UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:

Propuesta de un plan Estratégico de Prevención de Pérdida de Datos mediante Safetica (DLP) para fortalecer la seguridad de la información sensible, en Inforc.

Línea de Investigación:

Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable

Campo amplio de conocimiento:

Tecnologías de la Información y la Comunicación (TIC)

Autor:

Rogel Ramírez Alfredo Duberli

Tutor:

Ms. Renato Mauricio Toasa Guachi

PHD. Maryory Urdaneta Herrera

Quito – Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, Ms. Renato Mauricio Toasa Guachi C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado: _ **Propuesta de un plan Estratégico de Prevención de Pérdida de Datos mediante Safetica (DLP) para fortalecer la seguridad de la información sensible, en Inforc.**

Elaborado por: Rogel Ramírez Alfredo Duberli, de C.I: 172186517-6, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2024

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

_____

Mg. RENATO MAURICIO TOASA GUACHI

ORCID: 0000-0002-2138-300X

APROBACIÓN DEL TUTOR

Yo, MARYORY URDANETA HERRERA con C.I: 1759316126 en mi calidad de Tutor del proyecto de investigación titulado: _ **Propuesta de un plan Estratégico de Prevención de Pérdida de Datos mediante Safetica (DLP) para fortalecer la seguridad de la información sensible, en Inforc.**

Elaborado por: Rogel Ramírez Alfredo Duberli, de C.I: 172186517-6, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2024

Firmado electrónicamente por:
MARYORY URDANETA HERRERA

_____

PhD. MARYORY URDANETA HERRERA

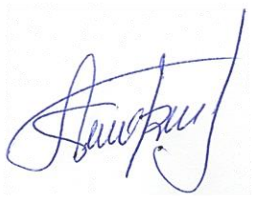
ORDIC: 0000-0001-8773-5349

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Rogel Ramírez Alfredo Duberli con C.I: 172186517-6, autor del proyecto de titulación denominado: **Propuesta de un plan Estratégico de Prevención de Pérdida de Datos mediante Safetica (DLP) para fortalecer la seguridad de la información sensible, en Inforc.**. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2024



_____

Firma

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

Garantizar la seguridad de los datos digitales es ahora una preocupación primordial en una variedad de sectores, como la educación, las finanzas y la administración pública. Esta información se ha vuelto un recurso fundamental para el funcionamiento de estas entidades. Sin embargo, el continuo progreso tecnológico ha traído consigo nuevas amenazas que comprometen la seguridad de la información (SI).

En este contexto, la adopción de soluciones integrales para la Prevención de Pérdida de Datos (DLP) se ha vuelto indispensable. Estas soluciones abordan una amplia gama de riesgos, muchos de los cuales provienen de factores humanos. Safetica, por ejemplo, proporciona defensa contra filtraciones de datos accidentales o intencionales, problemas de productividad y riesgos relacionados con la implementación de políticas "Bring Your Own Device" (BYOD), entre otros. Su enfoque se basa en la integridad, flexibilidad y facilidad de uso, brindando a los administradores una herramienta completa para evitar fugas de datos a nivel empresarial.

En Ecuador, al igual que en muchos otros países, el tema relacionado con salvaguardar la información ha adquirido una importancia creciente (Hernández et. al, 2023). Recientemente, se ha aprobado una legislación concerniente a la salvaguarda de datos personales y la seguridad de la información. Esta ley establece pautas y directrices para asegurar la confidencialidad y protección de la información de los residentes de Ecuador (Martínez et. al, 2023). Este reglamento subraya la importancia de que las compañías, incluyendo las pequeñas y medianas empresas (pymes), adopten medidas de seguridad robustas para resguardar la información confidencial de sus clientes y empleados.

Considerando todo lo expuesto anteriormente, nace la propuesta de implementar un software como Safetica para reforzar la seguridad de los datos sensibles en Inforc, una empresa que valora la protección de sus activos digitales. Este se encuentra alineado con los estándares óptimos y las normativas vigentes, con el propósito de brindar una solución completa que prevenga y reduzca los riesgos relacionados con la pérdida de información.

El objetivo principal de este plan es fomentar prácticas efectivas que contribuyan a establecer un sistema empresarial sólido y completo. Se propone la implementación de Safetica como una solución DLP que permita monitorear, detectar y prevenir la pérdida de datos sensibles, además de establecer políticas y procedimientos de seguridad que cumplan con las regulaciones vigentes y promuevan una cultura de seguridad informática dentro de la organización.

Problema de investigación

La pérdida de datos es una preocupación creciente en Inforc, especialmente en un contexto donde la información digital se ha vuelto un activo sumamente valioso. Esta problemática se manifiesta de diversas formas y puede tener consecuencias graves para la empresa, incluyendo daños a la reputación, pérdidas financieras y violaciones de la privacidad.

La carencia de control sobre quién accede a la información y su gestión constituye una de las principales causas de pérdida de datos. Los ciberataques representan una amenaza constante, con hackers que buscan acceder a datos sensibles para su beneficio personal o para fines maliciosos. Además, los errores humanos, como enviar información confidencial a destinatarios incorrectos o dejar dispositivos desprotegidos contribuyen una pérdida significativa de información.

La divulgación de información sensible puede ocurrir tanto de manera accidental como intencional. En algunos casos, los empleados pueden no estar al corriente las normas relacionadas a protección de la información de la empresa o pueden cometer errores involuntarios que resultan en la filtración de datos. En otros casos, la fuga de datos puede ser resultado de acciones maliciosas por parte de empleados descontentos o ex empleados con acceso no autorizado.

La creciente integración de nuevas tecnologías y métodos de trabajo, como el trabajo de forma remota y el empleo de dispositivos móviles personales en el ámbito laboral, también ha incrementado el riesgo de pérdida de datos dentro de la empresa. Estos cambios en los procesos laborales pueden aumentar la exposición de la información confidencial y complicar su protección adecuada.

Inforc, además de lidiar con riesgos tanto internos como externos, se ve confrontada con desafíos regulatorios dentro de este ámbito, debido a que la normativa que regula este se encuentra en continua transformación, exigiendo que la empresa cumpla con diversos requisitos legales y normativos para prevenir sanciones y multas.

En definitiva, la problemática de la pérdida de datos es compleja y multifacética, y requiere una atención cuidadosa por parte de la empresa. La implementación de medidas de prevención de pérdida de datos (DLP) se vuelve fundamental proteger la información sensible y asegurar la seguridad y privacidad de los datos en un entorno empresarial que experimenta cambios constantes y está expuesto a diversas formas de ataques y vulnerabilidades. De ahí que resulta importante utilizar Safetica ya que es una herramienta DLP que se integra a las necesidades de la empresa y ayuda rastrear del flujo de trabajo y permite conocer que información es compartida, así como la generación de políticas acorde a las necesidades de la empresa.

Objetivo general

Desarrollar una propuesta de un plan Estratégico de Prevención de Pérdida de Datos (DLP) mediante Safetica, para fortalecer la seguridad de la información sensible, en Inforc.

Objetivos específicos

- Contextualizar los fundamentos teóricos de Prevención de Pérdida de Datos (DLP) y seguridad de la información mediante los criterios de distintos autores.
- Determinar los activos importantes de la organización relacionados con la información sensible para fortalecer la seguridad.
- Diseñar el plan estratégico en prevención de perdida de datos, mediante Safetica,
- Validar la propuesta del plan estratégico de prevención de perdida datos.

Vinculación con la sociedad y beneficiarios directos

La implementación del sistema completo de Prevención de Pérdida de Datos (DLP) con Safetica en la empresa Inforc no solo representa un proceso interno, sino que también ejerce un impacto considerable en la sociedad y en aquellos directamente involucrados en la protección de información.

Desde una perspectiva más amplia, la adopción de Safetica y otras medidas de seguridad de la información se convierte en una contribución esencial para proteger la confidencialidad y la seguridad de los datos de la comunidad en general. Al prevenir la pérdida de datos, se disminuyen los riesgos relacionados con el robo de identidad, los fraudes financieros y otros delitos cibernéticos que pueden afectar tanto a individuos como a comunidades enteras.

Los principales beneficiarios directos de esta solución son los clientes, empleados y otras partes interesadas de la empresa Enforc. Los clientes confían en la empresa al compartir información personal y confidencial, y la implementación de Safetica les brinda una mayor seguridad al saber que sus datos están protegidos eficazmente contra amenazas tanto internas como externas. Por otro lado, los empleados se capacitan y se les proporcionan herramientas necesarias para resguardar la información sensible de la empresa, permitiéndoles desempeñar un papel activo en la seguridad de la información.

Además, la conexión con la sociedad y los beneficiarios directos implica una comunicación transparente y proactiva sobre las medidas de seguridad implementadas y sus beneficios. Enforc tiene la responsabilidad de informar a sus clientes y empleados sobre las políticas y procedimientos a seguir, así como sobre el uso de Safetica y otras herramientas de DLP. Esta comunicación abierta y educativa

no solo construye la confianza y la credibilidad de la empresa, sino que también demuestra su compromiso con las personas.

La implementación integral del sistema de Prevención de Pérdida de Datos (DLP) utilizando Safetica va más allá de los límites empresariales y se transforma en una empresa conjunta para fomentar la confianza y la integridad de la información en nuestra sociedad contemporánea. Esta interacción con la comunidad y los interesados directos ilustra el compromiso de la empresa con la integridad de los datos y la confidencialidad de los individuos en un entorno digital que evoluciona constantemente.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

La protección de la información digital es esencial en diversos sectores como el educativo, financiero y gubernamental. En un mundo donde la información se considera un activo fundamental, la seguridad de la información se vuelve primordial para el buen funcionamiento de las organizaciones. Sin embargo, el avance tecnológico también ha traído consigo nuevas amenazas que ponen en peligro la integridad de los datos.

En este contexto, la implementación de soluciones integrales para DLP se ha vuelto imperativa. Safetica, por ejemplo, ofrece protección ante fugas de datos, problemas de productividad y riesgos asociados "Traiga su propio dispositivo", entre otros. En Ecuador, al igual que en otros países, la reciente aprobación de leyes relacionadas con esta problemática resalta la necesidad imperativa de contar con sistemas de seguridad sólidos.

En este sentido, surge la propuesta de un plan estratégico de DLP mediante Safetica para fortalecer la protección de la información sensible en Inforc. El objetivo principal es establecer un sistema de seguridad de la información empresarial completo, que cumpla con las regulaciones y promueva una cultura de seguridad informática. Se busca implementar Safetica como una solución DLP que permita monitorear, detectar y prevenir la pérdida de datos sensibles.

La implementación de este plan no solo beneficia a Inforc, sino que también tiene un efecto real en la sociedad y en aquellos directamente implicados en la protección de la información sensible. Los clientes y empleados confían en que sus datos están protegidos de manera efectiva, lo que contribuye a la construcción de una comunidad digital más segura y protegida contra amenazas cibernéticas.

1.1. Contextualización general del estado del arte

Se empieza haciendo una revisión del estado de arte para lo que se considera las siguientes investigaciones:

Este trabajo de titulación se centró en la implementación de un modelo DLP en las empresas PYMES del Ecuador. Su objetivo principal fue identificar el origen de la fuga y pérdida de información en estas empresas, así como determinar qué herramienta sería más eficaz para desarrollar la metodología basada en la ley ecuatoriana y las normas internacionales ISO 27001 y 27002. El proyecto abordó la importancia de un modelo de gestión de seguridad de la información para las instituciones financieras, destacando los riesgos de incumplimiento legal, daños a la reputación y paralización de operaciones debido a ataques cibernéticos. Se enfoca en cumplir con las regulaciones de la Superintendencia de Economía Popular y Solidaria para proteger los activos de información y su

confidencialidad, integridad y disponibilidad. Se emplean términos de privacidad de datos, el cubo de McCumber para comprender los estados de la información, y los CIS Controls como buenas prácticas para el análisis de vulnerabilidades y definición de políticas de seguridad. La investigación, de tipo cuantitativa no experimental, facilita la implementación de un modelo de gestión de seguridad de la información basado en la norma ISO 27001 y en el marco de gobierno de Cobit 2019 (Arrellano, 2023).

Este artículo exhibe una revisión sistemática del panorama actual en cuanto a los marcos, modelos y otras propuestas planteadas para identificar las amenazas no intencionales de ciberseguridad originadas por el personal interno en las instituciones públicas. El desarrollo en el ámbito gubernamental ha impulsado a los estados de diversas partes del mundo a establecer servicios digitales de gobierno electrónico. No obstante, este progreso también ha suscitado la urgencia de enfrentar los desafíos de seguridad de la información asociados con dichos servicios. Estudios han demostrado que una gran parte de las amenazas a la ciberseguridad en las entidades estatales provienen del personal interno y suelen ser no intencionales (Castillo et. al, 2021).

Además, se implementó el diseño elaborado en una PYME ecuatoriana, cumpliendo con los requisitos establecidos, con el fin de realizar un análisis de resultados y determinar el costo-beneficio generado por la implementación de un sistema DLP. Este enfoque permitió evaluar la efectividad de la metodología propuesta y su impacto en el contexto empresarial ecuatoriano.

El Departamento de Tecnologías de la Información reconoce la importancia creciente de los datos digitales en el entorno educativo y la necesidad de prevenir infracciones relacionadas con su seguridad. Por ello, se plantea el objetivo de desarrollar un prototipo DLP en una plataforma de código abierto, utilizando enfoques como el análisis inductivo, deductivo, cualitativo, mixto transversal y cuasi experimental, se aborda el análisis de vulnerabilidades, impacto y riesgos, así como la formulación de métodos de seguridad para toda la infraestructura tecnológica de la institución. Sin embargo, los resultados muestran que las herramientas de prevención de pérdida de datos de código abierto no cumplen con los parámetros necesarios para prevenir la fuga de información en el entorno educativo de la PUCESA. Se destaca que la mayoría del software DLP disponible requiere licencias pagadas, lo que implica un alto costo de implementación, ya que se divide en versiones de cliente y servidor. Este hallazgo pone de relieve los desafíos financieros asociados con la implementación de plataformas de seguridad efectivas en el ámbito educativo (Arellano y Lagua, 2021).

El riesgo de fuga de datos es una preocupación constante para todas las organizaciones que utilizan sistemas de información, ya que puede acarrear problemas competitivos, de imagen y legales. Para abordar este desafío, se recurre a las soluciones DLP, que monitorean las actividades de los usuarios, el tráfico de red y la información en reposo para aplicar controles de seguridad que eviten la

fuga de datos, ya sea de forma voluntaria o involuntaria. En este estudio se exploran las características de las herramientas DLP, se comparan varias de ellas y se elige la más adecuada para implementar en una clínica dental. Se proporciona una guía detallada para la instalación, configuración y evaluación de controles específicos diseñados para limitar el uso de dispositivos extraíbles, prevenir el escape de información sensible por correo electrónico u otros programas, encriptar archivos con datos personales y detectar información sensible en reposo. Además, se realiza un análisis de la contextualización legal para garantizar el respeto a la privacidad de los trabajadores durante la implementación de estas soluciones. El principal resultado revela que estas herramientas permiten establecer de manera efectiva una amplia gama de controles de seguridad que logran detectar e impedir la fuga de datos antes de que acontezca (Fenoy Illacer, 2023).

