuentra la sección "Sensitive Data by File Type", en la que se identifican los tipos de archivos vulnerables en función de las políticas que se han configurado.

De esta manera, es posible verificar la presencia de datos sensibles de acuerdo con las políticas establecidas para el análisis de los archivos.

Figura 103.

Reporte de análisis de riesgo

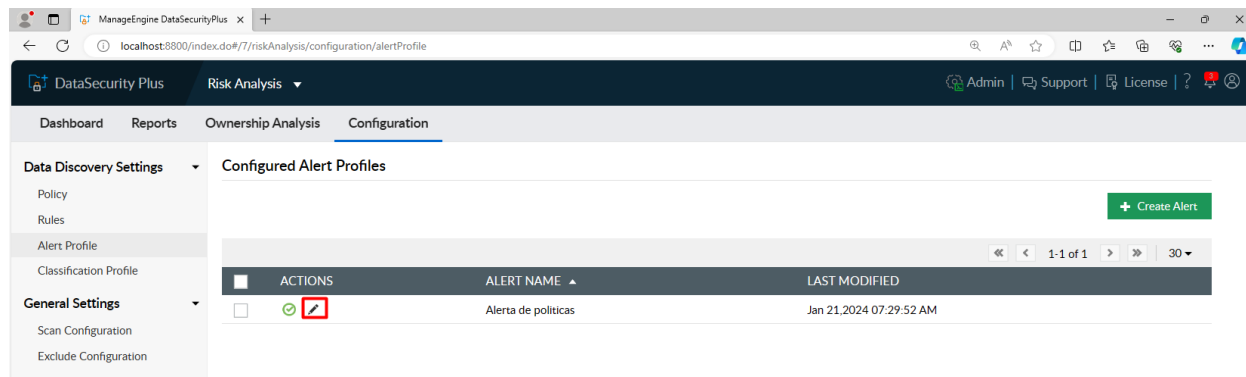


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 4: Se configura una alerta para comprobar el cumplimiento de las políticas definidas. Esto se logra al habilitar la notificación por correo electrónico y ajustar las configuraciones correspondientes en "Configuration > Alert Profile" al editar la alerta de políticas, como se muestra en la figura 68.

Figura 104.

Configuración de alerta

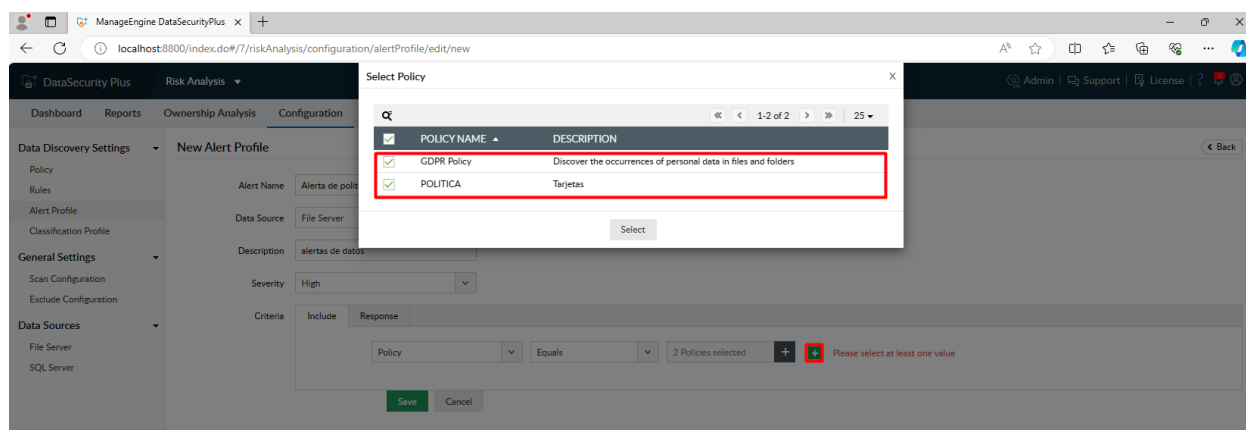


Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 5: A continuación, se opta por las políticas, marcando específicamente aquellas que están en proceso de evaluación. Esto se ilustra en la figura 69.

Figura 105.

Selección de políticas de análisis



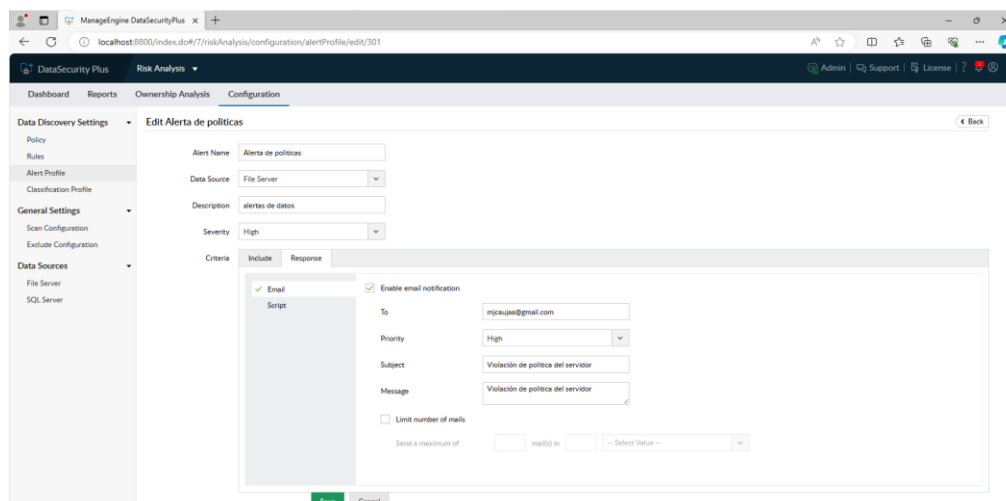
Nota: Elaboración propia basada en la experiencia con ManageEngine

Paso 6: En la sección de "Response" (Respuesta), se escoge la opción correspondiente.

En la Figura 70 se muestra cómo en la sección de correo electrónico se activan las notificaciones a través del correo electrónico, donde se configura la dirección de destino y el asunto para llevar a cabo la alerta.

Figura 106.

Alerta de política

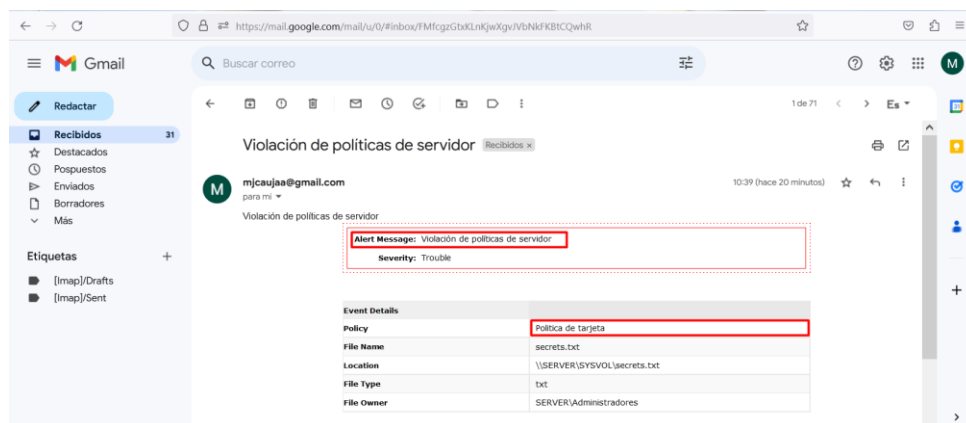


Nota: Elaboración propia basada en la experiencia con ManageEngine

- **Paso 7:** En el correo electrónico, se puede visualizar el mensaje de alerta junto con los detalles de los eventos y las especificaciones que describen la alerta, tal como se observa en la Figura 71.

Figura 107.

Notificación de Violación de políticas de servidor



Nota: Elaboración propia basada en la experiencia con ManageEngine

6. Lista de verificación de las acciones de acuerdo con la política de prevención de la fuga de información.

Dentro de la política de prevención de la fuga de información, se han definido procedimientos que se presentan como sugerencias de implementación en la entidad financiera COAC "Santa Anita Ltda." En este contexto, se ha creado una lista de verificación que permite

determinar cómo la herramienta ManageEngine puede ser útil para facilitar tanto el control como la prevención de la fuga de información. Esta lista de verificación se detalla en una tabla que incluye información sobre el procedimiento a seguir, una descripción del mismo y las acciones correspondientes que deben establecerse dentro de la herramienta en relación a las actividades.

Política	Actividad	Descripción	Acciones
Política de Prevención de Fuga de Información	Clasificación de información	Los activos de información se clasifican según los niveles de confidencialidad definidos en los procedimientos de la política de clasificación de información.	La herramienta de aplicación ofrece la posibilidad de categorizar la información de cada archivo, y esta configuración se puede realizar en la sección 4.5.1. Clasificación de información dentro de la guía.
	Acceso y control de datos	Implementar un sistema que restrinja los activos de información de acuerdo con los roles y niveles de acceso correspondientes a sus funciones respectivas	<p>Cada host se accede a través de usuarios de Active Directory en sus respectivos dominios, lo que permite detectar posibles intentos de violación de la seguridad de los archivos. Además, esta herramienta permite el monitoreo de cada dispositivo final en función de los usuarios que acceden a dichos dispositivos.</p> <p>Este proceso se divide en dos secciones.</p> <ul style="list-style-type: none"> - La primera implica la instalación de Active Directory en cada dispositivo final y la configuración de la conexión a través de los dominios, como se describe en la sección

			<p>4.5.2. Acceso y control de datos. La segunda sección se encuentra dentro de la herramienta ManageEngine, donde se realiza la configuración correspondiente para la administración de los dispositivos finales. Esta configuración se detalla en la sección 4.4.1. Admin Console</p>
	<p>Seguridad dispositivos finales</p>	<p>Una acción crucial para mitigar el riesgo de pérdida de datos consiste en supervisar los medios por los cuales la información podría filtrarse, como el correo electrónico, la transferencia de archivos, y unidades de almacenamiento portátiles</p>	<p>Dentro de la herramienta, es posible implementar políticas que tienen como objetivo prevenir la fuga de información al bloquear acciones específicas.</p> <p>Estas políticas abordan varias áreas, como sigue:</p> <ul style="list-style-type: none"> - Para evitar la filtración de información a través del correo electrónico, se pueden configurar políticas en la sección Configuración de restricción de correo electrónico. Estas políticas determinan el bloqueo y monitoreo de acuerdo con la clasificación de los archivos. - Con respecto a la transferencia de archivos, se establecen medidas en la sección Configuración de prevención de

			<p>copias de archivos, que determina el bloqueo y monitoreo de la copia de archivos.</p> <ul style="list-style-type: none">- En el caso de la transferencia de unidades de almacenamiento portátiles, estas políticas se encuentran en las sección Configuración para controlar la actividad de dispositivos USB, y Gestionar la autorización para el uso de dispositivos externos. Estas políticas permiten el bloqueo cuando se incumple la configuración de la política establecida para estos dispositivos y, en algunos casos, incluso impiden la detección de los mismos.- Para abordar las situaciones en las que la información se filtra a través de dispositivos de impresión, se ha implementado una configuración que supervisa y genera alertas cuando se realizan impresiones de archivos. Esta configuración se encuentra detallada en la sección Gestión y monitoreo de impresión.
--	--	--	---

Seguridad en base de datos	Evitar que los usuarios realicen acciones o transmitan datos a través de la red que puedan comprometer información confidencial, por ejemplo, bloqueando la copia de datos de bases de datos a hojas de cálculo u otras acciones que puedan exponer la información	<p>Las medidas implementadas en el procedimiento de seguridad para bases de datos y archivos confidenciales se pueden observar en las siguientes secciones:</p> <ul style="list-style-type: none"> - En la sección Desarrollo de políticas de archivos en el servidor, se detalla cómo verificar la información y cómo configurar políticas que determinen el nivel de riesgo asociado con una base de datos específica. - Además, en relación con los dispositivos, se han establecido políticas que se describen en la sección 4.5.4. Monitoreo de archivos compartidos, las cuales rastrean las actividades de copia o modificación de archivos compartidos en los dispositivos finales.
Monitorear y auditoria	Implementar sistemas de seguimiento para supervisar el acceso y la utilización de información sensible, además de	Esta herramienta permite la supervisión y el registro continuo de auditorías en cada una de sus secciones, lo que simplifica la detección de usuarios que no cumplen con las políticas predefinidas. Además, ofrece un monitoreo constante

		<p>llevar a cabo auditorías regulares para garantizar el cumplimiento de las políticas y detectar posibles fallos en la seguridad.</p>	<p>de las actividades en archivos, tanto confidenciales como públicos, lo que significa que se puede supervisar quién accede, modifica, elimina o comparte archivos en tiempo real.</p>
--	--	--	---

6. CONCLUSIONES

- La revisión de las fuentes bibliográficas fue de suma importancia para adquirir una comprensión precisa de los conceptos relacionados con la seguridad de la información. Esto resultó esencial para establecer una metodología que facilite la evaluación de riesgos en relación a los activos de información, con el objetivo de prevenir la fuga de datos en la entidad financiera COAC “Santa Anita Ltda.”.
- La evaluación de la situación actual de la entidad financiera, en la que se identifica el sistema de gestión basado en procesos utilizado para la administración de sus departamentos, resultó ser beneficioso para determinar los procedimientos que han sido el enfoque del trabajo de tesis. Dentro de este contexto, se logró identificar los activos de información.
- En consecuencia, se optó por emplear la metodología MAGERIT, que permite llevar a cabo una evaluación completa de los riesgos al contemplar todos los recursos de información administrados por la entidad financiera. Esta metodología implica la evaluación de aspectos de seguridad como la disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad, con el propósito de determinar el nivel de importancia de cada recurso de información en una matriz específica. Esto, a su vez, contribuye a establecer el grado de criticidad de cada activo de información.
- Durante la ejecución del análisis de riesgos y la clasificación de la información en la entidad financiera, se han introducido manuales para poner en práctica la metodología de seguridad propuesta. Esta metodología ha sido estructurada mediante la formulación de directrices y prácticas, lo que nos ha permitido establecer las políticas necesarias con el fin de evitar la fuga de información. Para la elaboración de estas políticas, se ha tomado como

punto de partida la norma ISO/IEC 27002:2022, con un enfoque especial en su sección 5.12, que proporciona una serie de recomendaciones para la gestión de activos de información. Esta sección ha resultado fundamental para llevar a cabo la clasificación de la información, tomando en consideración las necesidades de seguridad de la organización, y teniendo en cuenta aspectos como la confidencialidad, integridad, disponibilidad y los requisitos pertinentes de las partes interesadas. Por otro lado, la sección 8.12 de la norma, dedicada a la Prevención de fuga de datos, aborda la necesidad de implementar medidas de prevención de fuga de datos en sistemas, redes y cualquier otro dispositivo que maneje, almacene o transmita información confidencial.