El proyecto se desarrolló a partir de la consulta de diversas fuentes bibliográficas disponibles, con el objetivo de comprender el funcionamiento, la evolución y el uso de los sistemas DLP. Se buscaba identificar los riesgos inherentes a las empresas en cuanto al almacenamiento y compartición de información, así como los factores que motivan su implementación. Además, se estructuraron las funciones principales, características esenciales, fases y recursos de un DLP, con la finalidad de determinar qué conjunto de procesos podrían ser efectivos para evitar la pérdida de información en las organizaciones (Gantiva, 2021).

En la investigación realizada por Moya (2023) titulada “Propuesta de un plan de seguridad informático para la empresa E.P.-E.M.A.P.A.-A.” generada como requerimiento para conseguir el título de Magister en Gerencia Informática se encontró que “El conocimiento de la situación actual de la empresa con respecto a la seguridad de la información permitió definir un punto de partida, se facilita la selección e implementación de controles adecuados y enfocados en la mitigación de los riesgos” (Moya, 2023, p. 48).

Según Kickidler (2022). La tecnología ha simplificado considerablemente el análisis y la recopilación de datos, abarcando no solo información de clientes, sino también de personal. Por consiguiente, asegurar la protección de los datos se ha vuelto aún más fundamental en los procedimientos empresariales. Ya sea que su empresa sea de pequeña escala y de índole familiar o una corporación extensa con cientos de empleados, es imperativo desarrollar un plan de mitigación de riesgos y disponer de una estrategia de prevención de pérdida de datos.

Para la siguiente investigación se analiza las diferentes herramientas, Prevención de Pérdida de Datos (DLP) se erigen como herramientas esenciales, focalizadas en evitar la fuga de información y garantizar la seguridad de datos confidenciales en entornos digitales. Su importancia radica en la capacidad para supervisar, identificar y mitigar riesgos, asegurando la integridad de la información en

un contexto marcado por las amenazas cibernéticas y la continua necesidad de salvaguardar la privacidad.

El Instituto nacional de Ciberseguridad Española, estas soluciones a menudo integran tecnología de inteligencia artificial que les posibilita adquirir conocimiento acerca de los documentos confidenciales utilizados y las acciones realizadas por los usuarios en relación con estos, con el objetivo de mejorar continuamente su eficacia en la prevención de la fuga de información (Incibe, 2019).

Según (DLP) de Safetica incluyen una variedad de servicios incorporados que posibilitan la detección y seguimiento de la pérdida o sustracción de datos no autorizados. Estas soluciones informan sobre tales incidentes e incluso pueden evitarlos mediante la implementación de reglas y políticas predefinidas (Safetica, 2024).

1.2. Proceso investigativo metodológico

Este proyecto implica la introducción de Safetica, una herramienta avanzada de DLP, diseñada para vigilar, identificar y evitar la filtración de información delicada tanto desde fuentes internas como externas. Safetica proporciona una extensa variedad de funciones y características que permiten a Inforc tener un control detallado sobre sus datos, protegiéndolos contra amenazas cibernéticas, errores humanos y acciones malintencionadas.

La metodología de investigación propuesta para este proyecto abarca una combinación de enfoques cualitativos y cuantitativos lo que implica la utilización de técnicas de investigación como la entrevista y las encuestas tomando como indicadores que tipos de dispositivos usa para almacenar la información, que medios electrónicos utiliza para enviarla, el conocimiento de políticas de seguridad de la información así como si usa su correo personal para recibir o enviar información del trabajo, a esto adjuntaremos un estudio de caso específico centrado en la implementación de Safetica en la empresa Inforc. Comprender tanto los aspectos técnicos de la solución como los procesos organizacionales y las percepciones de los usuarios es fundamental para evaluar su efectividad en la protección de datos sensibles.

En primer lugar, se llevará a cabo una revisión exhaustiva de la literatura existente sobre DLP, seguridad de la información y soluciones tecnológicas como Safetica. Esta revisión proporcionará una base teórica sólida y ayudará a identificar mejores prácticas para el estudio.

Luego, se utilizará el caso de Inforc como un estudio de caso para investigar la implementación de Safetica y su impacto. Esto implicará entrevistas con los responsables de la toma de decisiones y los

usuarios finales de Safetica en Inforc, con el fin de comprender los desafíos específicos de seguridad que enfrenta la empresa y cómo Safetica aborda estas necesidades.

Además, se recopilarán datos cuantitativos sobre la eficacia de Safetica en la prevención de pérdida de datos, como el número de incidentes de seguridad antes y después de la implementación, y se realizarán análisis cualitativos mediante entrevistas en profundidad para explorar las percepciones y experiencias de los empleados con respecto a Safetica y la seguridad de la información en general.

Se compararán los hallazgos de esta investigación con estudios anteriores mencionados en la sección de "Contextualización general del estado del arte" para identificar similitudes, diferencias y contribuciones únicas del estudio.

Finalmente, se analizará cómo la implementación de Safetica en Inforc podría impactar a la sociedad y a los beneficiarios directos, como clientes, empleados y partes interesadas, para evaluar la confianza del cliente, la percepción del empleado sobre la seguridad de la información y otros indicadores relevantes.

1.3. Análisis de resultados

El análisis de resultados de un DLP es crucial para determinar si se han logrado los objetivos de seguridad de la información. Este análisis debe considerar la identificación de riesgos y vulnerabilidades, la medición del impacto de las estrategias DLP y la evaluación de su eficacia en la protección de datos sensibles.

Se llevó a cabo un análisis en Inforc entre enero de 2014 y febrero de 2024, la cual tuvo un alcance en la oficina matriz e involucró a 5 funcionarios. Durante este proceso, se formularon una serie de preguntas relacionadas con la fuga de información, con el propósito de identificar el nivel de participación y las causas que llevaron a los funcionarios a incurrir en este tipo de incidentes.

Tabla 1

Detalle y muestra

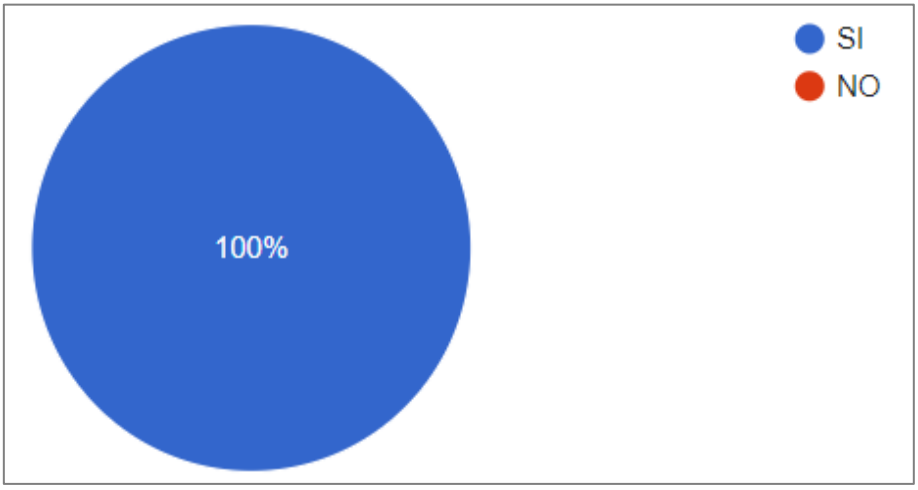
Detalle y Muestra	
Descripción	**Total**
Colaboradores	5
Jefatura Técnica	1
Total	**6**

Para determinar los resultados, se llevó a cabo una entrevista con el Mg. Francisco Changotasi, experto seguridad de la información, para verificar los resultados de la investigación, obteniendo los siguientes hallazgos:

a. **¿Considera que la utilización de herramientas tecnológicas resulta beneficiosa para desempeñar su labor?**

Figura 1

Resultados obtenidos

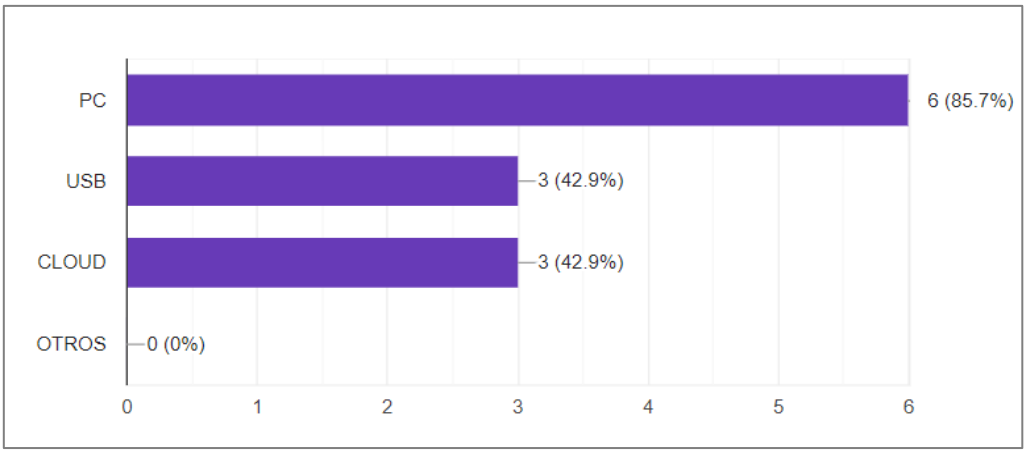


Se reveló que el total de los resultados obtenidos (100%) resultan beneficiosas para las actividades diarias. Ver Figura 1

b. **¿En qué lugar guarda toda la información que genera?**

Figura 2

Información almacenada

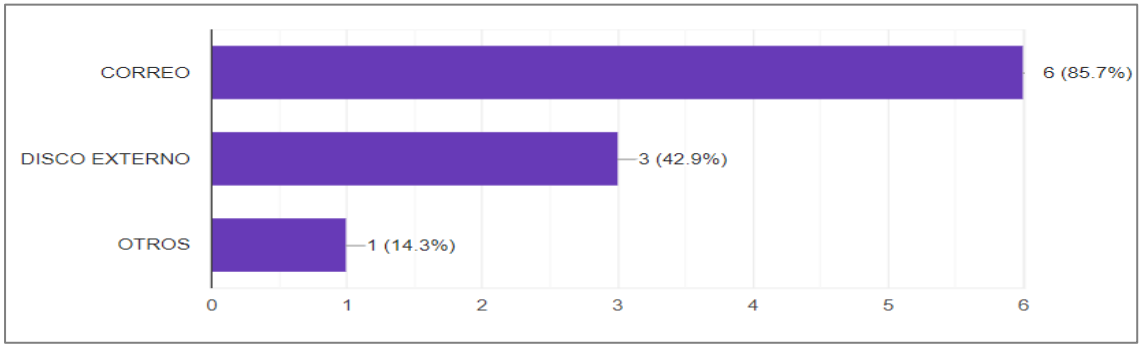


El la figura 2 se detalla a través de la investigación, se encontró que el 85,7% de los datos se almacenan en la computadora asignada por la institución, mientras que el 42,9% se guarda en la nube (Cloud) y una proporción menor, el 42,9%, utiliza dispositivos USB para almacenar la información. Ver Figura 2

c. ¿Qué método electrónico emplea para trasladar la información?

Figura 3

Traslado y almacenamiento

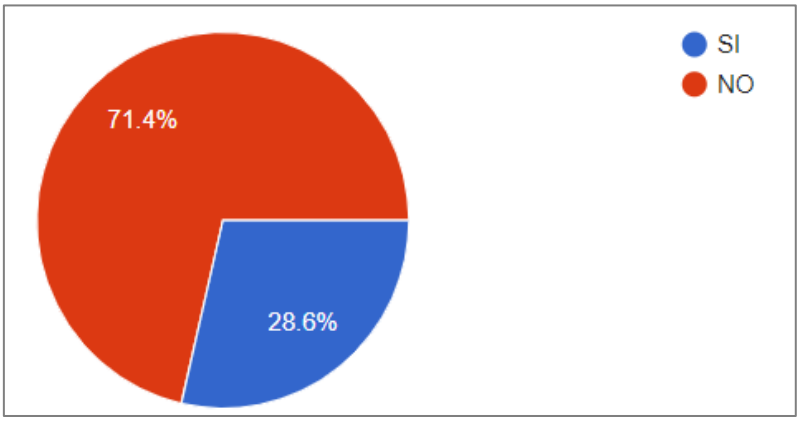


En este estudio también se concluyó que la mayoría de la información generada en la institución se transporta principalmente a través del correo electrónico, con un 85,7%, mientras que el 42,9% recurre a discos externos, y un 14,3% opta por otras alternativas para movilizar la información. Ver Figura 3.

d. Conoce Usted las políticas y normas de seguridad de la información.

Figura 4

Políticas de seguridad

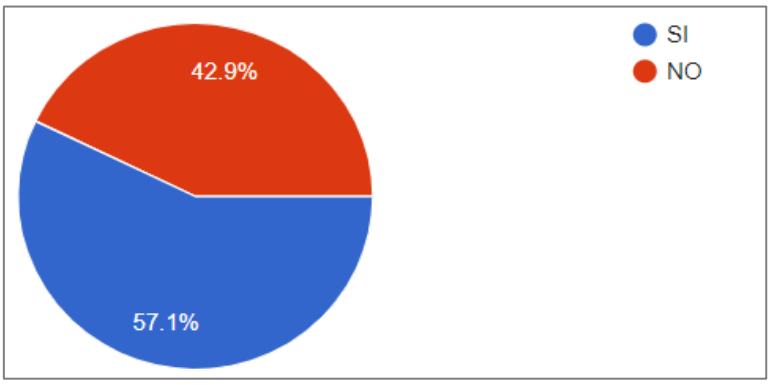


En este análisis, se descubrió que el 71,4% de los empleados de la institución tienen conocimiento de las normas y políticas de la organización, mientras que el 28,6% no las conocen, lo que ocasiona confusión al momento de proteger la información. Tras la realización de las encuestas, se determinó que hay un porcentaje significativo de filtración de información en la empresa, tanto sensible como no sensible. Es esencial resaltar que el departamento de seguridad de la información debe clasificar la información sensible para permitir que en el futuro la herramienta DLP bloquee de manera efectiva dicha información. Ver figura 4.

e. ¿Recurre al uso de su correo personal para llevar a cabo sus tareas en la institución?

Figura 5

Fuga de información



En este análisis también se observó que el 57,1% de los trabajadores de la organización emplean su correo electrónico personal para realizar sus labores cotidianas, en contraste con el 42,9% que no lo hace. Ver Figura 5.

El análisis de resultados basado en la entrevista con el Mg. Francisco Changotasi, experto en seguridad de la información, revela una serie de hallazgos importantes que destacan la utilización de herramientas tecnológicas, el almacenamiento y transporte de la información, el conocimiento de las políticas de seguridad de la información y el uso del correo electrónico personal en la institución.

En primer lugar, se encontró que el 100% de las soluciones tecnológicas son consideradas beneficiosas para el desempeño diario de los empleados. Esto sugiere una clara valoración de la tecnología como una herramienta efectiva en el entorno laboral.

En cuanto al lugar de almacenamiento de la información, se observó que la mayoría de los datos (85,7%) se guardan en la computadora asignada por la institución, seguido por el

almacenamiento en la nube (42,9%) y el uso de dispositivos USB (42,9%). Esta diversidad de métodos de almacenamiento destaca la importancia de implementar políticas de seguridad coherentes y exhaustivas.

En relación con el transporte de la información, se descubrió que la mayoría de los empleados (85,7%) utilizan el correo electrónico como método principal, seguido por el uso de discos externos (42,9%) y otras opciones (14,3%). Esta información resalta la necesidad de asegurar que los datos se transporten de manera segura y se sigan prácticas adecuadas de seguridad de la información.

En cuanto al conocimiento de las políticas y normas de seguridad de la información, se observó que un notable porcentaje (71,4%) de los empleados está familiarizado con ellas, mientras que el 28,6% no lo está. Esta disparidad puede generar confusión y resalta la importancia de la capacitación y concientización en seguridad de la información dentro de la organización.

Por último, en relación con el uso del correo electrónico personal para tareas laborales, se encontró que el 57,1% de los empleados recurren a esta práctica. Esto destaca la necesidad de establecer políticas claras y procedimientos adecuados para el uso seguro de los correos electrónicos personales en el entorno laboral.

En conclusión, el análisis de resultados resalta la importancia de implementar un plan de prevención de pérdida de datos (DLP) efectivo, que considere la diversidad de herramientas tecnológicas utilizadas, los métodos de almacenamiento y transporte de la información, el conocimiento de las políticas de seguridad y el uso adecuado del correo electrónico personal. Mediante un enfoque integral y la participación activa de todas las partes interesadas, las organizaciones pueden mejorar significativamente su postura de seguridad de la información y proteger sus activos digitales de manera más efectiva.

CAPÍTULO II: PROPUESTA

2.1 Fundamentos teóricos aplicados

Basado en la metodología de investigación propuesta y en el contexto del proyecto, es importante tener un entendimiento sólido de varios fundamentos teóricos y conceptos clave relacionados con DLP, seguridad de la información y tecnologías como Safetica. Aquí hay algunos fundamentos teóricos y conceptos importantes que debemos manejar:

Prevención y perdida de Datos (DPL). - Implica la integración de individuos, procedimientos y tecnología con el fin de identificar y evitar la divulgación de información confidencial (Microsoft, 2024).

La prevención de pérdida de datos tiene como objetivo principal proporcionar a las empresas y organizaciones, especialmente a aquellas dedicadas a la vigilancia y seguridad privada, estrategias y herramientas efectivas para evitar la pérdida de información en entornos digitales. Su propósito es mejorar la experiencia del usuario, fortalecer los negocios y gestionar de manera proactiva los riesgos de seguridad que puedan amenazar su integridad y funcionamiento (Viñas, 2022).

Seguridad de la Información. - Se centra en resguardar tanto la información como los sistemas informáticos de accesos, usos, revelaciones, interrupciones o daños no autorizados. La seguridad se define como la ausencia de riesgo o incertidumbre, representando un estado en el que cualquier sistema o tipo de información, ya sea informático o no, se encuentra protegido de posibles amenazas o daños que puedan comprometer su funcionamiento o los resultados esperados (Calidad, 2019).

Safetica Software. - se presenta como una solución especializada en contrarrestar las violaciones de datos causadas por errores humanos o ataques dirigidos, ofreciendo una variedad de herramientas que resguardan todos los aspectos de la empresa para evitar la salida de información no autorizada. Además, proporciona informes sólidos y alertas de seguridad instantáneas, garantiza el cumplimiento de las regulaciones legales y ofrece un diseño adaptado a las empresas remotas de la era moderna (Safetica, 2020).

Vulnerabilidades. - Una vulnerabilidad en informática se refiere a una debilidad o defecto en un sistema, red, software o configuración que puede ser explotada por un atacante para comprometer la seguridad del sistema o acceder a información de manera no autorizada. Estas vulnerabilidades pueden ser el resultado de diversos factores, incluyendo fallas en el diseño de protocolos de red, errores de programación, configuraciones inadecuadas de sistemas, ausencia de políticas de seguridad, desconocimiento de herramientas utilizadas por atacantes, presencia de puertas traseras y restricciones gubernamentales. Estas vulnerabilidades pueden permitir a los atacantes realizar una

variedad de acciones maliciosas, como robar datos sensibles, interrumpir servicios, tomar el control de sistemas, entre otros, lo que puede tener consecuencias graves para las organizaciones y los usuarios. La comprensión de las vulnerabilidades y sus causas es fundamental para implementar medidas de seguridad efectivas y proteger la integridad y confidencialidad de la información (Vaca y Narvaez, 2019).

Factor Humano. - La seguridad en el ámbito informático tiene una dependencia significativa del componente humano, superando incluso a la influencia de la tecnología en este aspecto. Se destaca que el usuario constituye el eslabón más frágil en la protección contra el fraude y en la garantía de la seguridad de los sistemas informáticos en cualquier entidad. Asimismo, se enfatiza que las aplicaciones y estrategias de seguridad en Tecnologías de la Información (TI) que previenen el fraude solo serán adoptadas por las empresas si perciben claramente los beneficios que ofrecen en relación con su costo. Además, se estima que una gran mayoría, aproximadamente el 82%, de los datos confidenciales de una empresa son generados por sus propios empleados. En conclusión, los expertos coinciden en señalar que el eslabón más vulnerable en la cadena de seguridad de TI es el usuario final, dado su desconocimiento, falta de cultura de seguridad y escasa conciencia sobre los riesgos asociados (Vaca y Narvaez, 2019).

Ataques Informáticos. - Los ciberataques buscan obtener ganancias a través del daño financiero a individuos y organizaciones. Estos ataques se originan por programas maliciosos, conocidos como malware. En respuesta, las empresas implementan estrategias de prevención basadas en el conocimiento actualizado de seguridad informática. El objetivo es identificar los tipos de ataques más comunes para comprender su funcionamiento y minimizar su impacto en la seguridad de la información. Sin embargo, la principal debilidad en la seguridad digital reside en el factor humano (Guilcapi, 2023).

Importancia de la seguridad de los datos. - La relevancia de la seguridad de los datos radica en salvaguardar y anticipar posibles incidentes relacionados con la información almacenada por las organizaciones. En la actualidad, los datos son esenciales para diversas áreas laborales, incluido el análisis de datos que respalda la formulación de estrategias de marketing basadas en dicha información (Vaca y Cueva, 2022).

2.2 Descripción de la Propuesta

La propuesta surge considerando la necesidad de fortalecer la seguridad de los datos sensibles en Inforc, una empresa comprometida con la protección de sus activos digitales. Se propone la implementación de un software como Safetica, que se alinea con estándares óptimos y regulaciones

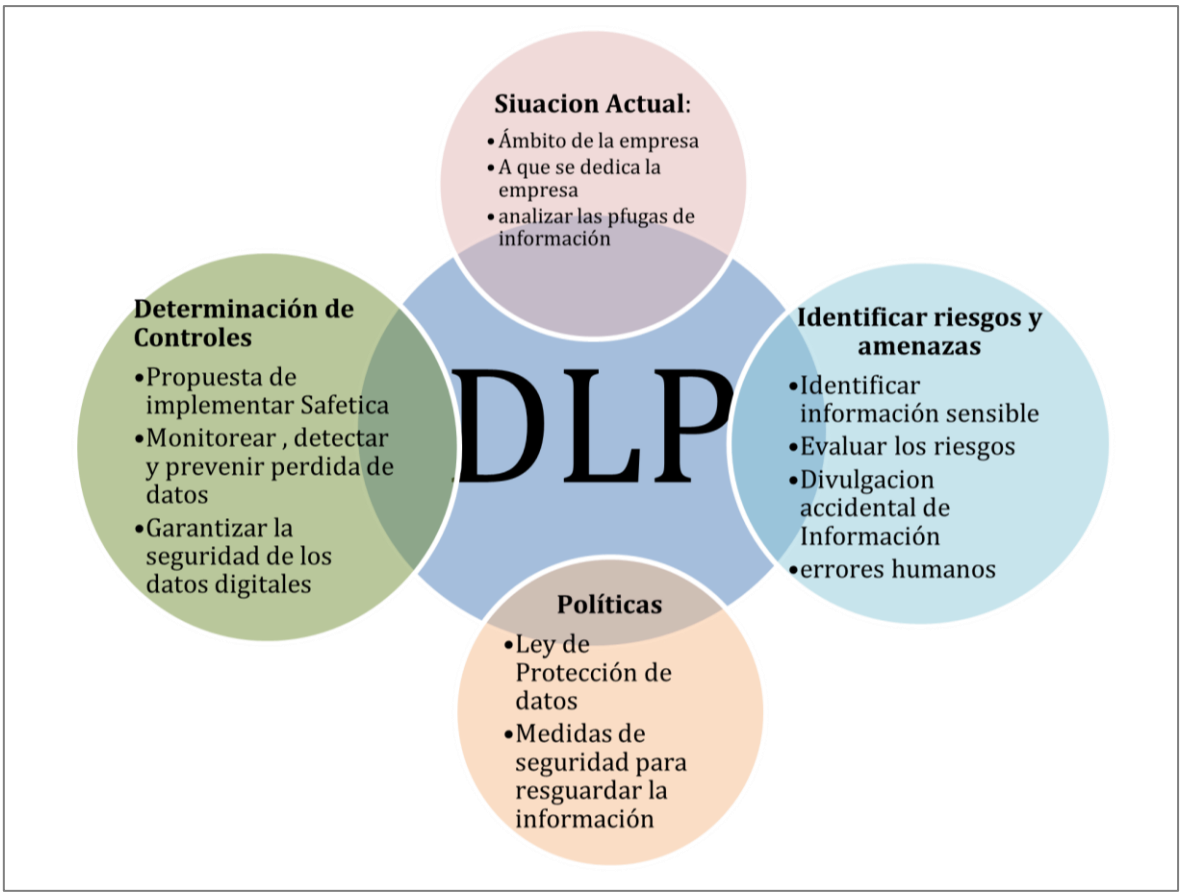
vigentes. El objetivo principal de este plan es promover prácticas efectivas que contribuyan a establecer un sistema empresarial sólido y completo. Safetica se plantea como una solución DLP que permita monitorear, detectar y prevenir la pérdida de datos sensibles, además de establecer políticas y procedimientos de seguridad que cumplan con las regulaciones vigentes y promuevan una cultura de seguridad informática dentro de la organización.

Estructura general

La propuesta se va a hacer según el diagrama que se encuentra en la Figura 6 la misma que contine las siguientes fases.

Figura 6

Estructura General de un DLP



Explicación del aporte

El aporte de la propuesta de implementar un plan estratégico de Prevención de Pérdida de Datos (DLP) mediante Safetica en la empresa Inforc radica en varios aspectos clave:

Seguridad de la Información Mejorada:

La implementación de Safetica como una solución DLP permitirá a Inforc fortalecer la seguridad de su información sensible. Esto incluye la capacidad de monitorear, detectar y prevenir la pérdida de datos, lo que ayuda a proteger la integridad de los activos digitales de la empresa.

Cumplimiento Normativo:

En un contexto donde las regulaciones sobre protección de datos son cada vez más estrictas, la implementación de Safetica ayuda a Inforc a cumplir con las normativas vigentes, como la legislación relacionada con la protección de datos personales y la seguridad de la información.

Cultura de Seguridad Informática:

La adopción de Safetica promueve una cultura de seguridad informática dentro de la organización. Al establecer políticas y procedimientos de seguridad, se sensibiliza a los empleados sobre la importancia de proteger la información sensible y se les proporciona las herramientas necesarias para hacerlo.

Beneficios para Clientes y Empleados:

La implementación de Safetica no solo beneficia a Inforc, sino también a sus clientes y empleados. Los clientes confían en la empresa al saber que sus datos están protegidos de manera efectiva, lo que contribuye a construir una relación de confianza. Además, los empleados son capacitados y se les proporcionan herramientas para participar activamente en la seguridad de la información de la empresa.

Impacto en la Sociedad:

La implementación de Safetica va más allá de los límites de la empresa y tiene un impacto en la sociedad en general. Contribuye a una comunidad digital más segura al prevenir la pérdida de datos, reduciendo así los riesgos de robo de identidad, fraude financiero y otros delitos cibernéticos que pueden afectar a individuos y comunidades enteras.

2.3. Validación de la Propuesta

Basados en la contextualización del tema y en la descripción de la propuesta presentada, la validación de la propuesta de implementar un plan estratégico de Prevención de Pérdida de Datos (DLP) mediante la utilización de Safetica en la empresa Inforc puede llevarse a cabo de la siguiente manera: Se debe realizar una evaluación exhaustiva de los riesgos y vulnerabilidades asociados con la seguridad de la información en Inforc. Esto implica identificar los posibles puntos de fuga de datos, tanto internos como externos, así como los factores humanos y tecnológicos que contribuyen a la

problemática. Se debe analizar detalladamente la propuesta presentada, incluyendo la descripción de Safetica como solución DLP, los objetivos específicos del plan estratégico, la metodología de implementación y los beneficios esperados tanto para la empresa como para la sociedad en general. Es importante evaluar la viabilidad técnica, financiera y operativa de implementar Safetica en Inforc. Esto implica considerar aspectos como el costo de adquisición e implementación, la capacidad técnica para integrar la solución en la infraestructura existente de la empresa, y la disponibilidad de recursos humanos para administrar y mantener el sistema. Se deben analizar y cuantificar los beneficios esperados de la implementación de Safetica, tanto a corto como a largo plazo. Esto incluye la mejora en la seguridad de la información, el cumplimiento normativo, la promoción de una cultura de seguridad informática y el impacto en los clientes, empleados y la sociedad en general. Se debe desarrollar un plan detallado para la implementación de Safetica en Inforc, que incluya la asignación de responsabilidades, el cronograma de actividades, los recursos necesarios y los indicadores clave de rendimiento para evaluar el éxito del proyecto.