- Se creó una guía utilizando la plataforma ManageEngine, la cual se centra en la Prevención de Pérdida de Datos (DLP). Esta herramienta DLP nos brinda la capacidad de respaldar los estándares de seguridad. A través de esta plataforma, se implementaron políticas de seguridad que trabajan en conjunto con la metodología de seguridad propuesta. De esta manera, pudimos demostrar cómo ciertas herramientas pueden desempeñar un papel eficaz en las estrategias de seguridad de la información en la entidad financiera, permitiendo la adopción de medidas preventivas contra la fuga de datos.

7. RECOMENDACIONES

- Dentro del contexto de las normas ISO/IEC 27001, se definen los criterios necesarios para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Esta norma se sustenta en un enfoque basado en procesos, lo que implica que se aconseja que las organizaciones establezcan y documenten procesos para gestionar la seguridad de la información de forma consistente. Esta norma interactúa de manera complementaria con ISO/IEC 27002:2022, lo que es relevante, ya que nos permite establecer directrices y controles de seguridad detallados, facilitando así una implementación más eficaz de medidas de seguridad y asegurando que las entidades cumplan con los estándares y requisitos en materia de seguridad de la información.
- En la norma ISO/IEC 27002:2022, se describen diversos controles, y es importante reconocer que no todas las directrices serán relevantes para todas las entidades. Se recomienda evaluar cuáles de estos controles son necesarios para las entidades y adaptarlos en función del contexto específico de la organización.
- En la actualidad, el uso de herramientas de prevención de pérdida de datos (Data Loss Prevention, DLP) permite la implementación de políticas de seguridad destinadas a prevenir la fuga de información. Por tanto, es recomendable que en investigaciones o proyectos futuros se investigue la viabilidad de emplear una herramienta DLP en entornos de nube. El objetivo principal de esta exploración es garantizar la seguridad de la información, lo cual, a su vez, asegurará la protección de datos críticos y la confidencialidad de la información en entornos de nube. Esto permitirá mantener un alto nivel de seguridad para las organizaciones.

8. REFERENCIAS

Abg. Cuarán Betty. (2021). *Acuerdo-No.- 006-2021 Política-de-Ciberseguridad*.

<https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf>

Aguilera López. (2011). *Introducción a la seguridad informática (Seguridad informática)* .

https://books.google.com.ec/books?id=jofTAAQBAJ&printsec=frontcover&dq=Seguridad+Inform%C3%A1tica+aguilera&hl=es&sa=X&redir_esc=y#v=onepage&q=Seguridad%20Inform%C3%A1tica%20aguilera&f=false

Alkilani, H., Nasereddin, M., Hadi, A., & Tedmori, S. (2019). Data exfiltration techniques and data loss prevention system. *Proceedings - 2019 International Arab Conference on Information Technology, ACIT 2019*, 124–127.

<https://doi.org/10.1109/ACIT47987.2019.8991131>

Baca Urbina Gabriel. (2016). *Introducción a la seguridad informática* .

https://books.google.com.ec/books?id=IhUhDgAAQBAJ&printsec=frontcover&dq=amenazas+riesgos+y+vulnerabilidad+ciberseguridad&hl=es&sa=X&redir_esc=y#v=onepage&q&f=false

Bijani Chiquero Gopal. (2017). *UF1863 - Instalación y configuración de dispositivos y servicios de conectividad asociados*.

https://books.google.com.ec/books?id=SbpWDwAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Bottini Claudio. (2022, January 24). *Seguridad en la Nube - AVANZADA* . RedUSERS.

<https://books.google.com.ec/books?id=i6FaEAAAQBAJ&pg=PT5&dq=soluciones+dlp&hl>

=es&sa=X&ved=2ahUKEwjz4OvL-sT-

AhUkSjABHYIbBeEQ6AF6BAgJEAI#v=onepage&q=soluciones%20dlp&f=false

Brian Svidergol, & Robert Clements. (2019, June 12). *Microsoft 365 Mobility and Security* .

https://books.google.com.ec/books?id=ucqcDwAAQBAJ&pg=PT327&dq=que+es+data+loss+prevention&hl=es&sa=X&ved=2ahUKEwjNsM39_Jz-

AhV8RTABHRKgDlw4KBD0AXoECA0QAg#v=onepage&q=que%20es%20data%20loss%20prevention&f=false

Cooperativa de Ahorro y Crédito Santa Anita Ltda. (2011). *Historia Santa Anita*.

<https://www.coacsantaanita.fin.ec/sitio/historia/>

Edwar Rodolfo Chalá Ibarra. (2020). *Propuesta de un Modelo de Seguridad para la prevención de pérdida de información sensible dirigido a la Asamblea Nacional*.

Gestión de incidencias. (2014).

https://extranet.who.int/lqsi/sites/default/files/attachedfiles/LQMS%2014%20Occurrence%20management_2.pdf

ISMS. (2022). <https://www.isms.online/iso-27002/control-8-12-data-leakage-prevention/>

ISO 27001. (2013). ISO Tools. <https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/>

ISO/IEC 27000. (2018). <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>

ISO/IEC 27002. (2022a). <https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en>. Online Browsing Platform (OBP).

ISO/IEC 27002. (2022b). <https://www.iso.org/standard/75652.html>

ISO/IEC TS 27110. (2021). <https://www.iso.org/obp/ui/#iso:std:iso-iec:ts:27110:ed-1:v1:en>

Ley Orgánica de Protección de datos personales. (2021). LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES. ASAMBLEA NACIONAL, Año II-Nº 459-70.

Liwei Ren. (2013, May). *DLP Systems: Models, Architecture and Algorithms*.

https://www.researchgate.net/publication/304080339_DLP_Systems_Models_Architecture_and_Algorithms

MAGERIT – versión 3.0 Libro I - Método. (2012).

MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (2012, October).

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

ManageEngine Browser Security Plus. (2023). <https://www.manageengine.com/latam/browser-security/ayuda/requisitos-del-sistema.html>

ManageEngine DataSecurity Plus. (2023). *Arquitectura*. www.datasecurityplus.com

ManageEngine DataSecurity Plus . (2023). <https://www.manageengine.com/data-security/index.html?topMenu>

ManageEngine DataSecurity Plus Store. (n.d.). Retrieved January 13, 2024, from <https://store.manageengine.com/data-security/>

Martínez Miguel Ángel DLP, T., & Martínez Miguel Ángel, T. (n.d.). *Universidad Piloto de Colombia DLP: PREVENCIÓN DE FUGA DE INFORMACIÓN (DATA LOSS*

PREVENTION). Retrieved April 24, 2023, from <http://www.symantec.com>.

Ministerio de Industria y Comercio de España. (2017). *Tecnología de la Información Técnicas de seguridad Código de prácticas para los controles de seguridad de la información*.

Ministerio de Tecnologías de la Información y Comunicaciones de COLOMBIA. (2016).

Seguridad y Privacidad de la Información.

- Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., Murillo Quimiz, Á. L., & Castillo Merino, M. A. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. *Introducción a La Seguridad Informática y El Análisis de Vulnerabilidades*.
<https://doi.org/10.17993/INGYTEC.2018.46>
- Romo Daniel, & Valarezo Joffre. (2012). *Análisis e Implementación de la Norma ISO 27002 para el departamento de Sistemas de la Universidad Politécnica Salesiana Sede Guayaquil*.
<https://dspace.ups.edu.ec/bitstream/123456789/3163/1/UPS-GT000319.pdf>
- Ruiz Larrocha Elena. (2017). *Nuevas tendencias en los sistemas de información*. Ramón Areces.
https://books.google.com.ec/books?id=6ZVADwAAQBAJ&printsec=frontcover&dq=Nuevas+tendencias+en+los+sistemas+de+informaci%C3%B3n&hl=es&sa=X&redir_esc=y#v=onepage&q=Nuevas%20tendencias%20en%20los%20sistemas%20de%20informaci%C3%B3n&f=false
- Safetica NXT*. (2023, January 15). <https://www.safetica.com/products-safetica-nxt>
- Sealpath. (2020, June 22). *Protegiendo la información en sus tres estados*. Sealpath.
https://www.sealpath.com/es/blog/tres_estados_info/
- Singh, K. P., Rishiwal, V., & Kumar, P. (2018). Classification of Data to Enhance Data Security in Cloud Computing. *Proceedings - 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages, IoT-SIU 2018*. <https://doi.org/10.1109/IOT-SIU.2018.8519934>
- Sistema de gestión por procesos (BPM)*. (2020, March 18). <https://www.ambitbst.com/blog/qu%C3%A9-es-un-sistema-de-gesti%C3%B3n-por-procesos-bpm>

Stallings William. (2018, July 20). *Effective Cybersecurity: A Guide to Using Best Practices and Standards* .

<https://books.google.com.ec/books?id=JMZIDwAAQBAJ&pg=PT590&dq=deep+content+inspection+2018&hl=es&sa=X&ved=2ahUKEwiHjqO958L-AhVxq4QIHcEKAXsQ6AF6BAgKEAI#v=onepage&q&f=false>

Superintendencia de Economía Popular y Solidaria. (2022). <https://www.seps.gob.ec/wp-content/uploads/SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.pdf>.

Tahboub, R., & Saleh, Y. (2014). Data leakage/loss prevention systems (DLP). *2014 World Congress on Computer Applications and Information Systems, WCCAIS 2014*.
<https://doi.org/10.1109/WCCAIS.2014.6916624>

UIT-T X.800. (1996). <https://www.itu.int/rec/T-REC-X.800-199610-I!Amd1/es>

Universidad EAFIT. (n.d.). *NORMAS ISO Y SU COBERTURA*.

Vega Briceño, E. (2021). *SEGURIDAD DE LA INFORMACIÓN*.

Vega Briceño Edgar. (2020, March). *Planificación y ejecución de evaluaciones de seguridad informática desde un enfoque de Ethical Hacking*.

https://books.google.com.ec/books?id=D9DWDwAAQBAJ&printsec=frontcover&dq=Planificaci%C3%B3n+y+ejecuci%C3%B3n+de+evaluaciones+de+seguridad+inform%C3%A1tica+desde+un+enfoque+de+Ethical+Hacking&hl=es&sa=X&redir_esc=y#v=onepage&q=Planificaci%C3%B3n%20y%20ejecuci%C3%B3n%20de%20evaluaciones%20de%20seguridad%20inform%C3%A1tica%20desde%20un%20enfoque%20de%20Ethical%20Hacking&f=false

Villamizar Carlos. (2023). *Cambios de la actualización de la norma ISO 27002:2022 / GSS.*

<https://www.globalsuitesolutions.com/es/cambios-norma-iso-27002-2022/>

Wáshington Marcelo Contero Ramos. (2019). *Diseño de una política de seguridad de la información basada en la norma ISO 27002:2013, para el Sistema de botones de seguridad del Ministerio del Interior.*

Yandún Marco, & Cando Eduardo Patricio. (2018). Fuga de información confidencial en las instituciones financieras y uso de data Loss Prevention. *Universidad Politécnica Estatal Del Carchi.*

Yuya, J. O., & Ramani, R. (2017). Context-Aware Data Loss Prevention for Cloud Storage Services. *IEEE.*

9. ANEXOS

9.1.ANEXOS A Entrevista para levantamiento de información de activos de información

El propósito de esta entrevista es recopilar la información necesaria sobre la gestión de los procedimientos de cartera de la COAC "Santa Anita Ltda."

Objetivo: Obtener información sobre los activos de información en el proceso de recuperación operativa de cartera, donde se evaluará la gestión de riesgos.

Activos de información relacionados con el procedimiento de cartera:

- a) Enumeración de los sistemas o plataformas utilizados para gestionar la cartera de clientes.
- b) ¿Hay bases de datos específicas destinadas al almacenamiento de información relacionada con el proceso recuperación operativa la cartera?
- c) ¿Cuáles son los documentos o registros físicos empleados en el proceso de recuperación operativa de cartera?
- d) ¿Cuáles son los documentos o registros digitales utilizados en el proceso de recuperación operativa cartera?

Acceso y control de los activos de información:

- a) ¿Quiénes tienen acceso a los sistemas o plataformas utilizadas en la gestión de recuperación operativa de cartera?
- b) ¿Se implementa un control de acceso basado en roles o privilegios para asegurar la seguridad de la información?
- c) ¿Se realiza alguna auditoría o seguimiento de los accesos a los activos de información relacionados con la recuperación operativa de cartera?

Respaldo y recuperación de los activos de información:

- a) ¿Se efectúa un respaldo periódico de los datos almacenados en los sistemas o plataformas relacionados con la recuperación operativa cartera?
- b) ¿Existen políticas o procedimientos establecidos para la recuperación de los activos de información en caso de fallos o desastres

Medidas de seguridad de los activos de información:

- a) ¿Qué medidas de seguridad se aplican para proteger los sistemas y plataformas utilizados en la gestión de recuperación operativa cartera?
- b) ¿Se utilizan soluciones de seguridad como firewalls, sistemas de detección de intrusiones, antivirus, u software Data Loss Prevention (Prevención de fuga de información)?
- c) ¿Se emplean controles de encriptación de datos para salvaguardar la confidencialidad de la información?

Actualizaciones y mejoras de los activos de información:

- a) ¿Se llevan a cabo actualizaciones periódicas de los sistemas y plataformas relacionados con la cartera
- b) ¿Se realizan evaluaciones de seguridad para identificar posibles vulnerabilidades y mejorar la protección de los activos de información?

9.2.ANEXOS B. Entrevista la Infraestructura Tecnológica COAC “Santa Anita”

La entrevista pretende obtener la información necesaria sobre la infraestructura tecnológica en la COAC "Santa Anita Ltda.", para conocer más completo el contexto actual de los activos tecnológicos.

Objetivo: Conocer información sobre la infraestructura tecnológica actual en la entidad financiera COAC "Santa Anita".

- a) ¿Cada departamento de COAC "Santa Anita Ltda." es responsable de su propio departamento de tecnología?
- b) ¿Qué bases de datos se utilizan?
- c) ¿Qué sistemas operativos utilizan los servidores de aplicaciones?
- d) ¿Qué marcas de dispositivos son utilizados en la red? (Cisco, Alcatel, 3Com, etc.)?
- e) ¿Se tiene estándares de configuraciones para los equipos?
- f) ¿Se cuenta con políticas o procedimientos para actividades críticas? (respaldo de información, incidentes de seguridad, etc.)
- g) En cuanto al internet,
- h) El tipo de enlace a internet es: dedicado, ADSL, institucional u otro:
- i) Velocidad de transmisión del enlace a internet es:
- j) ¿A nivel Institucional se han realizado análisis de riesgos sobre TI?
- k) ¿Se han desarrollado capacitaciones sobre riesgos de TI?

9.3.ANEXOS C. Encuesta sobre la herramienta Data Loss Prevention

Encuesta dirigida al personal de COAC "Santa Anita Ltda." sobre las opciones disponibles para la herramienta de prevención de datos

Objetivo: Obtener perspectivas sobre el desempeño de la herramienta Data Loss Prevention, evaluando su nivel de importancia

Contexto

1. ¿Ha experimentado la organización incidente de pérdida de datos en el pasado?
 - a) Si
 - b) No

Requisitos de la herramienta DLP

2. ¿Cuál es el principal objetivo de implementar una herramienta de prevención de pérdida de datos (DLP) en la entidad financiera?
 - a) Proteger datos confidenciales de clientes o empleados.
 - b) Cumplir con regulaciones y leyes de privacidad de datos.
 - c) Evitar la filtración de información sensible.
 - d) Supervisar las actividades de los empleados para prevenir mal uso de datos.
 - e) Otro (especificar):
3. ¿Es necesario que la plataforma cumpla con las normativas de privacidad y protección de información?
 - a) Si
 - b) No
4. ¿La herramienta debe ser compatible con las versiones de sistemas operativos?
 - a) Linux

- b) iOS
5. ¿La herramienta debe poder clasificar y etiquetar datos confidenciales?
- a) Si
 - b) No

Características Deseadas

6. Por favor, indique las características que considera más importantes en una herramienta DLP (Seleccionar todas las opciones que apliquen)
- a) Detección y clasificación de datos sensibles.
 - b) Prevención de filtraciones y exfiltraciones de datos.
 - c) Monitoreo y registro de actividades de usuarios.
 - d) Integración con sistemas y aplicaciones existentes.
 - e) Reportes y análisis detallados.
 - f) Fácil configuración y gestión.
 - g) Otras características (especificar):
7. ¿La herramienta debe brindar la opción de crear y personalizar políticas de prevención de pérdida de datos?
- a) Si
 - b) No
8. ¿Debe poder integrarse con los sistemas y aplicaciones existentes en la infraestructura de la entidad financiera?
- a) Si
 - b) No

Experiencias y Recomendaciones

c) ¿Ha tenido alguna experiencia previa con alguna herramienta de prevención de pérdida de datos (DLP)?

a) Si

b) No

En caso de afirmativo, ¿Cual?

9.4.ANEXOS D. Matriz Levantamiento Activos de la Información

IDENTIFICACIÓN BÁSICA DEL ACTIVO			PROPIEDADES DE SEGURIDAD DE LA INFORMACION				Tipo de Control	Conceptos Ciberseguridad	Capacidades Operativas	Dominios de seguridad
No.	Código de identificación del activo	Nombre del Activo de Información	1. Clas. Disponibilidad (Baja, Media, Alta o Muy Alta)	2. Clas. Confidencialidad (Clasificada, Reservada, Pública de Uso Interno, Pública)	3. Clas. Integridad (Baja, Media, Alta, Crítica)	4. Nivel de Criticidad (Clasificación del Nivel de Criticidad del activo de Información para la Alcaldía)				
1	ESGECO1/RM	Reportes de Mora	Alta	Pública Clasificada	Alta	Alta	#Preventivo #Detectivo	#Identidad	#Proteccion_Informacion	#Proteccion #Defensa
2	ESGECO2/CMA	Cartera en mora del Asesor	Alta	Pública Clasificada	Alta	Alta	#Preventivo #Detectivo	#Identidad	#Proteccion_Informacion	#Proteccion #Defensa
3	ESGECO3/HSC	Hoja de seguimiento del crédito	Alta	Pública Clasificada	Alta	Alta	#Preventivo #Detectivo	#Protector #Detector	#Proteccion_Informacion	#Proteccion #Defensa
4	ESGECO4/RLL	Registro de Llamadas	Baja	Pública Clasificada	Alta	Media	#Preventivo #Detectivo	#Identidad	#Proteccion_Informacion	#Proteccion #Defensa
5	ESGECO5/NG	Notificaciones gestionadas	Alta	Pública Clasificada	Alta	Alta	#Preventivo #Detectivo	#Identidad	#Proteccion_Informacion	#Proteccion #Defensa
6	ESGECO6/RP	Reporte de primera notificación de pago	Media	Pública Clasificada	Alta	Alta	#Preventivo #Detectivo	#Identidad	#Proteccion_Informacion	#Proteccion #Defensa

7	ESGECO8/NM	Notificación de morosidad	Media	Pública Clasificada	Alta	Alta	#Preventivo #Detectivo	#Protector #Detector	#Proteccion_Informacion	#Proteccion #Defensa
8	ESGECO9/NG	Notificación al garante	Media	Pública Clasificada	Alta	Alta	#Preventivo #Detectivo	#Protector #Detector	#Proteccion_Informacion	#Proteccion #Defensa
9	ESGECO10/CP	Compromiso de Pago	Media	Pública Clasificada	Alta	Alta	#Preventivo #Detectivo	#Identidad	#Proteccion_Informacion	#Proteccion #Defensa
10	ESGECO11/ACV	Anexos de créditos vinculados	Media	Pública Clasificada	Alta	Alta	#Preventivo #Detectivo	#Protector #Detector	#Proteccion_Informacion	#Proteccion #Defensa
11	DBGECO1/ADP	Anexo de Depósitos a Plazo Fijo	Media	Pública Clasificada	Alta	Alta	#Preventivo #Detectivo	#Protector #Detector	#Proteccion_Informacion	#Proteccion #Defensa
12	DBGECO2/AAV	Anexo de Ahorros a la vista	Media	Pública Clasificada	Alta	Alta	#Preventivo #Detectivo	#Protector #Detector	#Proteccion_Informacion	#Proteccion #Defensa
13	DBGECO3/BDC	Base de Datos de Clientes en Mora	Media	Pública Clasificada	Alta	Alta	#Preventivo #Detectivo	#Protector #Detector	#Proteccion_Informacion	#Proteccion #Defensa

9.5.ANEXOS E. Valoración de activos para COAC “Santa Anita Ltda”

Documento para anexar a la documentación de seguridad del sistema que se presenta para conseguir la aprobación o autorización de la autoridad responsable del sistema de información.

Datos del sistema sujeto a análisis:

Código: COAC

Nombre: Gestión de Riesgos

Descripción: Datos administrativos:

- Organización: COAC "Santa Anita Ltda."
- Descripción: Análisis de riesgo en procedimiento recuperación operativa
- Autor: María José Cauja
- Versión: 1
- Fecha: 24 de junio 2023
- Responsable del Sistema: Ing. Freddy Cauja

Dimensiones de valoración

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos
- [V] Valor (ej. vidas humanas, patrimonio corporativo, etc.)
- [DP] Datos personales

Valoración de los activos

capa: [B] Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]	[DP]
[ESGECO1/RM] Reporte de Mora	[9] ⁽¹⁾	[9] ⁽²⁾	[9] ⁽³⁾	[4] ⁽⁴⁾	[9] ⁽⁵⁾	[7]
[ESGECO2/CMA] Cartera en mora del Asesor	[8]	[10]	[8]	[6] ⁽⁶⁾	[8]	[7]
[ESGECO3/HSC] Hoja de seguimiento del crédito	[8]	[8]	[8]	[5] ⁽⁷⁾	[5]	[7]

[ESGECO4/RLL] Registro de llamadas	[9]	[10]	[10]	[9] ⁽⁸⁾	[6]	[7]
[ESGECO5/NG] Notificaciones Gestionadas	[8]	[9]	[9]	[4] ⁽⁹⁾	[7]	[7] ⁽¹⁰⁾
[ESGECO6/RP] Reporte de la primera notificación de pago	[9]	[9]	[8]	[7]	[7]	[7]
[ESGECO8/NM] Notificación de morosidad	[8]	[10]	[10]	[9]	[7]	[7]
[ESGECO9/NG] Notificación al garante	[7]	[10]	[10]	[6]	[8]	[7]
[ESGECO10/CP] Compromiso de pago	[10]	[10]	[10]	[10]	[7]	[7]
[ESGECO11/ACV] Anexos de créditos vinculados	[9] ⁽¹¹⁾	[10] ⁽¹²⁾	[8] ⁽¹³⁾	[9]	[9] ⁽¹⁴⁾	[7]
[DBGECO1/ADP] Anexo de Depósitos a Plazo Fijo	[8] ⁽¹⁵⁾	[10] ⁽¹⁶⁾	[8] ⁽¹³⁾	[8]	[5] ⁽¹⁷⁾	[7]
[DBGECO2/AAV] Anexo de Ahorros a la vista	[8] ⁽¹⁸⁾	[10] ⁽¹⁹⁾	[9] ⁽¹⁴⁾	[8]	[8] ⁽²⁰⁾	[8] ⁽¹³⁾
[DBGECO3/BDC] Base de Datos de Clientes en Mora	[8]	[8]	[9]	[8]	[7]	[8]

- (1) [5] probablemente sea causa de incumplimiento de una ley o regulación
- [1] pudiera causar el incumplimiento leve o técnico de una ley o regulación
- [9] de enorme interés para la competencia
- [9] causa de pérdidas económicas excepcionalmente elevadas
- [9] causa de muy significativas ganancias o ventajas para individuos u organizaciones
- [9] constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
- [7] causa de graves pérdidas económicas
- [7] constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros

[9] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones

[7] Probablemente tenga un gran impacto en otras organizaciones

[9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística

[9] probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre

Pérdida de Confianza (Reputación):

[9] Reservado

[8] Confidencial

[7] Confidencial

[6] Difusión Limitada

(2) [6] probablemente afecte gravemente a un grupo de individuos

[7] probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves

[3] Probablemente cause la interrupción de actividades propias de la Organización

[5] Puede causar un significativo malestar público

[7] probablemente impediría la operación efectiva de la Organización

[9] a las relaciones con el público en general

[9] Reservado

[8] podría amenazar seriamente la integridad física de uno o más individuos

(3) [4] probablemente afecte a un grupo de individuos

[9] probablemente cause un incumplimiento excepcionalmente grave de una ley o

regulación

[9] probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios

[3] Probablemente cause la interrupción de actividades propias de la Organización

[7] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

[7] probablemente impediría la operación efectiva de la Organización

[3] Probablemente afecte negativamente a las relaciones internas de la Organización Nacional

[9] Reservado

(4) [4] probablemente afecte a un grupo de individuos

(5) [4] probablemente afecte a un grupo de individuos

[9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística

Persecución de Delitos:

(6) [6] probablemente afecte gravemente a un grupo de individuos

[1] Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)

(7) [3] probablemente afecte a un individuo

[5] Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local

(8) [5] probablemente quebrante seriamente leyes o regulaciones

[7] probablemente sea causa de un grave incidente de seguridad o dificulte la

investigación de incidentes graves

[9] constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros

(9) [2] pudiera causar molestias a un individuo

[3] probablemente impediría la operación efectiva de una parte de la Organización

[4] podría lesionar a varios individuos

(10) [7] Confidencial

(11) [6] probablemente afecte gravemente a un grupo de individuos

[9] probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación

[7] constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros

[7] por afectar gravemente a las relaciones con el público en general

[8] Confidencial

[4] podría lesionar a varios individuos

(12) [10] probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios

[9] probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre

(13) [8] Confidencial

(14) [9] Reservado

(15) [6] probablemente afecte gravemente a un grupo de individuos

[3] probablemente sea causa de incumplimiento leve o técnico de una ley o

regulación

[7] causa de graves pérdidas económicas

[7] probablemente impediría la operación efectiva de la Organización

[8] Confidencial

(16) [10] probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios

[9] de enorme interés para la competencia

[8] Confidencial

(17) [5] probablemente afecte gravemente a un individuo

(18) [3] probablemente afecte a un individuo

[7] probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves

[4] Puede causar malestar público

[7] probablemente impediría la operación efectiva de la Organización

[7] por afectar gravemente a las relaciones con otras organizaciones

[8] Confidencial

[7] podría lesionar gravemente a varios individuos

(19) [10] probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios

[9] de enorme interés para la competencia

[9] Reservado

(20) [7] probablemente cause un incumplimiento grave de una ley o regulación

[8] Confidencial

capa: [IS] Servicios internos

activo	[D]	[I]	[C]	[A]	[T]	[DP]
[ISGECO1/INT] Acceso a internet	[9] ⁽¹⁾	[9] ⁽²⁾	[9] ⁽³⁾	[9] ⁽⁴⁾	[9] ⁽⁵⁾	n.a.
[ISGECO2/PW] Portal Web- Intranet	[10]	[10]	[5]	[5]	[7]	n.a.