Para evaluar la viabilidad y el éxito de la propuesta de implementar Safetica como un sistema de prevención de pérdida de datos (DLP) en Inforc, se establecen los siguientes criterios de validación, con profesionales especializados en el campo de la seguridad informática. Los hallazgos de este análisis se incluirán en la sección de anexos del documento, según lo propuesto por los especialistas.

Tabla 2

Perfil expertos

Especialista	Años de Experiencia	Estudios académicos	Cargo
MSc. Francisco Changotasi	3	Ing. En Electrónica y Telecomunicaciones Master en Telecomunicaciones con mención en Gestión de las Telecomunicaciones	Especialista de seguridad de Redes
Ing. John Edison Muñoz Arciniegas	9	Ing. En Electrónica y Telecomunicaciones	Especialista de Seguridad de la Información

Nota: Autoría propia. Detalle del perfil de expertos en la validación de la propuesta. Ver Tabla 2.

.

2.3.1. Criterios Técnicos:

2.3.1.1. Eficacia en la Prevención de Pérdida de Datos:

- **Reducción en el número de incidentes de fuga de datos:**
  - Medición del porcentaje de disminución en la cantidad de casos de pérdida de información confidencial antes y después de la implementación de Safetica.
  - Análisis comparativo de la frecuencia e impacto de las fugas de datos en un período determinado.
- **Detección precisa de fugas de datos:**
  - Evaluación de la capacidad de Safetica para identificar y alertar sobre la pérdida de información sensible en tiempo real.
  - Análisis de la precisión y confiabilidad de las alertas generadas por el sistema.
- **Prevención de fugas intencionales y accidentales:**
  - Verificación de la eficacia de Safetica en la detección y bloqueo de intentos de exfiltración de datos, tanto por parte de usuarios internos como externos.
  - Evaluación de la capacidad del sistema para prevenir la pérdida de datos por errores humanos o negligencia.

2.3.1.2. Cumplimiento de Regulaciones:

- **Adaptación a las normas locales e internacionales:**
  - Verificación de que las funcionalidades de Safetica se ajustan a las regulaciones ecuatorianas y a los estándares internacionales de protección de datos como GDPR e ISO 27001.
  - Evaluación del cumplimiento de las políticas y procedimientos internos de Inforc con respecto a la seguridad de la información.

2.3.1.3. Integración con la Infraestructura Tecnológica:

- **Compatibilidad con sistemas existentes:**
  - Verificación de la compatibilidad de Safetica con los sistemas informáticos, hardware y software, utilizados en Inforc.
  - Evaluación de la capacidad del sistema para integrarse a la arquitectura tecnológica actual sin afectar su funcionamiento.

2.3.1.4. Facilidad de Uso y Administración:

- **Interfaz intuitiva y amigable para los usuarios:**
  - Evaluación de la facilidad de uso y comprensión de la interfaz de Safetica por parte

de los empleados con diferentes niveles de experiencia tecnológica.
    - Análisis de la curva de aprendizaje y la necesidad de capacitación para el uso eficiente del sistema.

- **Administración eficiente por parte del equipo de IT:**
    - Verificación de la facilidad de gestión y configuración del sistema por parte del personal de TI de Inforc.
    - Evaluación de la disponibilidad de herramientas y recursos para la administración eficiente de Safetica.

2.3.2. Criterios Empresariales:

2.3.2.1. Retorno de la Inversión (ROI):

- **Reducción de costos asociados a la pérdida de datos:**
    - Análisis del impacto financiero de la implementación de Safetica en la prevención de fugas de información.
    - Cálculo del ROI a partir de la reducción de costos por multas, daños a la reputación y recuperación de datos.

- **Mejora en la productividad y eficiencia:**
    - Evaluación del impacto de Safetica en la optimización del tiempo y recursos empleados en la gestión de la seguridad de la información.
    - Análisis del aumento de la productividad por la disminución de interrupciones y tiempo de inactividad debido a incidentes de fuga de datos.

2.3.2.2. Aceptación y satisfacción de los usuarios:

- **Percepción positiva del sistema por parte de los empleados:**
    - Medición del nivel de satisfacción y aceptación de Safetica por parte de los usuarios finales.
    - Evaluación de la utilidad y facilidad de uso del sistema para el desempeño de las tareas cotidianas.

2.3.2.3. Fortalecimiento de la Cultura de Seguridad Informática:

- **Mayor conciencia sobre la importancia de la protección de datos:**
    - Evaluación del impacto de Safetica en la sensibilización y el compromiso de los

empleados con la seguridad de la información.

- Análisis del cambio en la cultura organizacional hacia una mayor responsabilidad en el manejo de datos sensibles.

2.3.2.4. Mejora en la Reputación de la Empresa:

- **Mayor confianza por parte de clientes y socios comerciales:**
  - Evaluación del impacto de la implementación de Safetica en la percepción de la empresa como una organización comprometida con la seguridad de la información.
  - Análisis del aumento en la confianza y fidelización de clientes y socios comerciales.

2.3.3. Criterios de Implementación:

2.3.3.1. Cumplimiento del Plan de Implementación:

- **Ejecución exitosa de las fases de planificación, implementación y monitoreo:**
  - Verificación del cumplimiento del cronograma y presupuesto establecidos para la implementación del proyecto.
  - Evaluación de la eficiencia en la gestión de recursos humanos, técnicos y financieros durante el proceso de implementación.

2.3.3.2. Capacitación Efectiva de los Usuarios:

- **Adquisición de habilidades y conocimientos para el uso de Safetica:**
  - Evaluación del nivel de conocimiento y comprensión del sistema por parte de los usuarios finales.
  - Análisis de la efectividad del programa de capacitación en la preparación de los empleados para utilizar Safetica de manera eficiente.

2.3.3.3. Soporte Técnico y Mantenimiento:

- **Disponibilidad de asistencia técnica oportuna y eficaz:**
  - Verificación de la existencia de un plan de soporte técnico para la resolución de problemas e incidentes relacionados con Safetica.
  - Evaluación de la capacidad del equipo de IT para brindar asistencia técnica eficiente a los usuarios.

2.3.3.4. Monitoreo y Evaluación Continua:

- **Análisis del rendimiento y la eficacia de Safetica:**
  - Implementación de un sistema de monitoreo para evaluar el desempeño del

sistema en la prevención de fugas de datos.

- Realización de evaluaciones periódicas para identificar oportunidades de mejora y optimizar la configuración del sistema.

2.3.3.5. Adaptación a Cambios y Actualizaciones:

- **Capacidad para ajustarse a nuevas necesidades y amenazas:**
  - Verificación de la flexibilidad del sistema para adaptarse a cambios en el entorno tecnológico y regulatorio.
  - Evaluación de la capacidad del equipo de IT para actualizar e implementar nuevas funcionalidades en Safetica.

Consideraciones Finales:

La evaluación de la propuesta de implementación de Safetica como un sistema DLP en Inforc debe considerar la ponderación de los criterios mencionados anteriormente, de acuerdo a las prioridades y necesidades específicas de la empresa. La validación exitosa de la propuesta estará sujeta al cumplimiento de los criterios técnicos, empresariales y de implementación, asegurando así la eficacia y el éxito del proyecto en el largo plazo.

2.4. Matriz de Articulación de la Propuesta

Esta matriz resume la integración del plan elaborado con los fundamentos teóricos, metodológicos, estratégico-técnicos y tecnológicos utilizados. Ver Tabla 3.

Tabla 3

Matriz de Articulación

Ejes o partes principales del proyecto	Sustento teórico	Sustento metodológico	Estrategias/técnicas	Descripción de resultados	Instrumentos aplicados
Marco de referencia de estudio ISO/IEC 27001	DLP y el cumplimiento de la Norma ISO 27001 (Safetica, 2024)	La metodología de investigación se basó en la revisión de la literatura especializada que proporciono una comprensión detallada de los conceptos relacionados con la seguridad de la información.	Identificación de riesgos y vulnerabilidades, evaluación de amenazas internas y externas, implementación de controles de seguridad, monitoreo de incidentes, capacitación del personal.	Se espera obtener un análisis exhaustivo de los riesgos de seguridad de la información en el entorno del proyecto, así como la identificación de posibles soluciones y controles para mitigar dichos riesgos.	Revisión de documentos académicos, libros especializados, artículos de revistas científicas.
Encuesta, entrevista al personal seleccionado de Inforc	Investigación cuantitativa	Encuesta	Entrevistas ejecutadas	Se realiza entrevistas para verificar el estado de la información en Inforce	Entrevista
Safetica como solución DLP	Fundamentos DLP (Data Loss Prevention)	Utilización de Safetica como solución DLP para la	Instalación y configuración de Safetica en los sistemas de información de la empresa definición de políticas de	Se espera lograr la implementación efectiva de Safetica, como solución DLP,	Registro de actividades de configuración e instalación, informes de análisis de incidentes,

	prevención de perdida de datos	seguridad, seguimiento y análisis de la actividad de los usuarios, generación de informes de incidentes de seguridad.	reduciendo la incidencia de perdida de datos y mejorando la seguridad de la información de la empresa	registros de políticas de seguridad implementadas.

Nota: Autoría propia

2.5. Análisis de resultados presentación y discusión.

A continuación, se hace un estudio sobre la empresa para conocer el giro de negocio y poder empezar a hacer un inventario de activos y evaluación de los mismos:

2.5.1. Estudio de la empresa

INFORC ECUADOR® fue fundada el año 2005, su objetivo es "ayudar a prevenir y gestionar el riesgo de los clientes frente a las amenazas informáticas" (Inforc Ecuador, 2024). La empresa ofrece una gama de soluciones relacionadas con la seguridad de la información. La empresa cuenta con un "portafolio integral de soluciones que hacen posible lograr una verdadera sociedad de negocio con clientes, que cubren necesidades desde el nivel estratégico hasta el nivel operativo" (Inforc Ecuador, 2024), esto se lo realiza mediante una alineación e integración de las iniciativas e inversiones asociadas con TI a los objetivos de la organización.

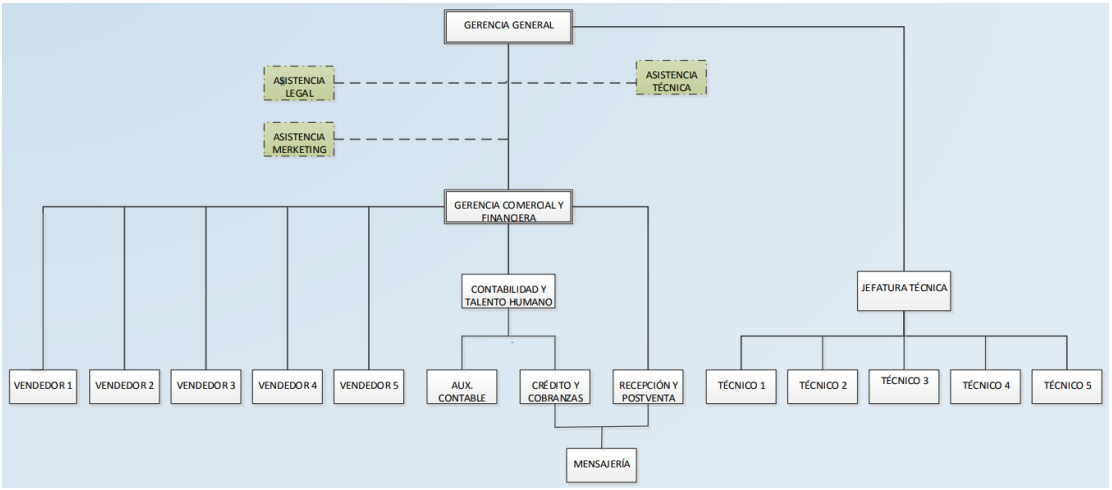
La cultura corporativa se centra en la "seguridad como prioridad, conciencia y formación, colaboración y comunicación, innovación y adaptabilidad, transparencia y responsabilidad" (Inforc Ecuador, 2024). La política de calidad se centra con proveer productos y servicios de ciberseguridad, que cumplan con los requisitos aplicables.

Estructura organizacional

INFORC ECUADOR® tiene el siguiente organigrama estructural en donde se cuenta con una gerencia general, una jefatura técnica, y una gerencia comercial y financiera. Como se detalla en la figura 7.

Figura 6

Organigrama Estructural INFORC ECUADOR



2.5.2. Inventario de Activos

Los activos que posee la empresa se los detalla en la tabla x en la cual se hace una clasificación de acuerdo a su uso por área de trabajo de ahí que se tiene los gerenciales, contabilidad, ventas, técnicos, servidores rack y equipos de escritorio como se detalla en la tabla 4:

Tabla 4

Inventario de activos

INVENTARIO DE ACTIVOS						
Identificador	**Nombre**	**Descripción**	**IP**	**Tipo**	**Ubicación**	**Crítico**
			GERENCIA			
ID_0001	Portátil 01 (Gerencia)	Gerencia	192.168.0.110	Portátil (física)	Departamento Gerencia	si
ID_0002	Portátil 02 (Presidente)	Presidente	192.168.0.104	Portátil (física)	Departamento Presidencia	si
			CONTABILIDAD			
ID_0003	Computador 03 (Contabilidad)	contabilidad.	192.168.0.113	Computador (físico)	Departamento Contabilidad	Sí
ID_0004	Computador 04 (Asistente Contabilidad)	Asistente Contable	192.168.0.119	Computador (físico)	Departamento Contabilidad	si
			VENTAS			
ID_0006	Computador 06 (Ventas 1)	Ventas	192.168.0.102	Computador (físico)	Ventas	si
ID_0007	Computador 07 (Ventas 2)	Ventas	192.168.0.106	Computador (físico)	Ventas	si
ID_0008	Portátil HP 08 (Ventas)	Ventas Presentaciones	DHCP	Portátil (física)	Ventas	si
			TÉCNICOS			
ID_0012	Computador 12 (Técnico)	Soporte Técnico	192.168.0.107	Computador (físico)	Soporte	si
ID_0013	Computador 13 (Técnico)	Soporte Técnico	192.168.0.1112	Computador (físico)	Soporte	si
ID_0014	Computador 14 (Técnico)	Soporte Técnico	192.168.0.1115	Computador (físico)	Soporte	si
			SERVIDORES RACK			
ID_0016	Servidor 16 (Contable)	Contabilidad	192.168.0.203	Servidor (físico)	Rack	si