- (1) [1] Pudiera causar la interrupción de actividades propias de la Organización
 [9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
 [7] probablemente impediría la operación efectiva de la Organización
- (2) [3] Probablemente cause la interrupción de actividades propias de la Organización
 [9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
 [1] pudiera impedir la operación efectiva de una parte de la Organización
- (3) [9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
- (4) [9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
 [3] probablemente impediría la operación efectiva de una parte de la Organización
- (5) [9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
 [7] RTO < 4 horas

capa: [E] Equipamiento

activo	[D]	[I]	[C]	[A]	[T]	[DP]
[HWGECO1/SBD] Servidor Base de Datos	[10] ⁽¹⁾	[10] ⁽²⁾	[10] ⁽³⁾	[8]	[9] ⁽⁴⁾	[8] ⁽⁵⁾

[HWGECO2/PTR] Puesto de trabajo	[7] ⁽⁶⁾	[7] ⁽⁷⁾	[9] ⁽⁸⁾	[9] ⁽⁸⁾	[9] ⁽⁹⁾	n.a.
[HWGECO3/SPW] Servidor de portal web	[10] ⁽¹⁰⁾	[10] ⁽¹¹⁾	[9] ⁽¹²⁾	[8]	[9] ⁽¹³⁾	n.a.
[HWGECO4/FIR] Firewall	[10]	[10] ⁽¹⁴⁾	[10] ⁽¹⁵⁾	[9]	[9] ⁽¹⁶⁾	[9] ⁽⁴⁾
[HWGECO6/SCF] Servidor Core Financiero	[7]	[10] ⁽¹⁷⁾	[9] ⁽¹⁸⁾	[9]	[9] ⁽¹⁹⁾	[8] ⁽²⁰⁾
[COMGECO1/DM] Dispositivos Moviles	[9] ⁽²¹⁾	[9] ⁽²²⁾	[7] ⁽²³⁾	[9] ⁽²¹⁾	[9] ⁽²¹⁾	[7] ⁽²³⁾
[COMGECO2/LAN] Red Local	[10]	[10] ⁽²⁴⁾	[9] ⁽²¹⁾	[8]	[9] ⁽²⁵⁾	[4] ⁽²⁶⁾
[AUXGECO1/VEH] Vehículos	[7] ⁽²⁷⁾	[6] ⁽²⁸⁾	[9] ⁽²⁹⁾	[7]	[7] ⁽⁷⁾	[4]
[AUXGECO2/EC] Equipo Climatización	[7] ⁽³⁰⁾	[7] ⁽³¹⁾	[7] ⁽⁶⁾	[7] ⁽⁶⁾	[7] ⁽³⁰⁾	n.a.
[AUXGECO3/GE] Generador Eléctrico	[7] ⁽⁶⁾	[7] ⁽⁶⁾	[7] ⁽⁶⁾	[7] ⁽³⁰⁾	[7] ⁽³⁰⁾	n.a.
[AUXGECO4/CF] Caja Fuerte	[7] ⁽³²⁾	[7] ⁽⁶⁾	[7] ⁽⁶⁾	[7] ⁽⁶⁾	[7] ⁽³⁰⁾	n.a.
[AUXGECO5/CD] Cableado de Datos	[7] ⁽³³⁾	[7] ⁽⁶⁾	[7] ⁽⁶⁾	[7] ⁽²³⁾	[7] ⁽³⁰⁾	n.a.
[SWGECO1/CFF] Core Financiero (Financial)	[9] ⁽³⁴⁾	[7] ⁽³⁵⁾	[7] ⁽³⁶⁾	[9] ⁽³⁷⁾	[7] ⁽³⁸⁾	[9] ⁽³⁹⁾
[SWGECO2/OFFICE] OFFICE365	[9] ⁽⁴⁰⁾	[7] ⁽⁴¹⁾	[7] ⁽⁴¹⁾	[7] ⁽⁴¹⁾	[7] ⁽⁴²⁾	[7] ⁽⁴³⁾

(1) [6] probablemente afecte gravemente a un grupo de individuos

[10] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística

[5] Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local

[9] Reservado

[10] podría causar la pérdida de muchas vidas humanas

(2) [10] probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios

[9] Probablemente cause un daño serio a la eficacia o seguridad de la misión

operativa o logística

[8] Confidencial

- (3) [10] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística

[8] Confidencial

- (4) [6] probablemente afecte gravemente a un grupo de individuos

[9] Reservado

- (5) [6] probablemente afecte gravemente a un grupo de individuos

[8] Confidencial

- (6) [7] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

[7] probablemente impediría la operación efectiva de la Organización

- (7) [7] probablemente impediría la operación efectiva de la Organización

- (8) [9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística

[7] probablemente impediría la operación efectiva de la Organización

- (9) [9] probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios

[9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística

- (10) [6] probablemente afecte gravemente a un grupo de individuos

[10] probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios

- [9] Probablemente tenga un serio impacto en otras organizaciones
- [7] probablemente impediría la operación efectiva de la Organización
- [5] Probablemente sea causa una cierta publicidad negativa
- [8] Confidencial
- [6] podría lesionar gravemente a un individuo
- (11) [9] probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
- [9] de enorme interés para la competencia
- [10] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
- [9] Reservado
- (12) [9] probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
- [9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
- [9] Reservado
- (13) [6] probablemente afecte gravemente a un grupo de individuos
- [9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
- [7] Probablemente causaría una publicidad negativa generalizada
- [8] Confidencial
- (14) [10] probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios

- (15) [6] probablemente afecte gravemente a un grupo de individuos
[10] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
[9] Reservado
- (16) [5] probablemente afecte gravemente a un individuo
[9] Probablemente tenga un serio impacto en otras organizaciones
[7] probablemente impediría la operación efectiva de la Organización
[9] Reservado
- (17) [10] probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
[9] Reservado
- (18) [6] probablemente afecte gravemente a un grupo de individuos
Seguridad:
[9] probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[7] probablemente impediría la operación efectiva de la Organización
[9] Reservado
[9] podría causar la pérdida de una o más vidas humanas
- (19) [9] Reservado

- (20) [6] probablemente afecte gravemente a un grupo de individuos
[8] Confidencial
[7] podría lesionar gravemente a varios individuos
- (21) [9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
- (22) [1] pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
- (23) [7] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
- (24) [10] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
[7] probablemente impediría la operación efectiva de la Organización
- (25) [6] probablemente afecte gravemente a un grupo de individuos
[9] probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[8] Confidencial
- (26) [2] pudiera causar molestias a un individuo
[4] Difusión Limitada

- (27) [5] probablemente afecte gravemente a un individuo
[5] de valor comercial significativo
- (28) [5] Probablemente cause un cierto impacto en otras organizaciones
[1] Pudiera causar una pérdida menor de la confianza dentro de la Organización
[6] podría lesionar gravemente a un individuo
- (29) [9] causa de pérdidas económicas excepcionalmente elevadas
- (30) [7] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[3] probablemente impediría la operación efectiva de una parte de la Organización
- (31) [7] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[5] probablemente impediría la operación efectiva de más de una parte de la Organización
[7] podría lesionar gravemente a varios individuos
- (32) [1] Pudiera causar la interrupción de actividades propias de la Organización
[7] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
- (33) [3] Probablemente cause la interrupción de actividades propias de la Organización
[7] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
- (34) [6] probablemente afecte gravemente a un grupo de individuos
[9] de enorme interés para la competencia

- (35) [6] probablemente afecte gravemente a un grupo de individuos
[7] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
- (36) [6] probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
[7] probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
[7] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
- (37) [7] probablemente cause un incumplimiento grave de una ley o regulación
[7] probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
[9] Reservado
[8] Confidencial
- (38) [6] probablemente afecte gravemente a un grupo de individuos
[7] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
- (39) [6] probablemente afecte gravemente a un grupo de individuos
[9] Reservado
[8] Confidencial
- (40) [6] probablemente afecte gravemente a un grupo de individuos
Seguridad:

[9] probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios

(41) [6] probablemente afecte gravemente a un grupo de individuos

[7] probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves

(42) [6] probablemente afecte gravemente a un grupo de individuos

[7] Probablemente tenga un gran impacto en otras organizaciones

(43) [5] probablemente afecte gravemente a un individuo

capa: [SS] Servicios subcontratados

activo	[D]	[I]	[C]	[A]	[T]	[DP]
[SSGECO1/ADSL] Conexión a Internet	[10]	[9] ⁽¹⁾	[9] ⁽²⁾	[8]	[9] ⁽²⁾	[6] ⁽³⁾
[SSGECO2/SAR] Servicio de Administración de Red	[10]	[9] ⁽⁴⁾	[9] ⁽²⁾	[8]	[9] ⁽⁵⁾	[8] ⁽⁶⁾

(1) [9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística

[7] probablemente impediría la operación efectiva de la Organización

(2) [9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística

(3) [3] probablemente afecte a un individuo

[6] Difusión Limitada

(4) [9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística

[7] Probablemente causaría una publicidad negativa generalizada

(5) [9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística

[8] Confidencial

(6) [6] probablemente afecte gravemente a un grupo de individuos

[8] Confidencial

capa: [L] Instalaciones

activo	[D]	[I]	[C]	[A]	[T]	[DP]
[LGECO1/DTEC] Departamento de tecnología	[8]	[7]	[10]	[10]	[7]	[7]
[LGECO2/OF] Oficinas	[9] ⁽¹⁾	[7] ⁽²⁾	[7] ⁽²⁾	[7] ⁽²⁾	[7] ⁽²⁾	[7] ⁽²⁾
[LGECO3/DCT] Data Center	[10]	[10] ⁽³⁾	[9] ⁽⁴⁾	[10] ⁽⁵⁾	[9] ⁽⁶⁾	[9] ⁽⁷⁾

(1) [9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística

(2) [7] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(3) [9] Probablemente tenga un serio impacto en otras organizaciones

[10] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística

(4) [9] probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios

[9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística

[7] probablemente impediría la operación efectiva de la Organización

[7] Probablemente causaría una publicidad negativa generalizada

[9] Reservado

- (5) [10] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística

[9] Reservado

- (6) [9] Probablemente tenga un serio impacto en otras organizaciones

[9] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística

[9] Reservado

- (7) [6] probablemente afecte gravemente a un grupo de individuos

[9] Reservado

capa: [P] Personal

activo	[D]	[I]	[C]	[A]	[T]	[DP]
[PGECO1/AC] Asesor de Crédito	[7]	[6]	[7]	[4]	[8]	[9] ⁽¹⁾
[PGECO4/RT] Responsable en Tecnología	[10]	[10] ⁽²⁾	[8] ⁽³⁾	[5]	[5]	[9]
[PGECO2/ADC] Administrador de Crédito	[9] ⁽⁴⁾	[10]	[9] ⁽⁵⁾	[7]	[5]	[9]
[PGECO3/ANC] Analista de Crédito	[8] ⁽⁶⁾	[9]	[10]	[8]	[5]	[9]

- (1) [9] causa de muy significativas ganancias o ventajas para individuos u organizaciones

[9] Reservado

- (2) [6] probablemente afecte gravemente a un grupo de individuos

[8] Confidencial

- 3 [8] Confidencial

- (4) [4] probablemente quebrante leyes o regulaciones
[9] causa de muy significativas ganancias o ventajas para individuos u organizaciones
[7] Confidencial
[8] podría amenazas seriamente la integridad física de uno o más individuos
- (5) [9] Reservado
[8] Confidencial
- (6) [4] probablemente afecte a un grupo de individuos
[3] probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
[8] Confidencial
[4] podría lesionar a varios individuos

9.6.ANEXOS F. Valoración de Amenazas para COAC “Santa Anita Ltda”

Amenazas	Nivel	D	I	C	A	T	DP
Activos Esenciales							
[N.*] Desastres naturales	0,1	100%					
[I.1] Fuego	0,5	100%					
[I.2] Daños por agua	0,5	50%					
[I.*] Desastres industriales	0,5	100%					
[I.3] Contaminación medioambiental	0,1	50%					
[I.4] Contaminación electromagnética	1	10%					
[I.5.1] Avería de origen lógico	1	50%					
[I.5.2] Avería de origen físico	1	50%					
[I.6] Corte del suministro eléctrico	1	100%					
[I.7] Condiciones inadecuadas de temperatura	1	100%					
[I.11] Emanaciones electromagnéticas (TEMPEST)	1			1%			
[E.8] Difusión de software dañino	1	10%	10%	10%			
[E.15] Alteración de la información	1		1%				
[E.18] Destrucción de la información	1	1%					
[E.19] Fugas de información	1			10%			
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%			
[E.21] Errores de mantenimiento / actualización de	10	1%	10%	50%			
[E.23] Errores de mantenimiento / actualización de	1	10%					
[E.24] Caída del sistema por agotamiento de recursos:	10	50%					
[E.25] Pérdida de equipos	5	100%		50%			
[A.5] Suplantación de la identidad	10		10%	50%	100%		
[A.6] Abuso de privilegios de acceso	10	1%	10%	50%			
[A.7] Uso no previsto	1	10%	1%	10%			
[A.8] Difusión de software dañino	1	100%	100%	100%			

[A.11] Acceso no autorizado	100	10%	10%	50%	[
[A.13] Repudio (negación de actuaciones)	1				50%
[A.22] Manipulación de programas	1	50%	100%	100%	
[A.23] Manipulación del hardware	0,5	50%		50%	
[A.24] Denegación de servicio	2	100%			
[A.25] Robo de equipos	5	100%		50%	
[A.26] Ataque destructivo	1	100%			
[PR. g1] 1. No facilitar la información en materia de protección de datos o no redactarla de forma accesible y fácil de entender	10				20%
[PR. g2] 2. Tratar datos inadecuados y excesivos para la finalidad del tratamiento	10				50%
[PR. g3] 3. Carecer de una base jurídica sobre la que se sustenten los tratamientos realizados sobre los datos	10				50%
[PR. g4] 4. Tratar datos personales con una finalidad distinta para la cual fueron recabados	10				90%
[PR. g5] 5. No disponer de una estructura organizativa, procesos y recursos para una adecuada gestión de la privacidad en la organización	10				20%
[PR. g6] 6. Almacenar los datos por periodos superiores a los necesarios para la finalidad del tratamiento y a la legislación vigente	10				50%
[PR. g7] 7. Realizar transferencias internacionales a países que no ofrezcan un nivel de protección adecuado	10				50%
[PR. g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados	10				100%

[PR. g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma	10	100%
[PR. g10] 10. Seleccionar o mantener una relación con un encargado de tratamiento sin disponer de las garantías adecuadas	10	90%
[PR. g11] 11. Carecer de mecanismos de supervisión y control sobre las medidas que regulan la relación con un encargado el tratamiento	10	90%
[PR. g12] 12. No registrar la creación, modificación o cancelación de las actividades de tratamiento efectuadas bajo su responsabilidad	5	50%
[PR. g13] 13. No llevar a cabo por parte del responsable del tratamiento una evaluación de impacto adecuada en los supuestos detallados por la normativa aplicable	5	50%
[PR. g24] 24. Información no actualizada o incorrecta (pe. registros duplicados con informaciones contradictorias o con campos de datos incorrectos)	10	50%
[PR.2g] Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales.	10	50%
[PR.2m] Accesos no autorizados a datos personales (modificación)	10	30%
[PR.2n] Accesos no autorizados a datos personales (lectura)	10	80%
Servicios internos		
[N.1] Fuego	0,1	100%
[N.2] Daños por agua	0,1	50%
[N.*] Desastres naturales	0,1	100%

[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	50%			
[I.4] Contaminación electromagnética	1	10%			
[I.5.2] Avería de origen físico	1	50%			
[I.6] Corte del suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura	1	100%			
[I.11] Emanaciones electromagnéticas (T	1			1%	
[E.23] Errores de mantenimiento / actualización;	1	10%			
[E.24] Caída del sistema por agotamiento	10	50%			
[E.25] Pérdida de equipos	1	20%		50%	
[A.7] Uso no previsto	1	10%			
[A.11] Acceso no autorizado	1	10%	10%	50%	
[A.23] Manipulación del hardware	0,5	100%			
Servicios internos					
[E.2] Errores del administrador del sistema	1	20%	20%	20%	
[E.15] Alteración de la información	1		1%		
[E.18] Destrucción de la información	1	10%			
[E.19] Fugas de información	1			10%	
[E.24] Caída del sistema por agotamiento d	10	50%			
[A.5] Suplantación de la identidad	10		50%	50%	100%
[A.6] Abuso de privilegios de acceso	10	1%	10%	50%	100%
[A.7] Uso no previsto	1	1%	10%	10%	
[A.11] Acceso no autorizado	100		10%	50%	100%
[A.13] Repudio (negación de actuaciones)	5				100%
[A.15] Modificación de la información	10		50%		
[A.18] Destrucción de la información	1	50%			
[4-24] Denegación de servicio	10	50%			
Equipamiento					
[N.1] Fuego	0,5	100%			
[N.2] Daños por agua	0,5	50%			

[N.*] Desastres industriales	0,5	100%			
[I.3] Contaminación medioambiental	0,1	-50%			
[I.4] Contaminación electromagnética	1	10%			
[I.5.1] Avería de origen lógico	1	50%			
[I.5.2] Avería de origen físico	1	50%			
[I.6] Corte del suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura	1	100%			
[I.11] Emanaciones electromagnética (TEMPEST)	1			1%	
[E.1] Errores de los usuarios	1	10%	10%	10%	
[E.2] Errores del administrador del sistema	1	20%	20%	20%	
[£.8] Difusión de software dañino	1	10%	10%	10%	
		-			
[£.15] Alteración de la información	1		1%		
[£-18] Destrucción de la información	1	10%			
[E.19] Fugas de información	1			10%	
[E.20] Vulnerabilidades de los programas	1	1%	20%	20%	
[E.21] Errores de mantenimiento	10	1%	10%	50%	
[E.23] Errores de mantenimiento	1	10%	10%	50%	
[E.24] Caída del sistema por agotamiento	10	50%			
[E.25] Pérdida de equipos	1	100%		100%	
[A.5] Suplantación de la identidad	1		50%	50%	100%
[A.6] Abuso de privilegios de acceso	1	10%	100%	100%	100%
[A.7] Uso no previsto	1	10%	10%	100%	
[A.8] Difusión de software dañino	1	100%	100%	100%	
[A.11] Acceso no autorizado	1	10%	100%	100%	100%
[A.13] Repudio (¡negación de actuación!	5				100%
[A.15] Modificación de la información	10		50%		
[A.18] Destrucción de la información	1	50%			
Servicios Subcontratados					
[1.8] Fallo de servicios de comunicaciones	1	100%			
[E.15] Alteración de la información	1		10%		
[E.18] Destrucción de la información	1	10%			

[E.19] Fugas de información	1			10%	
[A.5] Suplantación de la identidad	0,2		100%	100%	100%
[A.13] Repudio (negación de actuaciones)	1				100%
[A.15] Modificación de la información	1		50%		
[A.18] Destrucción de la información	1	50%			
[A.19] Revelación de información	1			50%	
[A.24] Denegación de servicio	1	50%			
Instalaciones					
[E.8] Difusión de software dañino	1	10%	10%	10%	
[E.9] Errores de [re-Encaminamiento	1			10%	
[E.10] Errores de secuencia	1		10%		
[E.15] Alteración de la información	1		10%		
[E.18] Destrucción de la información	1	1%			
[E.19] Fugas de información	1			10%	
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%	
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	10%	50%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%			
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	10	20%			
[E.28] Indisponibilidad del personal	1	20%			
[A.4] Manipulación de los ficheros de configuración	10	10%	10%	10%	
[A.5] Suplantación de la identidad	10		10%	50%	100%
[A.6] Abuso de privilegios de acceso	10	10%	10%	50%	
[A.7] Uso no previsto	1	10%	10%	10%	
[A.8] Difusión de software dañino	1	100%	100%	100%	
[A.9] [Re-Encaminamiento de mensajes	1			10%	
[A.10] Alteración de secuencia	1		10%		
[A.11] Acceso no autorizado	100	10%	10%	50%	100%

[A.12] Análisis de tráfico	1			2%
[A.13] Repudio (negación de actuaciones)	1			50%
[A-14] interceptación de información	1			10%
[A.15] Modificación de la información	1		50%	
[A:18] Destrucción de la información	1	50%		
[A.19] Revelación de información	10			50%
[A.22] Manipulación de programas	1	50%	100%	100%
[A.23] Manipulación del hardware	0,5	100%		50%
[A.24] Denegación de servicio	10	100%		
[A.25] Robo de equipos	10			100%
[A.26] Ataque destructivo	1	100%		
Personal				
A [E.8] Difusión de software dañino	1	10%	10%	10%
A [E.15] Alteración de la información	1		10%	
A [E.18] Destrucción de la información	1	1%		
A [E.19] Fugas de información	1			10%
A [E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%
A [E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	10%	50%
A [E.28] Indisponibilidad del personal	1	30%		
A [A.8] Difusión de software dañino	1	100%	100%	100%
A [A.13] Repudio (negación de actuaciones)	1			50%
A [A.15] Modificación de la información	1		50%	
A [A.18] Destrucción de la información	1	10%		
A [A.19] Revelación de información	10			50%
A [A.22] Manipulación de programas	1	50%	100%	100%
A [A.28] Indisponibilidad del personal	0,5	50%		
A [A.29] Extorsión	0,9	20%	10%	50%
A [A.30] Ingeniería social (picaresca)	0,5	20%	20%	20%
A [PR. g1] 1. No facilitar la información en materia de protección de datos o no	10			20%

redactarla de forma accesible y fácil de entender		
A [PR. g2] 2. Tratar datos inadecuados y excesivos para la finalidad del tratamiento	10	50%
A [PR. g3] 3. Carecer de una base jurídica sobre la que se sustenten los tratamientos realizados sobre los datos	10	50%
A [PR. g4] 4. Tratar datos personales con una finalidad distinta para la cual fueron recabados	10	90%
A [PR. g5] 5. No disponer de una estructura organizativa, procesos y recursos para una adecuada gestión de la privacidad en la organización	5	50%
A [PR. g6] 6. Almacenar los datos por periodos superiores a los necesarios para la finalidad del tratamiento y a la legislación vigente	10	50%
A [PR. g7] 7. Realizar transferencias internacionales a países que no ofrezcan un nivel de protección adecuado	10	90%
A [PR. g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados	10	100%
A [PR. g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma	10	100%
A [PR. g10] 10. Seleccionar o mantener una relación con un encargado de tratamiento sin disponer de las garantías adecuada	10	90%
A [PR. g11] 11. Carecer de mecanismos de supervisión y control sobre las medidas que regulan la relación con un encargado el tratamiento	10	90%

A [PR. g12] 12. No registrar la creación, modificación o cancelación de las actividades de tratamiento efectuadas bajo su responsabilidad	5	50%
A [PR. g13] 13. No llevar a cabo por parte del responsable del tratamiento una evaluación de impacto adecuada en los supuestos detallados por la normativa aplicable	5	50%
A [PR. g24] 24. Información no actualizada o incorrecta (pe. registros duplicados con informaciones contradictorias o con campos de datos incorrectos)	10	50%
A [PR.29] Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales.	10	50%

9.7.ANEXOS G. Análisis de Riesgo para COAC “Santa Anita Ltda”

- **Riesgo acumulado**

Se presentan los principales riesgos en cada dominio de seguridad del sistema en las diferentes fases de trabajo.

Amenaza: presenta la amenaza dentro del catálogo de PILAR. Una amenaza aparece cuando algún activo del sistema está expuesto a ella

D – dimensión: se muestra la dimensión (o dimensiones) de seguridad a las que afecta la amenaza

I – impacto: se muestra el máximo impacto causado por esta amenaza en algún activo del sistema

R – riesgo: se muestra el máximo riesgo al que está expuesto el sistema por causa de esta amenaza

amenaza	D	I	R
[A.11] Acceso no autorizado	C, A	[10]	{8,6}
[A.56] Retirada de objetos (a través del perímetro físico)	C	[10]	{8,6}
[A.3] Manipulación de los registros de actividad (log)	I	[9]	{8,1}

amenaza	D	I	R
[A.11] Acceso no autorizado	C, A	[10]	{8,6}
[A.56] Retirada de objetos (a través del perímetro físico)	C	[10]	{8,6}
[A.3] Manipulación de los registros de actividad (log)	I	[9]	{8,1}

amenaza	D	I	R
[A.11] Acceso no autorizado	A	[6]	{5,6}
[PR.g10] 10. Seleccionar o mantener una relación con un encargado de tratamiento sin disponer de las garantías adecuadas	DP	[6]	{4,9}

[PR.g7] 7. Realizar transferencias internacionales a países que no ofrezcan un nivel de protección adecuado	DP	[6]	{4,9}
[PR.g11] 11. Carecer de mecanismos de supervisión y control sobre las medidas que regulan la relación con un encargado el tratamiento	DP	[6]	{4,9}

amenaza	D	I	R
[A.11] Acceso no autorizado	A	[6]	{5,6}
[PR.g10] 10. Seleccionar o mantener una relación con un encargado de tratamiento sin disponer de las garantías adecuadas	DP	[6]	{4,9}
[PR.g7] 7. Realizar transferencias internacionales a países que no ofrezcan un nivel de protección adecuado	DP	[6]	{4,9}
[PR.g11] 11. Carecer de mecanismos de supervisión y control sobre las medidas que regulan la relación con un encargado el tratamiento	DP	[6]	{4,9}

- **Riesgo repercutido**

Se presentan los máximos riesgos a los que están expuestos los activos esenciales del sistema en cada fase de trabajo.

Activo: presenta el activo esencial que está en riesgo; es decir, sobre el que repercute indirectamente la amenaza

Amenaza: presenta la amenaza dentro del catálogo de PILAR.

D – dimensión: se muestra la dimensión (o dimensiones) de seguridad a las que afecta la amenaza

I – impacto: se muestra el máximo impacto causado por esta amenaza sobre el activo esencial

R – riesgo: se muestra el máximo riesgo al que está expuesto el activo esencial por causa de esta amenaza

ACTIVO	AMENAZA
ESENCIALES	
REPORTES	
[ESGECO1/RM] Reporte de Mora	[A.56] Retirada de objetos (a través del perímetro físico) [A.11] Acceso no autorizado [A.25] Robo de equipos [A.5] Suplantación de 3 la identidad [A.51] Inyección de código malicioso (a través de una frontera lógica) [E.24] Caída del sistema por agotamiento de recursos [A.55] Introducción de objetos (a través del perímetro físico) [A.6] Abuso de privilegios de acceso [E.21] Errores de mantenimiento / actualización de programas (software) [A.57] Acceso no autorizado (a través del perímetro físico) [A.15] Modificación de la información [PR. g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados [PR. g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma
[ESGECO2/CMA] Cartera en mora del Asesor	[A.11] Acceso no autorizado [A.56] Retirada de objetos (a través del perímetro físico) [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.25] Robo de equipos [A.15] Modificación de la información [A.51] Inyección de código malicioso (a través de una frontera lógica) [A.55] Introducción de objetos (a través del perímetro físico) [A.19] Revelación de información [E.25] Pérdida de equipos [E.21] Errores de mantenimiento / actualización de programas (software) [A.57] Acceso no autorizado (a través del perímetro físico) [PR. g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados [PR. g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma
[ESGECO3/HSC] Hoja de seguimiento del crédito	[A.56] Retirada de objetos (a través del perímetro físico) [A.11] Acceso no autorizado [A.25] Robo de equipos [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso

	[A.51] Inyección de código malicioso (a través de una frontera lógica)
	[A.55] Introducción de objetos (a través del perímetro físico)
	[A.15] Modificación de la información
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.19] Revelación de información
	[A.57] Acceso no autorizado (a través del perímetro físico)
	[PR. g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados
	[PR. g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma
[ESGECO4/RLL] Registro de llamadas	[A.11] Acceso no autorizado
	[A.56] Retirada de objetos (a través del perímetro físico)
	[A.5] Suplantación de la identidad
	[A.6] Abuso de privilegios de acceso
	[A.25] Robo de equipos
	[A.15] Modificación de la información
	[E.25] Pérdida de equipos
	[A.51] Inyección de código malicioso (a través de una frontera lógica)
	[A.55] Introducción de objetos (a través del perímetro físico)
	[A.19] Revelación de información
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.57] Acceso no autorizado (a través del perímetro físico)
	[A.24] Denegación de servicio
	[PR. g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados
[PR. g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma	
[ESGECO5/NG] Notificaciones Gestionadas	[A.56] Retirada de objetos (a través del perímetro físico)
	[A.11] Acceso no autorizado
	[A.25] Robo de equipos
	[A.6] Abuso de privilegios de acceso
	[A.5] Suplantación de la identidad
	[A.51] Inyección de código malicioso (a través de una frontera lógica)
	[A.55] Introducción de objetos (a través del perímetro físico)
	[A.15] Modificación de la información
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.19] Revelación de información
[A.57] Acceso no autorizado (a través del perímetro físico)	
[E.25] Pérdida de equipos	