ID_0017	Servidor Seagate 17 (Backup)	Backup Información Gerencia	192.168.0.205	Servidor (físico)	Rack	si
ID_0018	Servidor Synology 18 (Backup)	Backup Información Usuarios	192.168.0.202	Servidor (físico)	Rack	si
ID_0019	Servidor GPO 150 19(Firewall)	Firewall	192.168.0.254	Servidor (físico)	Rack	si
ID_0020	Router Ubiquiti 20 (Wireless)	Router Internet	192.168.0.20	Router (físico)	Rack	si
ID_0021	Swith D-LINK 24 PUERTOS 21	Swith	-	Swith	Rack	si
ID_0022	Central Telefónica Panasonic	Central Telefonica	-	Central Telefónica	Rack	si
		EQUIPOS ESCRITORIO				
ID_0022	Servidor Synology 22 (Demos)	Backup Demos	192.168.0.189	Servidor (físico)	Escritorio	si
ID_0023	Portátil Acer 23 (Técnico)	Implementaciones Firewall	DHCP	Portátil (física)	Escritorio	si
ID_0024	Portátil HP 24 (Técnico)	Implementaciones Firewall	DHCP	Portátil (física)	Escritorio	si
ID_0025	Portátil DELL 25 (Técnico)	Implementaciones Firewall	DHCP	Portátil (física)	Escritorio	si
ID_0025	Impresora Xerox	Impresora Red	192.168.0.210	Impresora (Red)	Escritorio	si
ID_0026	Impresora Samsung	Impresora Compartida	-	Impresora	Escritorio	si
ID_0027	Impresora EPSON LX-500	Impresora Compartida	-	Impresora	Escritorio	si

Una vez identificados los activos se procede a hacer una valoración en cuanto a disponibilidad, integridad y confidencialidad para lo que usa como referencia la siguiente escala presentada en la tabla 5:

Tabla 5

Escala para valoración de activos

Escala	Valor
Bajo	1
Medio	2
Alto	3
Crítico	4

Nota: En la tabla anterior se muestra la tabla de valoración que se usara para los activos. Tomado de Pandini (2015)

Luego se procede a hacer la valoración de los activos para determinar los más importantes para la organización como se muestra en la tabla 6, se lo realiza con el jefe de TI ya que el tiene mayor conocimiento del negocio de ahí que se considera un valoración baja cuando el activo no maneje información considera como importante para la empresa, medio cuando se maneje poca información, alto cuando el flujo de información sea mayor y críticos aquellos activos en los que se maneje la información más importante para la empresa y que además si ocurriera algún incidente afectaría directamente el funcionamiento de la misma:

Tabla 6

Valoración de activos

INVENTARIO DE ACTIVOS					
Identificador	**Nombre**	**Disponibilidad**	**Integridad**	**Confidencialidad**	**Criticidad**
GERENCIAL					
ID_0001	Portátil 01 (Gerencia)	4	4	4	4
ID_0002	Portátil 02 (Presidente)	4	4	4	4
CONTABILIDAD					
ID_0003	Computador 03 (Contabilidad)	4	4	4	4
ID_0004	Computador 04 (Asistente Contabilidad)	4	4	3	3.66
VENTAS					
ID_0006	Computador 06 (Ventas 1)	4	3	3	3.33
ID_0007	Computador 07 (Ventas 2)	4	3	3	3.33
ID_0008	Portátil HP 08 (Ventas)	4	3	3	3.33
TÉCNICOS					
ID_0012	Computador 12 (Técnico)	4	3	3	3.33
ID_0013	Computador 13 (Técnico)	4	3	3	3.33
ID_0014	Computador 14 (Técnico)	4	3	3	3.33
SERVIDORES RACK					
ID_0016	Servidor 16 (Contable)	4	4	3	3.66
ID_0017	Servidor Seagate 17 (Backup)	4	4	4	4
ID_0018	Servidor Synology 18 (Backup)	4	4	3	3.66

ID_0019	Servidor GPO 150 19(Firewall)	4	4	4	4
ID_0020	Router Ubiquiti 20 (Wireless)	4	3	3	3.33
ID_0021	Swith D-LINK 24 PUERTOS 21	4	3	3	3.33
ID_0022	Central Telefónica Panasonic	4	4	3	3.66
	EQUIPOS ESCRITORIO				
ID_0022	Servidor Synology 22 (Demos)	4	4	4	4
ID_0023	Portátil Acer 23 (Técnico)	4	3	3	3.33
ID_0024	Portátil HP 24 (Técnico)	4	3	3	3.33
ID_0025	Portátil DELL 25 (Técnico)	4	3	3	3.33
ID_0025	Impresora Xerox	4	3	2	3
ID_0026	Impresora Samsung	4	2	2	2.66
ID_0027	Impresora EPSON LX-500	4	2	2	2.66

Una vez realizada la valoración de activos se encontró que los activos críticos son del área gerencial la portátil 1 y 2 del área de contabilidad el computador 3, de los servidores rack se encontró el servidor Seagate 17 y el servidor GPO 150 19, y los equipos de escritorio se tiene el servidor Synology 22. (tabla 7)

Tabla 7

Valoración de activos críticos

VALORACIÓN DE ACTIVOS					
Identificador	**Nombre**	**Disponibilidad**	**Integridad**	**Confidencialidad**	**Criticidad**
	GERENCIAL				
ID_0001	Portátil 01 (Gerencia)	4	4	4	4
ID_0002	Portátil 02 (Presidente)	4	4	4	4
	CONTABILIDAD				
ID_0003	Computador 03 (Contabilidad)	4	4	4	4
	SERVIDORES RACK				
ID_0017	Servidor Seagate 17 (Backup)	4	4	4	4
ID_0019	Servidor GPO 150 19(Firewall)	4	4	4	4
	EQUIPOS ESCRITORIO				
ID_0022	Servidor Synology 22 (Demos)	4	4	4	4

2.5.3. Identificación de amenazas y estimación de riesgos

En los activos identificados cómo críticos para la organización se procede a identificar las posibles amenazas con las amenazas expuestas en la tabla 8 y posteriormente la estimación de riesgos.

Tabla 8

Amenazas

Amenaza	Código
Daño físico	DF
Eventos naturales	EN
Compromiso de la información	CI
Fallas técnicas	FT
Nivel de datos y redes	NDR
Acciones no autorizadas	ANA
Compromiso de las funciones	CF
Factor humano	FH

Nota: En la tabla anterior se muestra las posibles amenazas. Tomado de ISO 27005

Una vez identificadas las amenazas se procede a identificar en cada activo considerado como crítico cada amenaza de acuerdo a la escala presentada en la tabla 9:

Tabla 9:

Valoración de riesgos

Criterio	Valor		
Riesgo bajo	0	-	2
Riesgo medio	3	-	5
Riesgo alto	6	-	8

Nota: En la tabla anterior se muestra la tabla de valoración que se usara para las amenazas. Tomado de ISO 27005

Con la tabla anterior se procede a valorar el riesgo que presenta cada activo como se detalla en la tabla 10.

Tabla 10:

Valoración de riesgos

Nombre	DF	EN	CI	FT	NDR	ANA	CF	FH
Portátil 01 (Gerencia)	3	3	6	4	6	7	2	7
Portátil 02 (Presidente)	3	3	6	4	7	7	2	8
Computador 03 (Contabilidad)	3	3	5	5	7	8	6	7
Servidor Seagate 17 (Backup)	4	3	8	5	8	8	7	8
Servidor GPO 150 19(Firewall)	5	3	8	6	8	7	8	8
Servidor Synology 22 (Demos)	5	3	8	6	8	7	8	8
Promedio	**3.83**	**3.00**	**6.83**	**5.00**	**7.33**	**7.33**	**5.50**	**7.66**

De la valoración de riesgos se identificó que existe mayor riesgo relacionado con compromiso de la información con un 6.83 lo que indica que existen riesgos altos, a nivel de datos y redes se obtuvo

7.33 al igual que acciones no autorizadas, y finalmente se encontraron riesgos relacionados con factores humanos con un 7.66.

2.5.4. Identificación de vulnerabilidades

Una vez identificados los riesgos a los cuales están expuestos los activos más importantes de la organización se procede a hacer un escaneo de vulnerabilidades mediante una herramienta que identifique vulnerabilidades y que además indique las medidas a hacerse para mitigarlas o eliminarlas y que no puedan ocasionar daños en la organización. Para ello se presenta la comparativa hecha en la tabla 11.

Tabla 11:

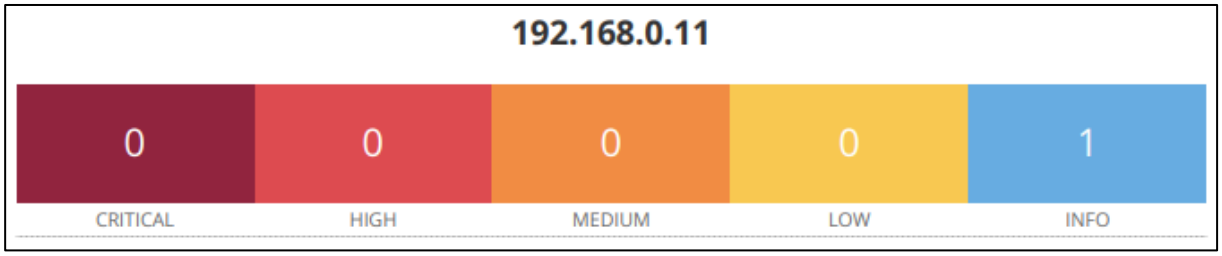
Tabla comparativa herramientas

Característica	Nessus	GFI Landward	Wireshark
Fácil de usar	4	4	4
Detección avanzada	4	4	3
Para todo tipo de empresas	3	4	4
Escaneo web	4	4	4
Administración de políticas	4	4	3
Priorización y evaluación de vulnerabilidades	4	4	4
Buenas prácticas	4	4	4
Permite crear informes sobre los tipos de vulnerabilidades; exportarlos en distintos formatos de archivos CSV, HTML y XML	4	4	3
Transparencia en los procesos	4	4	4
Ordenar los datos por cliente o equipo	4	0	0
Evaluaciones de vulnerabilidades en modo offline para detectar, validar y priorizar los problemas	4	0	0
Versión de prueba gratuita	4	0	0
Total	**47**	**36**	**33**

Al ser Nessus la herramienta que más se aproxima a las necesidades del estudio se procede a tomarla como referencia para el estudio y los resultados se muestran a continuación en la figura 7:

Figura 7

Escaneo computadora gerencial

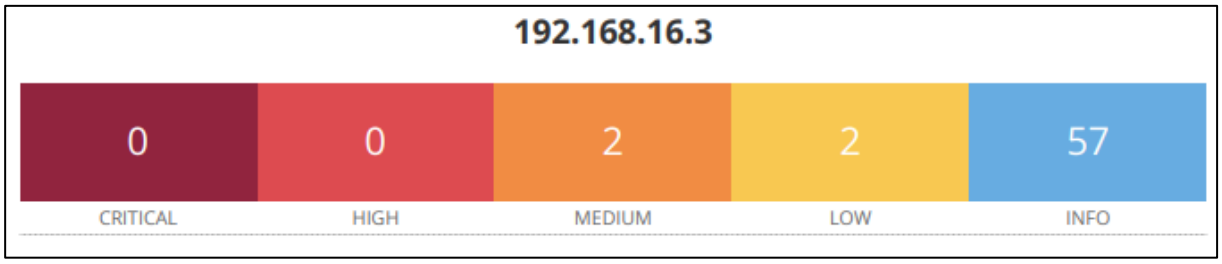


Al realizar el escaneo de vulnerabilidades se encontró que la laptop permite hacer ping al host remoto de ahí que se obtuvo que:

- “Un ping ARP, siempre que el host esté en la subred local y Nessus se esté ejecutando a través de Ethernet”.
- Un ping ICMP.
- “Un ping TCP, en el que el complemento envía al host remoto un paquete con el indicador SYN, y el host responderá con un RST o un SYN/ACK”.
- Un ping UDP.

Figura 8

Escaneo computadora contabilidad

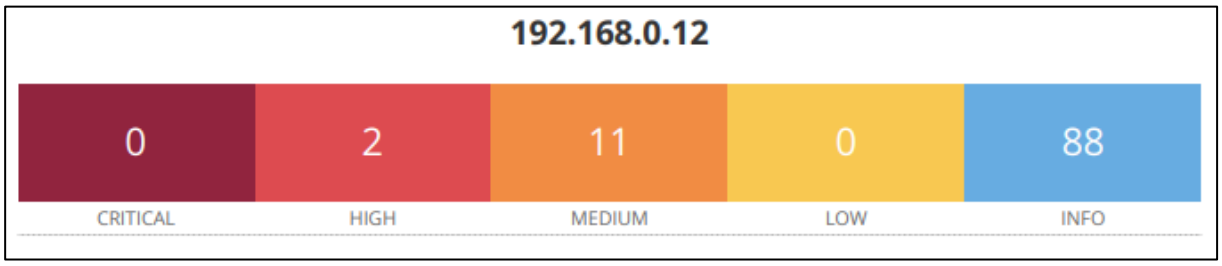


Al hacer el escaneo en la computadora de contabilidad (figura 8) se encontró que existen dos vulnerabilidades medias, 2 bajas y 57 relacionadas con la información lo que indica que el servidor SSH remoto es vulnerable a un ataque de truncamiento del hombre del medio. Para ello la herramienta recomienda que se pongan “en contacto con el proveedor para obtener una actualización de las estrictas contramedidas de intercambio de claves o deshabilite los algoritmos afectados” (Nessus, 2024).

También se encontró que el servidor SSH está configurado para utilizar Cipher Block Chaining la solución es consultar con el “proveedor o consultar la documentación del producto para deshabilitar el cifrado de modo CBC y habilitar el cifrado de modo de cifrado CTR o GCM”. Por otro lado, se encontró que el servidor “SSH remoto está configurado para permitir algoritmos de intercambio de claves débiles” (Nessus, 2024), cuya solución es desactivar los algoritmos débiles.

Figura 9

Escaneo Servidor Seagate 17



El servidor Seagate 17 (figura 9) mostro dos vulnerabilidades consideradas como altas, 11 medias y 88 relacionadas con la información la herramienta recomienda que se vuelva a configurar el servicio remoto para evitar el uso de cifrados de intensidad media. También se encontró que "el servicio remoto admite el uso de cifrados SSL de potencia media" para corregir esta vulnerabilidad se recomienda que se "vuelva a configurar la aplicación afectada si es posible para evitar el uso de cifrados de intensidad media" (Nessus, 2024).

Por otro lado, se encontró que "el host remoto admite el uso de RC4 en uno o más conjuntos de cifrado. El cifrado RC4 tiene fallas en la generación de un flujo pseudoaleatorio de bytes, de modo que se introduce una amplia variedad de pequeños sesgos en el flujo, lo que disminuye su aleatoriedad" (Nessus, 2024).