	[PR. g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma
	[PR. g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados
[ESGECO6/RP] Reporte de la primera notificación de pago	[A.56] Retirada de objetos (a través del perímetro físico)
	[A.11] Acceso no autorizado
	[A.25] Robo de equipos
	[A.51] Inyección de código malicioso (a través de una frontera lógica)
	[A.55] Introducción de objetos (a través del perímetro físico)
	[A.15] Modificación de la información
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.57] Acceso no autorizado (a través del perímetro físico)
	[A.19] Revelación de información
	[PR. g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma
	[PR. g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados
	[A.24] Denegación de servicio
	[E.25] Pérdida de equipos
[ESGECO8/NM] Notificación de morosidad	[A.5] Suplantación de la identidad
	[A.5] Suplantación de la identidad
	[A.6] Abuso de privilegios de acceso
	[A.25] Robo de equipos
	[A.15] Modificación de la información
	[E.25] Pérdida de equipos
	[A.51] Inyección de código malicioso (a través de una frontera lógica)
	[A.55] Introducción de objetos (a través del perímetro físico)
	[A.19] Revelación de información
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.57] Acceso no autorizado (a través del perímetro físico)
	[PR. g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados
	[PR. g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma
[ESGECO9/NG] Notificación al garante	[A.56] Retirada de objetos (a través del perímetro físico)
	[A.5] Suplantación de la identidad
	[A.6] Abuso de privilegios de acceso
	[A.25] Robo de equipos
	[A.15] Modificación de la información

	[E.25] Pérdida de equipos
	[A.51] Inyección de código malicioso (a través de una frontera lógica)
	[A.55] Introducción de objetos (a través del perímetro físico)
	[A.19] Revelación de información
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.57] Acceso no autorizado (a través del perímetro físico)
	[PR. g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma
	[PR. g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados
[ESGECO10/CP] Compromiso de pago	[A.11] Acceso no autorizado
	[A.56] Retirada de objetos (a través del perímetro físico)
	[A.24] Denegación de servicio
	[E.25] Pérdida de equipos
	[A.5] Suplantación de la identidad
	[A.6] Abuso de privilegios de acceso
	[A.15] Modificación de la información
	[E.24] Caída del sistema por agotamiento de recursos
	[A.51] Inyección de código malicioso (a través de una frontera lógica)
	[A.55] Introducción de objetos (a través del perímetro físico)
	[A.19] Revelación de información
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.57] Acceso no autorizado (a través del perímetro físico)
	[PR. g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma
[PR. g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados	
[ESGECO11/ACV] Anexos de créditos vinculados	[A.11] Acceso no autorizado
	[A.56] Retirada de objetos (a través del perímetro físico)
	[A.5] Suplantación de la identidad
	[A.6] Abuso de privilegios de acceso
	[A.25] Robo de equipos
	[A.15] Modificación de la información
	[A.51] Inyección de código malicioso (a través de una frontera lógica)
	[A.55] Introducción de objetos (a través del perímetro físico)
	[A.19] Revelación de información
	[E.25] Pérdida de equipos
	[E.21] Errores de mantenimiento / actualización de programas (software)
[A.57] Acceso no autorizado (a través del perímetro físico)	

	[A.24] Denegación de servicio
	[PR. g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados
	[PR. g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma
ESENCIALES	
BASE DE DATOS	
[DBGECO1/ADP] Anexo de Depósitos a Plazo Fijo	[A.11] Acceso no autorizado
	[A.56] Retirada de objetos (a través del perímetro físico)
	[A.51] Inyección de código malicioso (a través de una frontera lógica)
	[A.55] Introducción de objetos (a través del perímetro físico)
	[A.19] Revelación de información
	[E.25] Pérdida de equipos
	[E.21] Errores de mantenimiento / actualización de programas (software)
[DBGECO2/AAV] Anexo de Ahorros a la vista	[A.57] Acceso no autorizado (a través del perímetro físico)
	[A.11] Acceso no autorizado
	[A.56] Retirada de objetos (a través del perímetro físico)
	[A.51] Inyección de código malicioso (a través de una frontera lógica)
	[A.55] Introducción de objetos (a través del perímetro físico)
	[A.19] Revelación de información
	[E.25] Pérdida de equipos
[DBGECO3/BDC] Base de Datos de Clientes en Mora	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.57] Acceso no autorizado (a través del perímetro físico)
	[A.56] Retirada de objetos (a través del perímetro físico)
	[A.51] Inyección de código malicioso (a través de una frontera lógica)
	[A.55] Introducción de objetos (a través del perímetro físico)
	[A.6] Abuso de privilegios de acceso
	[A.57] Acceso no autorizado (a través del perímetro físico)
[DBGECO1/ADP] Anexo de Depósitos a Plazo Fijo	[E.25] Pérdida de equipos
	[A.15] Modificación de la información
	[PR. g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados
	[PR. g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma
	[A.5] Suplantación de la identidad
	[A.6] Abuso de privilegios de acceso
	[A.25] Robo de equipos
	[A.15] Modificación de la información

	[PR. g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma
	[PR. g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados
[DBGECO2/AAV] Anexo de Ahorros a la vista	[A.5] Suplantación de la identidad
	[A.6] Abuso de privilegios de acceso
	[A.25] Robo de equipos
	[A.15] Modificación de la información
	[PR. g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados
	[PR. g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma
[DBGECO3/BDC] Base de Datos de Clientes en Mora	[A.25] Robo de equipos
	[A.5] Suplantación de la identidad
SERVICIOS INTERNOS	
[ISGECO2/PW] Portal Web-Intranet	[A.11] Acceso no autorizado
	[A.56] Retirada de objetos (a través del perímetro físico)
	[A.24] Denegación de servicio
	[E.25] Pérdida de equipos
	[A.5] Suplantación de la identidad
	[A.6] Abuso de privilegios de acceso
	[A.15] Modificación de la información
	[E.24] Caída del sistema por agotamiento de recursos
	[A.51] Inyección de código malicioso (a través de una frontera lógica)
	[A.55] Introducción de objetos (a través del perímetro físico)
	[A.19] Revelación de información
	[E.21] Errores de mantenimiento / actualización de programas (software)
[A.57] Acceso no autorizado (a través del perímetro físico)	
[ISGECO1/INT] Acceso a internet	[E.24] Caída del sistema por agotamiento de recursos
EQUIPAMIENTO	
EQUIPOS	
[HWGECO3/SPW] Servidor de portal web	[A.11] Acceso no autorizado
	[A.56] Retirada de objetos (a través del perímetro físico)
	[A.24] Denegación de servicio
	[E.25] Pérdida de equipos
	[A.5] Suplantación de la identidad
	[A.6] Abuso de privilegios de acceso
	[A.15] Modificación de la información
	[E.24] Caída del sistema por agotamiento de recursos
	[A.51] Inyección de código malicioso (a través de una frontera lógica)
	[A.55] Introducción de objetos (a través del perímetro físico)

	[A.19] Revelación de información	
	[E.21] Errores de mantenimiento / actualización de programas (software)	
	[A.57] Acceso no autorizado (a través del perímetro físico)	
[HWGECO4/FIR] Firewall	[A.24] Denegación de servicio	
	[E.25] Pérdida de equipos	
	[A.5] Suplantación de la identidad	
	[A.6] Abuso de privilegios de acceso	
	[A.15] Modificación de la información	
	[A.11] Acceso no autorizado	
	[A.56] Retirada de objetos (a través del perímetro físico)	
	[E.24] Caída del sistema por agotamiento de recursos	
	[A.51] Inyección de código malicioso (a través de una frontera lógica)	
	[A.55] Introducción de objetos (a través del perímetro físico)	
	[A.19] Revelación de información	
	[E.21] Errores de mantenimiento / actualización de programas (software)	
	[A.57] Acceso no autorizado (a través del perímetro físico)	
	[PR. g10] 10. Seleccionar o mantener una relación con un encargado de tratamiento sin disponer de las garantías adecuadas	
	[PR. g11] 11. Carecer de mecanismos de supervisión y control sobre las medidas que regulan la relación con un encargado el tratamiento	
	[PR.2n] Accesos no autorizados a datos personales (lectura)	
	[PR. g7] 7. Realizar transferencias internacionales a países que no ofrezcan un nivel de protección adecuado	
	[PR. g4] 4. Tratar datos personales con una finalidad distinta para la cual fueron recabados	
	[HWGECO6/SCF] Servidor Core Financiero	[A.51] Inyección de código malicioso (a través de una frontera lógica)
		[E.24] Caída del sistema por agotamiento de recursos
[A.55] Introducción de objetos (a través del perímetro físico)		
[A.19] Revelación de información		
[E.25] Pérdida de equipos		
[E.21] Errores de mantenimiento / actualización de programas (software)		
[A.57] Acceso no autorizado (a través del perímetro físico)		
[A.11] Acceso no autorizado		
[A.56] Retirada de objetos (a través del perímetro físico)		
[A.5] Suplantación de la identidad		
[A.6] Abuso de privilegios de acceso		
[A.25] Robo de equipos		
[A.15] Modificación de la información		

[HWGECO1/SBD] Servidor Base de Datos	[E.24] Caída del sistema por agotamiento de recursos
	[A.15] Modificación de la información
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.24] Denegación de servicio
[HWGECO2/PTR] Puesto de trabajo	[A.25] Robo de equipos
	[A.24] Denegación de servicio
	[A.19] Revelación de información
COMUNICACIONES	
[COMGECO2/LAN] Red Local	[A.11] Acceso no autorizado
	[A.56] Retirada de objetos (a través del perímetro físico)
	[A.24] Denegación de servicio
	[E.25] Pérdida de equipos
	[A.5] Suplantación de la identidad
	[A.6] Abuso de privilegios de acceso
	[A.15] Modificación de la información
	[E.24] Caída del sistema por agotamiento de recursos
	[A.51] Inyección de código malicioso (a través de una frontera lógica)
	[A.55] Introducción de objetos (a través del perímetro físico)
	[A.19] Revelación de información
	[E.21] Errores de mantenimiento / actualización de programas (software)
[A.57] Acceso no autorizado (a través del perímetro físico)	
[COMGECO1/DM] Dispositivos Móviles	[A.24] Denegación de servicio
	[E.24] Caída del sistema por agotamiento de recursos
ELEMENTOS AUXILIARES	
[AUXGECO1/VEH] Vehículos	[A.25] Robo de equipos
[AUXGECO2/EC] Equipo Climatización	[A.25] Robo de equipos
[AUXGECO3/GE] Generador Eléctrico	[A.25] Robo de equipos
APLICACIONES	
[SWGECO1/CFF] Core Financiero (Financial)	[E.21] Errores de mantenimiento / actualización de programas (software)
[SWGECO2/OFFICE] OFFICE365	[E.21] Errores de mantenimiento / actualización de programas (software)
SERVICIOS SUBCONTRATADOS	
[SSGECO2/SAR] Servicio de Administración de Red	[A.56] Retirada de objetos (a través del perímetro físico)
	[A.24] Denegación de servicio
	[E.25] Pérdida de equipos
	[E.24] Caída del sistema por agotamiento de recursos
	[A.51] Inyección de código malicioso (a través de una frontera lógica)

	[A.55] Introducción de objetos (a través del perímetro físico)
	[A.57] Acceso no autorizado (a través del perímetro físico)
INSTALACIONES	
[LGECO1/DTEC] Departamento de tecnología	[A.11] Acceso no autorizado
	[A.56] Retirada de objetos (a través del perímetro físico)
	[A.51] Inyección de código malicioso (a través de una frontera lógica)
	[E.24] Caída del sistema por agotamiento de recursos
	[A.55] Introducción de objetos (a través del perímetro físico)
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.19] Revelación de información
	[A.57] Acceso no autorizado (a través del perímetro físico)
	[A.24] Denegación de servicio
	[A.5] Suplantación de la identidad
	[A.6] Abuso de privilegios de acceso
	[A.25] Robo de equipos
	[E.25] Pérdida de equipos
[A.15] Modificación de la información	
[LGECO2/OF] Oficinas	[A.56] Retirada de objetos (a través del perímetro físico)
	[A.55] Introducción de objetos (a través del perímetro físico)
	[A.57] Acceso no autorizado (a través del perímetro físico)
	[A.19] Revelación de información
	[A.25] Robo de equipos
[LGECO3/DCT] Data Center	[A.11] Acceso no autorizado
	[A.56] Retirada de objetos (a través del perímetro físico)
	[E.24] Caída del sistema por agotamiento de recursos
	[A.51] Inyección de código malicioso (a través de una frontera lógica)
	[A.55] Introducción de objetos (a través del perímetro físico)
	[A.19] Revelación de información
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.57] Acceso no autorizado (a través del perímetro físico)
	[A.24] Denegación de servicio
	[E.25] Pérdida de equipos
	[A.5] Suplantación de la identidad
	[A.6] Abuso de privilegios de acceso
	[A.15] Modificación de la información
PERSONAL	
[PGECO1/AC] Asesor de Crédito	[A.56] Retirada de objetos (a través del perímetro físico)
	[A.25] Robo de equipos
	[A.51] Inyección de código malicioso (a través de una frontera lógica)
	[A.55] Introducción de objetos (a través del perímetro físico)

	[A.19] Revelación de información
	[A.57] Acceso no autorizado (a través del perímetro físico)
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[PR. g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma
	[PR. g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados
[PGECO4/RT] Responsable en Tecnología	[A.24] Denegación de servicio
	[E.25] Pérdida de equipos
	[A.5] Suplantación de la identidad
	[A.6] Abuso de privilegios de acceso
	[A.15] Modificación de la información
	[A.11] Acceso no autorizado
	[A.56] Retirada de objetos (a través del perímetro físico)
	[E.24] Caída del sistema por agotamiento de recursos
	[A.51] Inyección de código malicioso (a través de una frontera lógica)
	[A.55] Introducción de objetos (a través del perímetro físico)
	[A.19] Revelación de información
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.57] Acceso no autorizado (a través del perímetro físico)
	[PR. g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma
	[PR. g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados
[PGECO2/ADC] Administrador de Crédito	[A.11] Acceso no autorizado
	[A.56] Retirada de objetos (a través del perímetro físico)
	[A.5] Suplantación de la identidad
	[A.6] Abuso de privilegios de acceso
	[A.25] Robo de equipos
	[A.15] Modificación de la información
	[A.51] Inyección de código malicioso (a través de una frontera lógica)
	[A.55] Introducción de objetos (a través del perímetro físico)
	[A.19] Revelación de información
	[E.25] Pérdida de equipos
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.57] Acceso no autorizado (a través del perímetro físico)
	[A.24] Denegación de servicio
[PR. g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma	

	[PR. g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados
[PGECO3/ANC] Analista de Crédito	[A.11] Acceso no autorizado
	[A.56] Retirada de objetos (a través del perímetro físico)
	[A.5] Suplantación de la identidad
	[A.6] Abuso de privilegios de acceso
	[A.25] Robo de equipos
	[E.25] Pérdida de equipos
	[A.15] Modificación de la información
	[A.51] Inyección de código malicioso (a través de una frontera lógica)
	[A.55] Introducción de objetos (a través del perímetro físico)
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.19] Revelación de información
	[A.57] Acceso no autorizado (a través del perímetro físico)
	[PR. g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma
	[PR. g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados

9.8.ANEXOS H. Cumplimiento ISO/IEC 27002:2022

Este documento se incluye en la documentación de seguridad del sistema con el propósito de evaluar el cumplimiento de la normativa ISO/IEC 27002:2022 y determinar el nivel de madurez de la entidad financiera en relación con la metodología Magerit.