Si el texto sin formato se cifra repetidamente (por ejemplo, cookies HTTP) y un atacante puede obtener muchos (es decir, decenas de millones) de textos cifrados, es posible que pueda derivar el texto sin formato.

Figura 10

Escaneo Servidor GPO 150 19 (Firewall)

Al hacer el escaneo en el Servidor GPO 150 19 (Firewall) se encontraron las vulnerabilidades de la figura 11, de las cuales dos son consideradas como altas, 3 medias, 2 bajas y 48 relacionadas con la información.

Las vulnerabilidades altas se relacionan con "la aplicación web que se ejecuta en el servidor web remoto se ve afectada por una vulnerabilidad de omisión de seguridad".

“La vulnerabilidad afecta las instancias de Grafana con varias organizaciones y permite a un usuario con permisos de administrador de la organización en una organización cambiar los permisos asociados con los roles de visor de organización, editor de organización y administrador de la organización en todas las organizaciones. También permite que un administrador de la organización asigne o revoque cualquier permiso que tenga para cualquier usuario a nivel mundial. Esto significa que cualquier administrador de la organización puede elevar sus propios permisos en cualquier organización de la que ya sea miembro, o elevar o restringir los permisos de cualquier otro usuario”. La vulnerabilidad no permite que un usuario se convierta en miembro de una organización de la que aún no es miembro, ni agregue otros usuarios a una organización de la que el usuario actual no es miembro. (Nessus, 2024)

La solución para la vulnerabilidad es que “actualice a Grafana 9.4.17, 9.5.13, 10.0.9, 10.1.5 o posterior” (Nessus, 2024).

2.5.5. Matriz de riesgos

La matriz de riesgos permite observar cada uno de los riesgos identificados en ella se encuentra de tallado el número de riesgo, la frecuencia de ocurrencia, la severidad del daño, el impacto y el tratamiento que debe de darse para ello se toma como referencia el análisis de vulnerabilidades mediante Nessus como se muestra en el anexo 3, tabla 2.

2.5.6. Implementación de herramienta DLP

Las herramientas de DLP empresarial tienen la capacidad de descubrir, inventariar y clasificar automáticamente datos confidenciales y sus metadatos. Los datos se crean y cambian constantemente, por lo que a una herramienta DLP que no puede seguir el ritmo de posibles fugas de datos siempre le faltan cosas. Además, tienen la capacidad de utilizar varios tipos de análisis para encontrar problemas con precisión. Todo análisis debe tener en cuenta el contexto de la comunicación porque una actividad que es completamente normal en un contexto puede resultar muy sospechosa en otro. (De Groot, 2023) De ahí que se procede a hacer una comparativa de herramientas para encontrar la más adecuada para la presente investigación, como se muestra en la tabla 12, en donde 4 indica que cubre todas las necesidades de la investigación, 3 que lo hacen parcialmente, 2 lo hacen rara vez, 1 no lo hacen.:

Tabla 12:

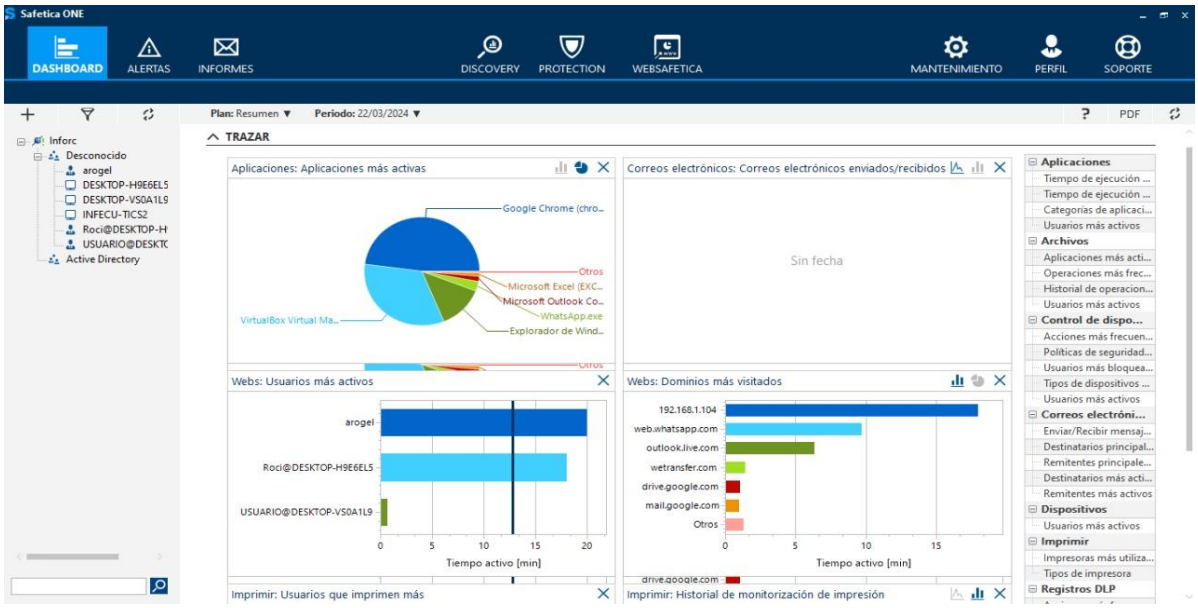
Tabla comparativa herramientas DLP

Característica	Safetica DLP	McAfee Total Protection for DLP	Endpoint Protector DLP
Análisis de contenido mediante palabras clave específicas	4	3	4
Auditoría de seguridad	4	4	3
Protección de datos en la nube	4	3	4
Escaneo web	4	4	4
Administración de políticas	4	3	3
Conjunto de modos informativos y alertas a los empleados que proporcionan un control total del entorno de la empresa y crean conciencia por parte del usuario.	4	4	2
Buenas prácticas	3	4	4
Clasificación de datos que ayuda a identificar y clasificar los datos	3	4	3
Cifrado, redirección, cuarentena o bloqueo de las transmisiones de datos que infringen las políticas de la empresa	3	4	2
Ordenar los datos por cliente o equipo	4	3	3
Evaluaciones de vulnerabilidades en modo offline para detectar, validar y priorizar los problemas	4	2	3
Consola centralizada para la gestión de políticas e incidentes	3	2	3
Versión de prueba gratuita	4	3	3
Total	**48**	**43**	**41**

Una vez hecho el análisis de las herramientas DLP se llegó a la conclusión que Safetica DLP es la que proporciona las mejores herramientas y es por ello que se la usa para el desarrollo de la investigación y se procede a hacer un barrido en la empresa con la herramienta seleccionada, de lo que se obtuvo los siguientes resultados de la figura 11:

Figura 11

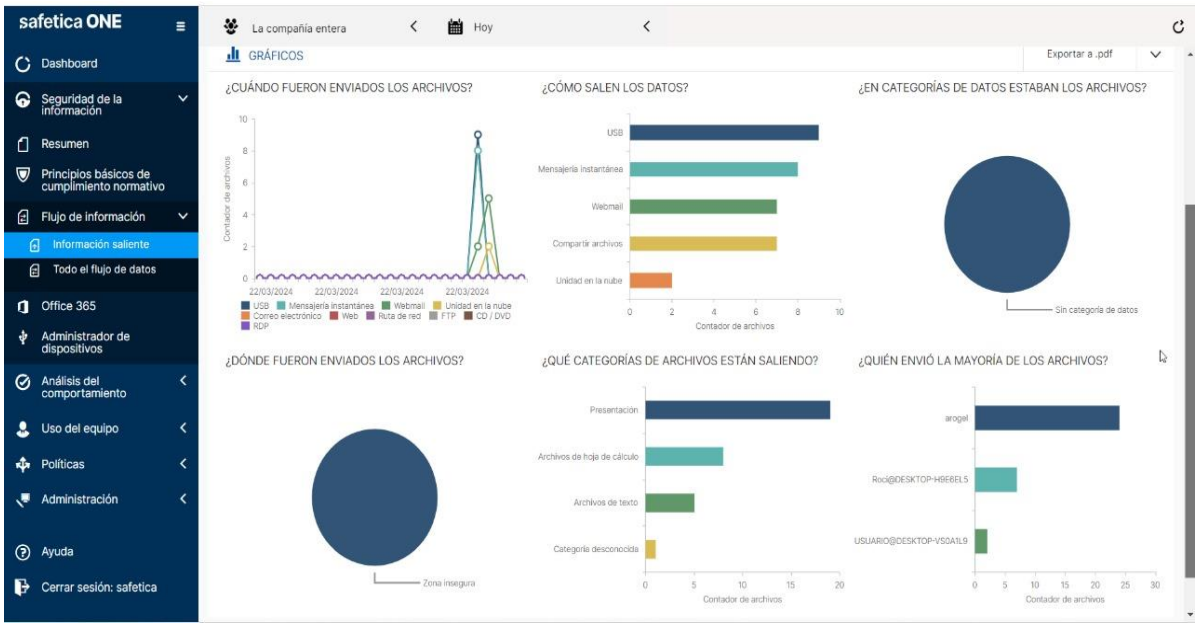
Escaneo Safetica DLP



En la figura 11 se puede ver las aplicaciones más activas de lo cual se tiene que Google Chrome es una de las aplicaciones más usadas, al analizar los usuarios más activos se encontró que arogel fue uno de los usuarios más activos, también no se encontraron correos electrónicos enviados, mientras que en el uso de medios electrónicos se tienen que la dirección IP 192.168.1.104 fue la que imprimió mayor cantidad de documentos.

Figura 12

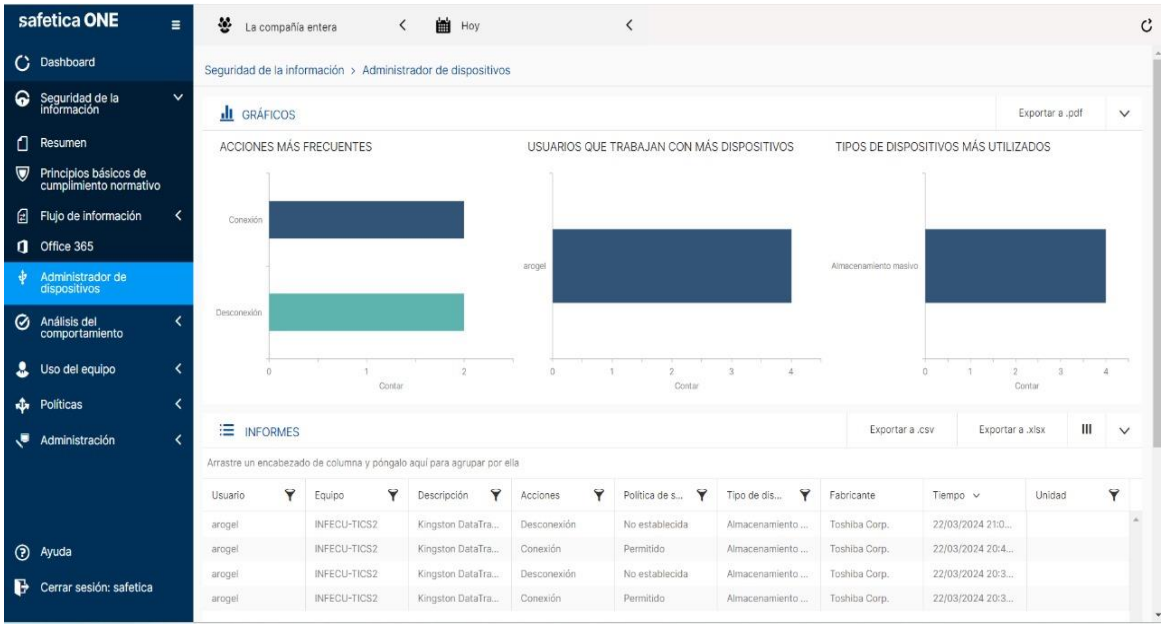
Escaneo Safetica DLP sobre información saliente



Por otro lado, la figura 12 muestra que la mayor parte de información sale por USB, además que los archivos no se encuentran clasificados, entre las categorías se encontró que las presentaciones son las más usadas. Esta herramienta también muestra la persona que usa la mayor parte de la información.

Figura 13

Escaneo Safetica DLP sobre información saliente



En la figura 13 se muestra el administrador de dispositivos, y entre los principales resultados se tiene que las acciones más frecuentes son la conexión y desconexión, también muestra el flujo de trabajo de los usuarios y los tipos de dispositivos más usados que son los de almacenamiento. En esta parte la herramienta permite descargar informes relacionados con los usuarios, los equipos la descripción, las acciones, las políticas de seguridad, los tipos de dispositivos, el fabricante y el tiempo de uso.

Safetica también proporcionan informes en exel como se muestra en la tabla 13.

Tabla 13:

Registros DLP

Usuario	Acción	Operación	Archivo	Aplicación	Desde	Tipo de fuente	Riesgo	Destino	Tipo de destino	Dispositivo de destino	Tamaño [B]	Módulos
arogel	Registro	MI - Enviar archivo	ORGANIGAMA INFORC.pdf	WhatsApp.exe	22/3/2024 20:36	Ruta local	Sí		Mensajería instantánea		228053	Registros DLP
arogel	Registro	Subir a la web	comprobante (3).pdf	Google Chrome (chrome.exe)	22/3/2024 20:37	Ruta local	No	mail.google.com/mail/u/0/%23inbox%3Fcompose%3DGTvVlcSKhphdPBhlfZBwnqwvffDCQzgZJWkLsHhpmScJjQdBwsXpwbdBghpcVzHCjDRQVFqDNhJNv	Correo web		27817	Registros DLP
arogel	Registro	Copiar	ORGANIGRAMA.xls	Explorador de Windows (explorer.exe)	22/3/2024 20:45	Ruta local	Sí	D:\Informacion conf\ORGANIGRAMA.xls	USB	Kingston DataTraveler 2.0 USB Device (0930-6545-1C1B0D6C1C01B341D963D9BB)	84992	Registros DLP
arogel	Registro	Copiar	plan_de_seguridad__inventario_activos.xlsx	Explorador de Windows (explorer.exe)	22/3/2024 20:45	Ruta local	Sí	D:\Informacion conf\plan_de_seguridad__inventario_activos.xlsx	USB	Kingston DataTraveler 2.0 USB Device (0930-6545-1C1B0D6C1C01B341D963D9BB)	51907	Registros DLP
arogel	Registro	Copiar	CONVOCATORIA SEGURIDAD INFORMATICA.xlsx	Explorador de Windows (explorer.exe)	22/3/2024 20:45	Ruta local	Sí	D:\Informacion conf\CONVOCATORIA SEGURIDAD INFORMATICA.xlsx	USB	Kingston DataTraveler 2.0 USB Device (0930-6545-1C1B0D6C1C01B341D963D9BB)	74301	Registros DLP
arogel	Registro	MI - Enviar archivo	Informe Técnico Sophos Email COAC CHONE LTDA - signed.pdf	WhatsApp.exe	22/3/2024 20:46	Ruta local	Sí		Mensajería instantánea		668996	Registros DLP

arogel	Registro	MI - Enviar archivo	ORGANIGAMA INFORC.pdf	WhatsApp.exe	22/3/2024 20:46	Ruta local	Sí		Mensajería instantánea		228053	Registros DLP
arogel	Registro	Subir a la web	Gastos Viaje.xlsx	Google Chrome (chrome.exe)	22/3/2024 20:47	Ruta local	Sí	wetransfer.com	Compartir archivos		28654	Registros DLP
arogel	Registro	Copiar	Registros DLP_2024_3_22.xls	Explorador de Windows (explorer.exe)	22/3/2024 20:51	Ruta de red	Sí	D:\Informacion conf\Registros DLP_2024_3_22.xls	USB	Kingston DataTraveler 2.0 USB Device (0930-6545-1C1B0D6C1C01B341D963D9BB)	23040	Registros DLP
arogel	Registro	Copiar	Registros DLP_2024_3_22.pdf	Explorador de Windows (explorer.exe)	22/3/2024 20:51	Ruta de red	Sí	D:\Informacion conf\Registros DLP_2024_3_22.pdf	USB	Kingston DataTraveler 2.0 USB Device (0930-6545-1C1B0D6C1C01B341D963D9BB)	809410	Registros DLP
arogel	Registro	MI - Enviar archivo	[INFECU]Ampliación_Licenciamiento_de_consola_ESET_GAD PROVINCIAL DE NAPO.docx	WhatsApp.exe	22/3/2024 20:55	OneDrive Business	No		Mensajería instantánea		1090780	Registros DLP
arogel	Registro	MI - Enviar archivo	[INFECU]Ampliación_Licenciamiento_de_consola_ESET_GAD PROVINCIAL DE NAPO.pdf	WhatsApp.exe	22/3/2024 20:55	OneDrive Business	No		Mensajería instantánea		692448	Registros DLP
arogel	Registro	MI - Enviar archivo	[INFECU]Actualización_de_consola_ESET_Banco Ecuatoriano de la Vivienda.docx	WhatsApp.exe	22/3/2024 20:55	OneDrive Business	No		Mensajería instantánea		1851042	Registros DLP

arogel	Registro	MI - Enviar archivo	[INFECU]Actualización_de_consola_ESET_Nucleo de Solca Machala.docx	WhatsApp.exe	22/3/2024 20:55	Ruta local	No		Mensajería instantánea	971663	Registros DLP
Roci@DESKTOP-H9E6EL5	Registro	Subir a la web	CarteraPorCobrar (2).xls	Google Chrome (chrome.exe)	22/3/2024 21:06	Ruta local	Sí	wetransfer.com	Compartir archivos	26112	Registros DLP
Roci@DESKTOP-H9E6EL5	Registro	Subir a la web	INFORME.pdf	Google Chrome (chrome.exe)	22/3/2024 21:06	Ruta local	Sí	wetransfer.com	Compartir archivos	1306522	Registros DLP
Roci@DESKTOP-H9E6EL5	Registro	Subir a la web	[INFECU]Actualización_de_consola_ESET_Nucleo de Solca Machala.docx	Google Chrome (chrome.exe)	22/3/2024 21:07	Ruta local	No	outlook.live.com/mail/0/	Correo web	971663	Registros DLP
Roci@DESKTOP-H9E6EL5	Registro	Subir a la web	ORGANIGRAMA.xls	Google Chrome (chrome.exe)	22/3/2024 21:07	Ruta local	No	outlook.live.com/mail/0/	Correo web	84992	Registros DLP
Roci@DESKTOP-H9E6EL5	Registro	Subir a la web	Informe Técnico Sophos Email COAC CHONE LTDA - signed.pdf	Google Chrome (chrome.exe)	22/3/2024 21:07	Ruta local	No	outlook.live.com/mail/0/	Correo web	668996	Registros DLP
Roci@DESKTOP-H9E6EL5	Registro	Subir a la web	ORGANIGAMA INFORC.pdf	Google Chrome (chrome.exe)	22/3/2024 21:07	Ruta local	No	outlook.live.com/mail/0/	Correo web	228053	Registros DLP
Roci@DESKTOP-H9E6EL5	Registro	Subir a la web	INFORME.pdf	Google Chrome (chrome.exe)	22/3/2024 21:07	Ruta local	No	outlook.live.com/mail/0/	Correo web	1306522	Registros DLP
USUARIO@DESKTOP-VS0A1L9	Registro	Copiar	Document (1) (1).docx	Explorador de Windows (explorer.exe)	22/3/2024 21:22	OneDrive Personal	No	C:\Users\USUARIO\OneDrive\Documentos\Document (1) (1).docx	OneDrive Personal	105298	Registros DLP

USUARIO @DESKTOP-VS0A1L9	Registro	Mover	189-Texto del artículo-669-1-10-20230804.pdf	Explorador de Windows (explorer.exe)	22/3/2024 21:24	Ruta local	No	C:\Users\USUARIO\OneDrive\Escritorio\189-Texto del artículo-669-1-10-20230804.pdf	OneDrive Business	655986	Registros DLP
USUARIO @DESKTOP-VS0A1L9	Registro	Mover	GUIA GENERO[4559] (1).docx	Explorador de Windows (explorer.exe)	22/3/2024 21:25	Ruta local	No	C:\Users\USUARIO\OneDrive\Escritorio\GUIA GENERO[4559] (1).docx	OneDrive Business	621241	Registros DLP

CONCLUSIONES

La integración de los fundamentos teóricos de Prevención de Pérdida de Datos (DLP) y seguridad de la información a través de los criterios de diversos autores resulta fundamental para establecer una base sólida en la protección de datos.

La identificación de los activos de la organización que contienen información sensible es fundamental para fortalecer la seguridad y optimizar la protección. Al priorizar los recursos de seguridad en estos activos críticos, se reduce el riesgo de que la información confidencial sea comprometida, se asegura un uso eficiente de los recursos y se fortalece la postura de seguridad general de la organización.

La prevención de pérdida de datos ofrece un marco estructurado y específico para la protección de la información, se adapta a las necesidades de la organización, aborda los desafíos identificados y establece medidas preventivas adecuadas, lo que resulta en una mayor seguridad de la información y una gestión eficiente de la seguridad.

La validación de la propuesta del plan estratégico de prevención de pérdida de datos garantiza su viabilidad y efectividad, al someterlo a evaluación y ajustes necesarios antes de su implementación completa.

RECOMENDACIONES

Priorizar la capacitación y actualización del personal en cuanto a las prácticas de seguridad de la información y Prevención de Pérdida de Datos (DLP), con el fin de garantizar la comprensión y adopción adecuadas de las políticas y procedimientos establecidos.

Implementar un proceso continuo de monitoreo y evaluación de los activos de información crítica de la organización, utilizando herramientas similares a Safetica o incluso mejores y más actuales, para detectar y mitigar posibles vulnerabilidades y amenazas de manera proactiva.

Establecer políticas claras y procedimientos robustos para gestionar los riesgos relacionados con la confidencialidad de la información, incluyendo medidas de seguridad física y lógica, así como protocolos de respuesta ante incidentes.

Fomentar la colaboración y comunicación entre los diferentes departamentos y niveles jerárquicos de la organización para asegurar una implementación efectiva del plan estratégico de prevención de pérdida de datos.

Realizar revisiones periódicas y auditorías de seguridad para validar la efectividad de las medidas implementadas, identificar áreas de mejora y adaptarse a los cambios en el entorno de amenazas y tecnológico.

BIBLIOGRAFÍA

Acosta Robles, X. R. (2015). *Repositorio Digital Universidad De Las Américas.* Retrieved 06 de 02 de 2024, from https://dspace.udla.edu.ec/bitstream/33000/4476/1/UDLA-EC-TIERI-2015-02.pdf

Arellano, A. L., & Lagua, A. S. (2021). *Repositorio Pontificia Universidad católica del Ecuador.* Retrieved 06 de 02 de 2024, from https://repositorio.pucesa.edu.ec/bitstream/123456789/3121/1/77287.pdf

Arrellano, c. (01 de 2023). https://repositorio.pucesa.edu.ec/bitstream/123456789/4033/1/79184.pdf

Calidad, A. E. (2019). *Asociación Española para la Calidad*. Retrieved 08 de 02 de 2024, from https://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

Castillo et. al. (2021). *Revista Ibérica de Sistemas e Tecnologias de Informação.* Retrieved 06 de 02 de 2024, from https://www.proquest.com/openview/4fc3316c510c3b225e5378667120e7e6/1?pq-origsite=gscholar&cbl=1006393

Fenoy Illacer, D. R. (2023). *Universitat Oberta de Catalunya (UOC).* Retrieved 06 de 02 de 2024, from https://openaccess.uoc.edu/bitstream/10609/147303/4/dillacerTFM0123memoria.pdf

Gantiva, C. (2021). *Repositorio Universidad Abierta y a Distancia UNAD.* Retrieved 06 de 02 de 2024, from https://repository.unad.edu.co/handle/10596/39404

Guevara G; Verdesoto E; & Castro N. (01 de Julio de 2020). *REVISTA CIENTÍFICA MUNDO DE LA INVESTIGACIÓN Y EL CONOCIMIENTO*. http://recimundo.com/index.php/es/article/view/860

Guilcapi, J. (2023). *Repositorio de la Universidad Israel.* Retrieved 18 de 02 de 2024, from https://repositorio.uisrael.edu.ec/bitstream/47000/3953/1/UISRAEL-EC-MASTER-SEG-INF%20-378.242-2023-019.pdf

Hernández et. al. (01 de 12 de 2023). *Revista Dilemas Contemporáneos Educación Política y Valores.* https://doi.org/https://doi.org/10.46377/dilemas.v11iEspecial.3988

Incibe. (15 de 01 de 2019). *Instituto Nacional de Siberseguridad*. Instituto Nacional de Siberseguridad: https://www.incibe.es/empresas/blog/dlp-protege-tus-datos-fugas-informacion

Kickidler. (9 de Marzo de 2022). *https://www.kickidler.com/es/info/top-mejor-dlp-software.html*. https://www.kickidler.com/es/info/top-mejor-dlp-software.html.

Martínez et. al. (29 de 05 de 2023). *Estudios Del Desarrollo Social: Cuba Y América Latina.* Retrieved 06 de 02 de 2024, from https://revistas.uh.cu/revflacso/article/view/3594

Microsoft. (2024). *Seguridad de Microsoft*. Retrieved 08 de 02 de 2024, from https://www.microsoft.com/es-es/security/business/security-101/what-is-data-loss-prevention-dlp#:~:text=La%20prevenci%C3%B3n%20de%20p%C3%A9rdida%20de%20datos%20es%20una%20combinaci%C3%B3n%20de,la%20filtraci%C3%B3n%20de%20datos%20confidenciales.

Moya Gavilanes, C. A. (2023). *Propuesta de un plan de seguridad informático para la empresa.* Pontificia Universidad Cat{olica del Ecuador. https://repositorio.pucesa.edu.ec/bitstream/123456789/4088/1/79247.pdf

Ocampo. (3 de Diciembre de 2019). *INVESTIGALIA*. https://investigaliacr.com/investigacion/investigacion-bibliografica/

Safetica. (2017). *Data Leak Prevention.* Retrieved 12 de diciembre de 2023, from Eset Tegnology alliance: https://www.eset.com/fileadmin/ESET/LATAM/Overviews/Empresas/Safetica-Product-Overview.pdf

Safetica. (2020). *Safetica*. Retrieved 08 de 02 de 2024, from https://www.nsit.com.co/safetica/

Safetica. (08 de Marzo de 2023). *DLP dedicado VS DLP integrado*. https://www.safetica.com/es/blog/dlp-dedicado-vs-dlp-integrado-cual-tiene-mas-sentido-para-su-organizacion

Safetica. (2023). *https://nirien.com/safetica-dlp-1*. https://nirien.com/safetica-dlp-1.

Safetica. (2024). *https://www.safetica.com/es/solucion-dlp*. https://www.safetica.com/es/solucion-dlp.

Vaca, C., & Cueva, J. (09 de 2022). Retrieved 18 de 02 de 2024, from http://repositorio.uisrael.edu.ec/handle/47000/3358

Vaca, C., & Narvaez, A. (2019). Retrieved 18 de 02 de 2024, from https://repositorio.uisrael.edu.ec/handle/47000/2044

Viñas, D. E. (24 de 01 de 2022). *Repositorio de Universidad Militar de Nueva Granada.* Retrieved 08 de 02 de 2024, from http://hdl.handle.net/10654/40524

ANEXOS

Anexo 1: Encuesta

ENCUESTA

1. ¿Considera que la utilización de herramientas tecnológicas resulta beneficiosa para desempeñar su labor?

a. SI b. NO

2. ¿En qué lugar guarda toda la información que genera?

a. PC b. USB C. CLOUD D. OTROS

3. ¿Qué método electrónico emplea para trasladar la información?

a. CORREO b. DISCO EXTERNO C. OTROS

4. Conoce Usted las políticas y normas de seguridad de la información.

a. SI b. NO

5. ¿Recurre al uso de su correo personal para llevar a cabo sus tareas en la institución?

a. SI b. NO

6. ¿Utiliza utiliza con frecuencia el correo institucional?

a. SIEMPRE b. OCASIONAL C. NUNCA

7. ¿Cuáles son los obstáculos que encuentra al utilizar el correo electrónico de la institución?

a. BASTANTE b. POCO C. NINGUNA

8. ¿CUENTA CON UN COMPUTADOR DE LA EMPRESA PARA DESEMPEÑAR SU TRABAJO?

a. SI b. NO

9. ¿Cuál es la longitud de la contraseña que utiliza para acceder a su correo electrónico?

a. MAYOR A 8 CARACTERES b. MENOR A 8 CARACTERES

Anexo 2: Validación de expertos en ciberseguridad

VALADACIÓN EXPERTOS EN CIBERSEGURIDAD

con profesionales especializados en el campo de la seguridad informática,

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **Propuesta de un plan Estratégico de Prevención de Pérdida de Datos mediante Safetica (DLP) para fortalecer la seguridad de la información sensible, en INFORC.**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: ___John Edison Muñoz Arciniegas_____

Título obtenido
Ingeniero en Electrónica y Telecomunicaciones
Cédula de Identidad
0401375233
E- mail
john.munoz@gmsseguridad.com
Institución de Trabajo
GMS Grupo Microsistemas JOVICHSA.
Cargo
Especialista de Seguridades de Tecnologías de la Información
Años de experiencia en el área
9 años

1

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: *Propuesta de un plan Estratégico de Prevención de Pérdida de Datos mediante Safetica (DLP) para fortalecer la seguridad de la información sensible, en INFORC.*

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	X				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*	X				
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*		X			
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*		X			
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	X				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	X				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	X				
Total		25	8			

Observaciones:

Como profesional con varios años de experiencia en la rama de Ciberseguridad y con base en mi en el diseño de la propuesta del Ing. Alfredo Rogel considero que el plan estratégico es de suma importancia para el entorno de la institución.