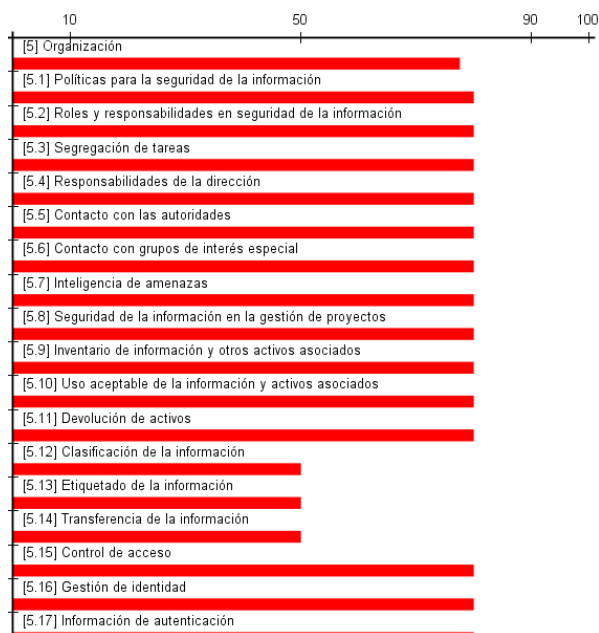
Niveles de madurez

- L0 - inexistente
- L1 - inicial / ad hoc
- L2 - reproducible, pero intuitivo
- L3 - proceso definido
- L4 - gestionado y medible
- L5 - optimizado

[5] Controles organizativos`

Control	aplica	PILAR
[5] Organización	/ sí	L2-L3
[5.1] Políticas para la seguridad de la información	/ sí	L3
[5.2] Roles y responsabilidades en seguridad de la información	/ sí	L3
[5.3] Segregación de tareas	/ sí	L3
[5.4] Responsabilidades de la dirección	/ sí	L3
[5.5] Contacto con las autoridades	/ sí	L3
[5.6] Contacto con grupos de interés especial	/ sí	L3
[5.7] Inteligencia de amenazas	/ sí	L3
[5.8] Seguridad de la información en la gestión de proyectos	/ sí	L3
[5.9] Inventario de información y otros activos asociados	/ sí	L3
[5.10] Uso aceptable de la información y activos asociados	/ sí	L3
[5.11] Devolución de activos	/ sí	L3
[5.12] Clasificación de la información	/ sí	L2
[5.13] Etiquetado de la información	/ sí	L2

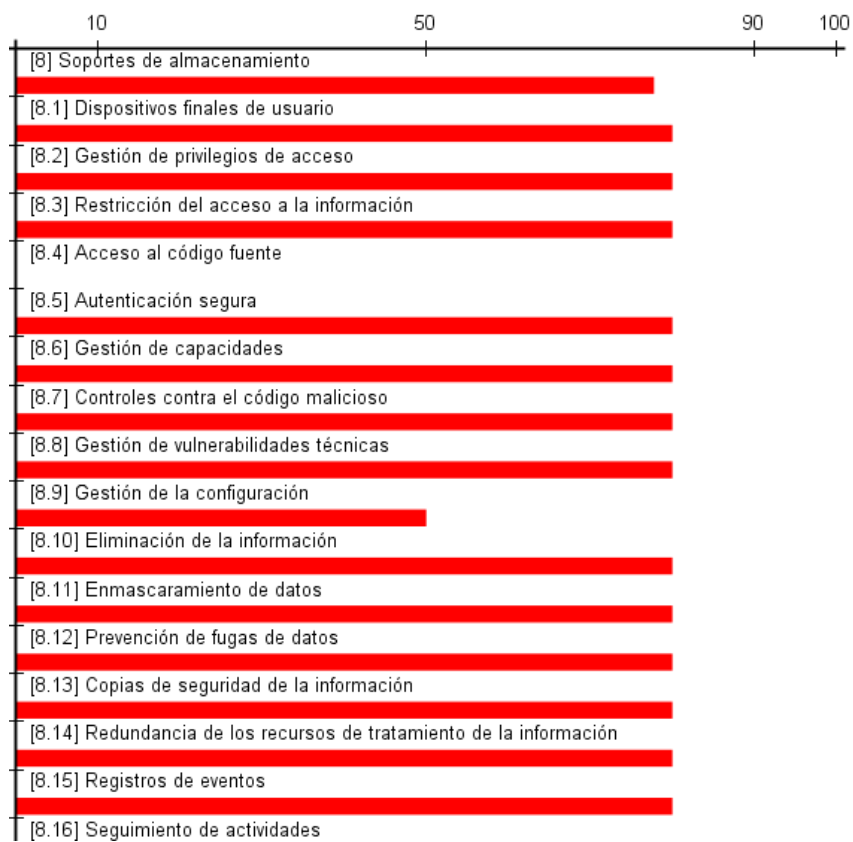
[5.14] Transferencia de la información	/ sí	L2
[5.15] Control de acceso	/ sí	L3
[5.16] Gestión de identidad	/ sí	L3
[5.17] Información de autenticación	/ sí	L3



[8] Controles tecnológicos

Controles Tecnológicos	aplica	PILAR
[8] Soportes de almacenamiento	/ sí	L2-L3
[8.1] Dispositivos finales de usuario	/ sí	L3
[8.2] Gestión de privilegios de acceso	/ sí	L3
[8.3] Restricción del acceso a la información	/ sí	L3
[8.4] Acceso al código fuente	/ sí	n.a.
[8.5] Autenticación segura	/ sí	L3
[8.6] Gestión de capacidades	/ sí	L3
[8.7] Controles contra el código malicioso	/ sí	L3
[8.8] Gestión de vulnerabilidades técnicas	/ sí	L3
[8.9] Gestión de la configuración	/ sí	L2
[8.10] Eliminación de la información	/ sí	L3

[8.11] Enmascaramiento de datos	/ sí	L3
[8.12] Prevención de fugas de datos	/ sí	L3
[8.13] Copias de seguridad de la información	/ sí	L3



**COOPERATIVA DE AHORRO Y
CRÉDITO SANTA ANITA LTDA.**
SISTEMA DE GESTIÓN POR PROCESOS



Santa Anita
COOPERATIVA DE AHORRO Y CRÉDITO

**GUÍA PARA ELABORACIÓN Y GESTIÓN
DE DOCUMENTOS**
SGP-GA-01

SISTEMA DE GESTION DE PROCESOS

GUIA PARA LA ELABORACIÓN Y CONTROL DE DOCUMENTOS

Control de documentación

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre:			
Cargo:			
Firma:			
Fecha:			

Ficha de Edición del documento

Nombre del Documento:		
Código del Documento		
Edición		
Fecha de Edición		
Responsable de Edición		
Cargo		
Cambios Realizados	Autor de Edición	Fechas de Ediciones

7. Tabla de contenido

Control de documentación	0
Ficha de Edición del documento	0
1. Introducción	3
2. Objetivo.....	3
3. Alcance	3
4. Referencias.....	3
5. Responsabilidad	4
6. Definiciones	4
7. Estructura de presentaciones de los documentos	5
7.1. Elaboración revisión y aprobación	5
7.2. Ficha de Edición de Documento.....	6
7.3. Formato Control de Políticas	7
7.4. Actualización y Modificaciones	8
7.5. Formato de los documentos	9
7.5.1. Encabezado.....	10
7.5.2. Formato de redacción	10
8. Tipos de Documentos de Prevención de Fuga de Información	9
8.1. Manual de Prevención de Fuga de Información	9
8.1.1. Responsabilidades	12
8.1.2. Estructura de Manual de Prevención de Fuga de Información	12
8.2. Manual de políticas y procedimiento.....	13
8.2.1. Responsabilidades	13
8.2.2. Estructura de Manual de Procedimiento	14
8.2.3. Estructura de los procedimientos	14

9.	Nomenclatura de Procesos	15
9.1.	Nomenclatura de Proceso	16
9.2.	Nomenclatura de Manuales	17
9.3.	Nomenclatura de Políticas	17
9.4.	Nomenclatura de Guías	18

1. Introducción

En esta guía, se proporcionará un marco para la elaboración y control de estos documentos. Se cubrirán los elementos clave que deben incluirse en las políticas y procedimientos, así como los procesos necesarios para garantizar que se implementen y se sigan correctamente. Al seguir esta guía, las organizaciones pueden fortalecer su protección de la información confidencial y reducir el riesgo de filtraciones de datos.

2. Objetivo

El propósito de la guía para elaboración y control de documentos de prevención de fuga de información es brindar a las organizaciones una herramienta efectiva para establecer la estructura apropiada de la documentación.

3. Alcance

La guía pretende proporcionar una referencia exhaustiva para ayudar a las organizaciones a establecer una estructura de documentación adecuada, que garantice un enfoque sólido para evitar la fuga de información sensible.

4. Referencias

Las referencias normativas aplicables a este Manual son las siguientes:

- ISO/IEC 27002 Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información.
- Normativa vigente de la entidad financiera COAC “Santa Anita Ltda.”
- Manual de políticas y procedimiento de Administración de Cartera.
- Manual de Seguridad

5. Responsabilidad

La guía para elaboración y control de documentos tiene la responsabilidad de establecer los criterios y normas para la creación y gestión de documentos en la entidad financiera COAC "Santa Anita Ltda.". Esta guía estará a cargo del coordinador del Sistema de Gestión por Procesos (SGP), quien se encargará de supervisar el cumplimiento de los lineamientos.

Es fundamental que esta guía se mantenga actualizada y sea fácilmente accesible para que los colaboradores de la organización puedan consultarla en caso de dudas o necesidades. Entre otros aspectos, la guía deberá incluir información sobre los formatos de documentos permitidos, las normas de redacción y estilo, los procesos de revisión y aprobación, así como las políticas de almacenamiento y disposición de documentos. Además, se asegurará de cumplir con los requisitos legales y normativos aplicables en cuanto a la creación y control de documentos.

6. Definiciones

La prevención de fuga de información, consiste en una serie de acciones y tecnologías diseñadas para impedir la divulgación no autorizada de información confidencial o sensible dentro de la entidad financiera. A continuación, se proporcionan algunas definiciones de términos asociados con la prevención de fuga de información:

- Política de seguridad de la información: un conjunto de reglas y procedimientos que regulan el acceso, uso y divulgación de información sensible o confidencial en una organización.
- Análisis de contenido: se refiere a la evaluación del contenido de los mensajes, correos electrónicos, archivos y otros tipos de información para detectar posibles fugas de información.

- Formato: Se entiende por formato a la disposición y presentación particular que se emplea para organizar y exhibir información de manera clara y coherente en diversos tipos de documentos o archivos.

7. Estructura de presentaciones de los documentos

La estructura de presentación de la "Guía para Elaboración y Control de Documentos" puede seguir una secuencia lógica y organizada para facilitar la comprensión y uso de la documentación.

7.1. Elaboración, revisión y aprobación

Las responsabilidades relacionadas con la creación, revisión y aprobación de los documentos están determinadas conforme a la Matriz de Proceso y Procedimientos establecida en el Manual de Prevención de fuga de información.

- El Coordinador de la entidad financiera será responsable del control de nuevos documentos hasta que sean aprobados definitivamente.
- Durante la fase de elaboración o revisión de los documentos propuestos, según corresponda, el Coordinador de la entidad financiera brindará asesoramiento o verificará para asegurar que cumplan con los requisitos de la Norma ISO/IEC 27002:2022, así como con la normativa interna aplicable a los involucrados en el procedimiento de recuperación operativa.
- La ficha de control de la documentación se observa en la Tabla 1, que tiene como propósito mantener un registro y controlar la información vinculada a la documentación del proceso. Esta ficha identifica claramente cada etapa del documento, incluyendo la elaboración, revisión y aprobación. Además, contiene detalles adicionales de relevancia sobre los documentos gestionados.

- **Elaborado por:** nombre del responsable que elaboró la documentación que se presenta.
- **Revisado por:** Se señala el nombre del individuo que llevó a cabo la revisión del contenido, asegurando su calidad y precisión.
- **Aprobado por:** Representa el nombre de la autoridad competente que otorgó la aprobación final.
- **Cargo:** La ocupación de dicha persona según la entidad
- **Fecha:** Puede corresponder a la fase de elaboración, revisión y aprobación del documento.

Tabla 34. Ficha de Control de Documentación

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre:			
Cargo:			
Firma:			
Fecha:			

7.2. Ficha de Edición de Documento

La ficha de edición del documento se observa en la Tabla 2 y consta de la siguiente información:

- **Nombre del Documento:** Indica el nombre del documento que será modificado.
- **Código del Documento:** El código se determina de acuerdo con las instrucciones presentes en la documentación del procedimiento.
- **Edición:** Número de la versión del documento
- **Fecha de Edición:** Fecha de la última modificación
- **Responsable de Edición:** El encargado de las modificaciones especificadas en cada documentación

- **Cargo:** La ocupación de dicha persona según el cargo que establece en la entidad
- **Cambios realizados:** Se determina la sección donde se llevará a cabo la modificación.
- **Autor de Edición:** La persona encargada de llevar a cabo la modificación en la sección designada.
- **Fecha de Edición:** La fecha en la que se efectúan las modificaciones.

Tabla 35. Ficha de Edición de Documento

FICHA DE EDICIÓN DEL DOCUMENTO

Nombre del Documento:		
Código del Documento		
Edición		
Fecha de Edición		
Responsable de Edición		
Cargo		
Cambios Realizados	Autor de Edición	Fecha de Edición

7.3.Formato Control de Políticas

Este formato de control será empleado como parte del Manual de Política y Procedimiento de Prevención de Fuga de Información, con el fin de registrar información relevante, que incluye:

- **Título de Política:** Especifica los nombres de las políticas que serán detalladas
- **Código de Política:** Identificación particular del documento en base a grupos de letras, números y símbolos; conforme se describe en la sección 11 del presente documento
- **Versión:** Señala el número de modificaciones secuenciales realizadas en el documento, siendo la primera versión el número uno (01)
- **Fecha de aprobación:** Se determina cuándo las políticas han sido aprobadas por la alta dirección.

- **Fecha de Revisión:** Se especifica la fecha de revisión por los miembros pertinentes.
- **Proceso:** Proceso al que pertenece el documento que se va a elaborar
- **Procedimiento:** Nombre del procedimiento que está incluido en el proceso mencionado.
- **Dominio:** Se identifica el marco normativo en el que se enfoca la política.
- **Control:** Se señala el control que describe la norma específica.

Tabla 36. Ficha de control de política

Título de Política	
<i>Código de Política</i>	
<i>Versión</i>	
<i>Fecha de aprobación</i>	
<i>Fecha de Revisión</i>	
<i>Responsable de aprobación</i>	
<i>Proceso</i>	
<i>Procedimiento</i>	
<i>Dominio</i>	
<i>Control</i>	

7.4. Actualización y Modificaciones

Los documentos complementarios al manual de prevención de fuga de información serán revisados y actualizados según las necesidades de la gestión y desarrollo en la entidad financiera (SGP).

- Las responsabilidades para la revisión, actualización y modificaciones de dichos documentos se regirán por las pautas establecidas en la sección 7.2 del presente documento, en relación con la elaboración, revisión y aprobación del Manual de prevención de fuga de información

- Cualquier personal involucrado en el procedimiento de recuperación operativa podrá proponer las modificaciones que se consideren necesarias durante el ciclo de gestión. Estas propuestas se gestionarán de manera específica y estarán sujetas al sistema de elaboración, revisión y aprobación.
- El Coordinador brindará asesoramiento a los responsables de cada área involucrada en el procedimiento de recuperación operativa, con el fin de asegurar que las propuestas cumplan con los requisitos establecidos en la Norma ISO/IEC 27002:2022 y las normativas internas aplicables de la COAC "Santa Anita Ltda."
- Una vez aprobada la modificación, se procederá a la actualización de la documentación de acuerdo con el procedimiento de ficha de edición de documento establecido en la sección 7.1 mencionada anteriormente.
- Las versiones anteriores de los documentos modificados o actualizados serán consideradas como "documentos obsoletos" y carecerán de validez y aplicabilidad en el Manual de prevención de fuga de información.

8. Tipos de Documentos de Prevención de Fuga de Información

Según la estructura documental del Manual de Prevención de Fuga de Información (pirámide documental) establecida en la sección 3, se encuentran los siguientes tipos de documentos: manuales, guías y formatos. A continuación, se detalla la organización de cada uno de estos documentos.


8.1.Formato de los documentos

Se requiere que todos los documentos del Manual de Prevención de Fuga de Información sean elaborados siguiendo la estructura que se detalla a continuación.

8.1.1. Encabezado

Los documentos del Manual de prevención de fuga de información se redactan empleando el encabezado que se presenta en la Figura 1.

Figura 108. Formato del encabezado para los documentos del PFI

MANUAL DE PREVENCIÓN FUGA DE INFORMACIÓN		Código:
 Santa Anita <small>COOPERATIVA DE AHORRO Y CRÉDITO</small>	PROCESO:	Versión:
	PROCEDIMIENTO	Página:

Todas las hojas creadas deben contener la información del encabezado con la secuencia numérica correspondiente. El encabezado incluye la siguiente información:

- **Proceso:** Proceso al que pertenece el documento que se va a elaborar.
- **Procedimiento:** Nombre del procedimiento que está incluido en el proceso mencionado.
- **Código:** Identificación particular del documento en base a grupos de letras, números y símbolos; conforme se describe en la sección 11 del presente documento.
- **Versión:** Señala el número de modificaciones secuenciales realizadas en el documento, siendo la primera versión el número uno (01).
- **Página:** Numeración consecutiva que indica el número de página dentro del total de páginas del documento.

8.1.2. Formato de redacción

Todos los documentos del Manual de prevención de fuga de información deberán adherirse a los requisitos de la norma APA 7, que están detallados en la redacción presentada en la Tabla 4.

Tabla 37. Formato de Redacción

FORMATO DE REDACCIÓN

Papel	A4
Márgenes	Superior e inferior: 2,54 cm Derecho e Izquierdo: 2,54 cm
Interlineado	1.5 líneas
Tipo de Letra	Times New Román
Tamaño de Letra	12 puntos
Títulos y Subtítulos	Nivel 1: Negrita y mayúscula sostenida. Nivel 2. Negrita y mayúscula inicial. Nivel 3 en adelante: Negrita, Cursiva y mayúscula inicial.
Figuras	Ubicar el nombre en la parte superior del gráfico correspondiente, centrado y tamaño de letra de 10 puntos
Tablas	Ubicar el nombre en la parte superior izquierda de la tabla.

Al crear un documento del Manual de Prevención de Fuga de Información, es importante tener en consideración las siguientes condiciones generales:

- El texto debe ser redactado de manera clara y precisa, utilizando el tiempo presente y una forma impersonal. Es importante evitar el uso de términos en idioma extranjero, a menos que sean comúnmente utilizados en el lenguaje técnico.
- Al redactar el documento, es necesario emplear términos uniformes para asegurar la coherencia en el texto.
- Las definiciones presentes en la documentación se dispondrán en orden alfabético.

8.2. Manual de Prevención de Fuga de Información

El Manual de Prevención de Fuga de Información es un documento singular que detalla el procedimiento de recuperación operativa en la entidad financiera COAC "Santa Anita Ltda.". Este manual presenta información explícita, organizada y sistemática acerca de sus objetivos,

políticas, atribuciones, organización y procesos. Se basa en los objetivos y la normativa institucional aplicable como su marco de referencia.

8.2.1. Responsabilidades

El cumplimiento de estas responsabilidades resulta fundamental para garantizar una administración efectiva y el adecuado acatamiento de las políticas y procedimientos definidos en el Manual de Prevención de Fuga de Información.

- **Elaboración:** Se indica la persona encargada del desarrollo del proyecto
- **Revisión:** La responsabilidad recae en el jefe de Tecnología de la entidad financiera.
- **Aprobación:** La responsabilidad corresponde a la autoridad pertinente de la COAC "Santa Anita Ltda."

8.2.2. Estructura de Manual de Prevención de Fuga de Información

El Manual de Prevención de Fuga de Información de la entidad financiera COAC "Santa Anita Ltda." presenta la siguiente estructura:

- Portada del Manual de Prevención de Fuga de Información

Se presenta la portada propuesta, como se muestra en la Figura 2, que incluye la siguiente información: nombre y logotipo de la organización, título del documento y código del mismo.

Figura 109. Portada propuesta del Manual de Prevención de Fuga de Información



8.3. Manual de políticas y procedimiento

El presente Manual documenta el proceso de recuperación operativa vinculado al macroproceso de gestión de crédito y cobranza. Su función es proporcionar orientación para llevar a cabo de manera adecuada las actividades de prevención de fuga de información, centrándose en los activos de la información identificados. Los procedimientos detallados en este manual han sido elaborados teniendo en cuenta el cumplimiento de los requisitos establecidos en la Norma ISO/IEC 27002:2022.

8.3.1. Responsabilidades

El cumplimiento de estas responsabilidades es esencial para asegurar la correcta ejecución de las actividades definidas en el Manual de Prevención de Fuga de Información.

- **Elaboración:** Se indica la persona encargada del desarrollo del proyecto
- **Revisión:** La responsabilidad recae en el jefe de Tecnología de la entidad financiera.

- **Aprobación:** La responsabilidad corresponde a la autoridad pertinente de la COAC "Santa Anita Ltda."

8.3.2. Estructura de Manual de Procedimiento

El Manual de Procedimiento de Prevención de Fuga de Información de la entidad financiera COAC "Santa Anita Ltda." presenta la siguiente estructura.

- Portada de Procedimiento de Manual de Prevención de Fuga de Información

Se presenta la portada propuesta, como se muestra en la Figura 3, que incluye la siguiente información: nombre y logotipo de la organización, título del documento y código del mismo.

Figura 110. Portada propuesta del Manual de Procedimiento de Prevención de Fuga de Información



8.3.3. Estructura de los procedimientos

El documento proporciona una estructura general que puede ser utilizada como guía para la elaboración de estos procedimientos.

- **Objetivo:** El objetivo representa la finalidad o intención que se persigue al implementar un plan, acción o proyecto.
- **Alcance:** El alcance define los límites y contenidos del proyecto, determinando qué será incluido y qué quedará fuera de su desarrollo.
- **Definiciones y Abreviaturas:** Son términos y siglas presentes en un documento o manual que necesitan ser explicados o acortados para facilitar su comprensión.
- **Responsables:** Ejecutor (es) directo del procedimiento.
- **Documentos y Referencias:** Estos documentos y referencias pueden provenir de diversas fuentes, como estándares internacionales, legislaciones, regulaciones, manuales técnicos, entre otras.
- **Descripción del Procedimiento:** La descripción del procedimiento es una exposición minuciosa y organizada de cómo se realiza un proceso particular.
- **Control de documentación:** Se proporciona una lista de registros y formatos en los cuales se documenta la información obtenida durante la aplicación del documento.

9. Nomenclatura de Procesos

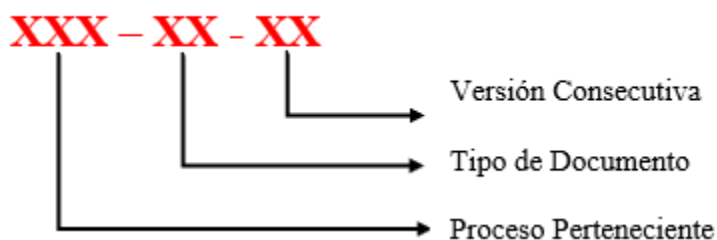
La nomenclatura de los documentos funcionará como una referencia para la entidad financiera COAC “Santa Anita Ltda.”, quien determinará su utilización siguiendo las indicaciones establecidas en estos manuales.

La nomenclatura de los documentos para el procedimiento de prevención de fuga de información se ha generado utilizando una combinación de letras, números y guiones, basándose en la Matriz de Proceso y Procedimientos actualmente establecida en la entidad.

Cada documento cuenta con un código de identificación compuesto por tres partes, tal como se muestra en la Figura 4.

- **Proceso:** Hace referencia al proceso al cual está relacionado el documento.
- **Tipo de documento:** Se refiere al tipo de documento que puede ser Manual de Prevención de Fuga de Información, Manual de Procedimientos, Guía o Formato.

Figura 111. Código de identificación



- **Versión consecutiva:** Si se trata de documentos del Proceso Sistema de Gestión por Procesos correspondiente al Macro proceso de Apoyo de la entidad financiera COAC “Santa Anita Ltda.”, el consecutivo será la numeración ascendente (01, 02, 03,...) que se asigna según el orden de las versiones editadas del documento.

En la Tabla 5 se proporciona una lista de las abreviaturas utilizadas para identificar los diferentes tipos de documentos.

Tabla 38. Abreviaturas para nomenclatura de documentos de PFI

TIPO DE DOCUMENTO	ABREVIATURA
Manual de Prevención de Fuga de Información	MPFI
Manual de Procedimiento de Prevención de Fuga de Información	MPPFI
Proceso	PR
Procedimiento	PD
Guía	GA

9.1.Nomenclatura de Proceso

La nomenclatura empleada para los procesos consta de tres componentes, como se muestra en la Figura 5. La primera parte representa el código del control establecido, seguido de un guion, y luego se añade la sigla "PR" en mayúsculas, identificando así el documento como un

proceso. Finalmente, se agrega un número consecutivo que sigue el orden de creación, o edición de la documentación.

Figura 112. Estructura de Nomenclatura de procesos

“ABREVIATURA DE PROCESO” – PR – “VERSION CONSECUTIVA”

9.2.Nomenclatura de Manuales

Los manuales de Prevención de Fuga de Información (PFI) se codifican siguiendo el formato presentado en la Figura 6. Primero se incluye el código del proceso al cual pertenece el manual, seguido de un guion, y después las siglas en mayúscula "MPFI" para el Manual de Prevención de Fuga de Información o "MPPFI" para el Manual de Procedimientos de Prevención de Fuga de Información. Posteriormente, se agrega un número consecutivo que corresponde al orden de creación o edición.

Figura 113. Estructura de Nomenclatura de Manuales

“ABREVIATURA DE PROCESO” – MPFI o MPPFI – “VERSION CONSECUTIVA”

9.3.Nomenclatura de Políticas

Los controles son identificados y codificados siguiendo lo dispuesto en la norma ISO/IEC 27002:2022, específicamente en las secciones 5.12 y 8.12 del manual de prevención de fuga de información. Para esta codificación, se emplean las abreviaturas detalladas en la Figura 8.

Figura 114. Abreviatura de nomenclatura de Controles

CONTROL	ABREVIATURA
Política de Clasificación de Información	PCI
Política de Prevención de fuga de información	PPI

Figura 115. Estructura de Nomenclatura de Políticas

“ABREVIATURA DE POLITICA”– “VERSION CONSECUTIVA”

9.4.Nomenclatura de Guías

Las Guías de Prevención de Fuga de Información (PFI) se codifican de acuerdo al formato presentado en la Figura 9, donde se incluye el código del proceso al que pertenece la Guía, seguido de un guion, seguido de las siglas en mayúscula "GA", y finalmente, un número consecutivo que sigue el orden de creación.

Figura 116. Estructura de Nomenclatura de Guías

“ABREVIATURA DE PROCESO” – GA – “VERSION CONSECUTIVA”