Actualmente rige en el país la Ley Orgánica de Protección de Datos Personales y una herramienta de prevención de fuga de datos permitirá el cumplimiento de esta normativa para el tratamiento, administración y control de la información interna y externa.

La herramienta escogida para el diseño de esta propuesta (SAFETICA) cuenta con las garantías de funcionamiento y respaldo del fabricante para el cumplimiento de los objetivos de dicha propuesta. Por lo expuesto anteriormente, la propuesta del Plan estratégico es aplicable, necesario y viable.

2

Recomendaciones

Mi recomendación para esta propuesta es, hacer participe a todos los colaboradores de la institución, tanto el personal de experiencia técnica, así el personal de áreas administrativas para socializar la importancia de esta propuesta y la herramienta DLP para contribuir en la mejora de la seguridad de la información y protección de los datos personales.

Lugar, fecha de validación:___Quito 08 de marzo del 2024_____

Firma del especialista

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: *Propuesta de un plan Estratégico de Prevención de Pérdida de Datos mediante Safetica (DLP) para fortalecer la seguridad de la información sensible, en Inforc.*

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: MSc. Francisco Changotasi.

Título obtenido
Ingeniero en Electrónica y Telecomunicaciones - Máster en Telecomunicaciones con mención en Gestión de las Telecomunicaciones
Cédula de Identidad
0401802384
E- mail
fjchangotasi@gmail.com
Institución de Trabajo
INFORC Ecuador
Cargo
Especialista de Seguridad de Redes
Años de experiencia en el área
3

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Propuesta de un plan Estratégico de Prevención de Pérdida de Datos mediante Safetica (DLP) para fortalecer la seguridad de la información sensible, en Inforc.

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*		X			
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*	X				
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	X				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	X				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	X				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*		X			
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	X				
Total						

Observaciones:
La implementación de Safetica en INFORC Ecuador constituye una excelente solución integral para mitigar el riesgo de fuga de datos. Su integración con sistemas de gestión de identidad y acceso, así como su capacidad para adaptarse a entornos heterogéneos, lo convierten en una opción sólida para la empresa ya que protegerá los activos digitales de manera efectiva y eficiente.

Recomendaciones:
Como bien se menciona en el trabajo, uno de los eslabones más frágiles en la protección de información es el factor humano sería importante promover campañas de concientización sobre la fuga de información y proporcionar capacitaciones adecuada a los empleados sobre las políticas y procedimientos de seguridad de datos implementados en la empresa. Finalmente se podría considerar realiza evaluaciones periódicas de riesgos para identificar nuevas áreas de vulnerabilidad y ajustar las políticas de seguridad en consecuencia. Esto ayudará a mantener una postura de seguridad proactiva y adaptativa.

Lugar, fecha de validación: Quito, 8 de marzo de 2024.

Firmado digitalmente por FRANCISCO JOSSUE CHANGOTASI PUGA
DN: cn=FRANCISCO JOSSUE CHANGOTASI PUGA, o=SECURITY DATA S.A. 2, ou=ENTIDAD DE CERTIFICACION DE INFORMACION
Fecha: 2024-03-08 23:06:09:00

Firma del especialista
2

Anexo 3: Plan estratégico en prevención de pérdida de datos

Plan estratégico en prevención de pérdida de datos Infoc Ecuador

Introducción:

La seguridad de TI ya no se trata solo de prevenir ataques ni de bloquear totalmente la aparición de amenazas. La mejor manera de describir la mentalidad de los CISO hoy en día es la aceptación de riesgos.

Después de todo, con las tendencias cambiantes en el robo cibernético, evitar las infracciones es prácticamente imposible. Una vez que las empresas aceptan que ya están bajo ataque o que podrían ser atacadas por ciberdelincuentes en cualquier momento, pueden centrarse en lo que se debe hacer a continuación para salvaguardar sus datos críticos. Al anticipar un ataque en cada esquina y prepararse para diferentes tipos de escenarios, las empresas no quedarán desprevenidas cuando un ataque atraviese sus defensas. En cambio, estarán preparados para enfrentar y mitigar el daño que una violación puede causar a sus almacenes de datos.

Objetivo:

Proporcionar un plan estratégico para la prevención de perdida de datos en la empresa INFOC ECUADOR.

Desarrollo:

Una solución DLP integral puede:

- Descubrir datos personales confidenciales, como información de identificación personal e información de salud protegida electrónicamente almacenada en repositorios de almacenamiento empresariales.
- Evaluar los riesgos asociados con los datos analizando los permisos, la ubicación de almacenamiento, el tipo de datos y más.
- Clasificar y catalogar archivos que contengan datos personales para permitir a los administradores controlar el movimiento de datos entre servidores de archivos y puntos finales.
- Supervisar la actividad de los usuarios en archivos que contienen información confidencial y clasificada, y alerte a los administradores sobre actividades sospechosas.
- Detectar el movimiento de archivos restringidos a dispositivos de almacenamiento externos y aplicaciones web.
- Prevenir fugas de datos mediante el uso de políticas DLP personalizadas para detectar y

bloquear intentos de transferencia de archivos dañinos.

Datos que necesitan mayor protección

Comprender el tipo, contenido y contexto de los datos almacenados y obtener información sobre el nivel de protección requerido es el primer paso de la evaluación. Para proteger los datos críticos, los responsables de seguridad deben localizarlos, monitorear quién accede a ellos y controlar cómo y dónde se utilizan.

Con una solución DLP integral, pueden descubrir y clasificar automáticamente datos confidenciales en todo el almacenamiento empresarial. También puede proporcionar una visibilidad profunda del uso y movimiento de datos, con información sobre las tendencias de acceso de los empleados. A su vez, esto ayudará a comprender mejor el nivel de protección necesario, dónde se deben aplicar salvaguardas, así como a identificar cualquier deficiencia en los procesos de seguridad de datos existentes. De la investigación realizada se encontró que los datos que necesitan ser protegidos se encuentran en los activos considerados como importantes para la organización que se presentan en la tabla 1.

Tabla 1

Matriz de valoración de activos

VALORACIÓN DE ACTIVOS					
Identificador	**Nombre**	**Disponibilidad**	**Integridad**	**Confidencialidad**	**Criticidad**
GERENCIAL					
ID_0001	Portátil 01 (Gerencia)	4	4	4	4
ID_0002	Portátil 02 (Presidente)	4	4	4	4
CONTABILIDAD					
ID_0003	Computador 03 (Contabilidad)	4	4	4	4
SERVIDORES RACK					
ID_0017	Servidor Seagate 17 (Backup)	4	4	4	4
ID_0019	Servidor GPO 150 19(Firewall)	4	4	4	4
EQUIPOS ESCRITORIO					
ID_0022	Servidor Synology 22 (Demos)	4	4	4	4

Además, se encontró que estos activos tienen amenazas relacionadas con: Daño físico, Eventos naturales, Compromiso de la información, Fallas técnicas, Nivel de datos y redes, Acciones no autorizadas, Compromiso de las funciones, Factor humano. Y al realizar la valoración de riesgos se encontró que las amenazas relacionadas con Compromiso de la información, nivel de datos y redes, acciones no autorizadas y factor humano presentan mayor riesgo de ocurrencia. Como se muestra en la tabla 2.

Tabla 1

Valoración de riesgos

Nombre	DF	EN	CI	FT	NDR	ANA	CF	FH
Portátil 01 (Gerencia)	3	3	6	4	6	7	2	7
Portátil 02 (Presidente)	3	3	6	4	7	7	2	8
Computador 03 (Contabilidad)	3	3	5	5	7	8	6	7
Servidor Seagate 17 (Backup)	4	3	8	5	8	8	7	8
Servidor GPO 150 19(Firewall)	5	3	8	6	8	7	8	8
Servidor Synology 22 (Demos)	5	3	8	6	8	7	8	8
Promedio	**3.83**	**3.00**	**6.83**	**5.00**	**7.33**	**7.33**	**5.50**	**7.66**

Una vez realizado el análisis se contrarresta con las vulnerabilidades y procede a elaborar la matriz de riesgos mostrada en la tabla 3:

Finalmente se procede a implementar medidas para prevenir las vulnerabilidades y riesgos identificados mediante un plan estratégico en prevención de perdida de datos Infoc Ecuador con la herramienta Safetica DLP Analizando el flujo de trabajo tal como se muestra en la tabla 4:

Tabla 3

Matriz de riesgos

	INFOC ECUADOR				
		Fecha de actualización:		Versión:	
		23/03/2024		1	
		ANÁLISIS		EVALUACIÓN	TRATAMIENTO
	Riesgo	Frecuencia de ocurrencia	Severidad del daño	Jerarquización del impacto	Solución
1	Entrega a destiempo de acervo	Media	Moderado	Medio	Vuelva a configurar la aplicación afectada si es posible para evitar el uso de cifrado de intensidad media.
2	No se puede confiar en el certificado X.509 del servidor. Esta situación puede darse de tres formas diferentes, en las que se puede romper la cadena de confianza, como se indica a continuación: - En primer lugar, es posible que la parte superior de la cadena de certificados enviada por el servidor no descienda de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido o cuando faltan certificados intermedios que conectarían la parte superior de la cadena de certificados con una autoridad de certificación pública conocida. - En segundo lugar, la cadena de certificados puede contener un certificado que no sea válido en el momento del análisis. Esto puede ocurrir cuando el análisis se realiza antes de una de las fechas 'notBefore' del certificado o después de una de las fechas 'notAfter' del certificado. - En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o no se pudo verificar. Las firmas incorrectas se pueden solucionar haciendo que su emisor vuelva a firmar el certificado con la firma incorrecta. Las firmas que no se pudieron verificar son el resultado de que el emisor del certificado utilizó un algoritmo de firma que Nessus no admite o no reconoce. Si el host remoto es un host público en producción, cualquier interrupción en la cadena dificulta que los usuarios verifiquen la	Media	Moderado	Medio	Vuelva a configurar la aplicación afectada si es posible para evitar el uso de cifrado de intensidad media.

	autenticidad y la identidad del servidor web. Esto podría facilitar la realización de ataques de intermediario contra el host remoto.				
3	El host remoto admite el uso de RC4 en uno o más conjuntos de cifrado. El cifrado RC4 tiene fallas en la generación de un flujo pseudoaleatorio de bytes, de modo que se introduce una amplia variedad de pequeños sesgos en el flujo, lo que disminuye su aleatoriedad. Si el texto sin formato se cifra repetidamente (por ejemplo, cookies HTTP) y un atacante puede obtener muchos (es decir, decenas de millones) de textos cifrados, es posible que el atacante pueda derivar el texto sin formato.	Baja	Moderado	Medio	Vuelva a configurar la aplicación afectada, si es posible, para evitar el uso de cifrados RC4. Considere usar TLS 1.2 con suites AES-GCM sujetas a la compatibilidad del navegador y del servidor web.
4	La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL ya que cualquiera podría establecer un ataque de intermediario contra el host remoto. Tenga en cuenta que este complemento no busca cadenas de certificados que terminen en un certificado que no esté autofirmado, pero que esté firmado por una autoridad certificadora no reconocida.	Baja	Crítico	Medio	Compre o genere un certificado SSL adecuado para este servicio.
5	El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 tiene varios defectos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más nuevas de TLS, como 1.2 y 1.3, están diseñadas contra estos defectos y deben usarse siempre que sea posible. A partir del 31 de marzo de 2020, los puntos finales que no estén habilitados para TLS 1.2 y versiones posteriores ya no funcionarán correctamente con los principales navegadores web ni con los principales proveedores. PCI DSS v3.2 requiere que TLS 1.0 esté completamente deshabilitado antes del 30 de junio de 2018, excepto para los terminales POS POI (y los puntos de terminación SSL/TLS a los que se conectan) que se puede verificar que no son susceptibles a ningún exploit conocido.	Media	Moderado	Medio	Habilite la compatibilidad con TLS 1.2 y 1.3 y deshabilite la compatibilidad con TLS 1.0
6	El servicio remoto acepta conexiones cifradas mediante TLS 1.1. TLS 1.1 carece de soporte para los conjuntos de cifrado actuales y recomendados. Cifrados que admiten cifrado antes del cálculo MAC y autenticados Los modos de cifrado como GCM no se pueden utilizar con TLS 1.1. A partir del 31 de marzo de 2020, los puntos finales que no estén habilitados para TLS 1.2 y versiones posteriores ya no funcionarán	Baja	Moderado	Medio	Habilite la compatibilidad con TLS 1.2 y/o 1.3 y deshabilite la compatibilidad con TLS 1.1.

	correctamente con los principales navegadores web ni con los principales proveedores.				
7	El host remoto admite el uso de cifrados SSL que ofrecen cifrado de intensidad media. Nessus considera de potencia media cualquier cifrado que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice el conjunto de cifrado 3DES. Tenga en cuenta que es considerablemente más fácil eludir el cifrado de intensidad media si el atacante está en la misma red física.	Baja	Moderado	Medio	Vuelva a configurar la aplicación afectada si es posible para evitar el uso de cifrados de potencia media.
8	No se puede confiar en el certificado X.509 del servidor. Esta situación puede darse de tres formas diferentes, en las que la cadena de confianza se puede romper, como se indica a continuación: - En primer lugar, es posible que la parte superior de la cadena de certificados enviada por el servidor no descienda de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido o cuando faltan certificados intermedios que conectarían la parte superior de la cadena de certificados con una autoridad de certificación pública conocida. - En segundo lugar, la cadena de certificados puede contener un certificado que no sea válido en el momento del análisis. Esto puede ocurrir cuando el análisis se realiza antes de una de las fechas 'notBefore' del certificado o después de una de las fechas 'notAfter' del certificado. - En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o no se pudo verificar. Las firmas incorrectas se pueden solucionar haciendo que su emisor vuelva a firmar el certificado con la firma incorrecta. Las firmas que no se pudieron verificar son el resultado de que el emisor del certificado utilizó un algoritmo de firma que Nessus no admite o no reconoce. Si el host remoto es un host público en producción, cualquier interrupción en la cadena dificulta que los usuarios verifiquen la autenticidad y la identidad del servidor web. Esto podría facilitar la realización de ataques de intermediario contra el host remoto.	Media	Moderado	Medio	Compre o genere un certificado SSL adecuado para este servicio.
9	No se puede confiar en el certificado X.509 del servidor. Esta situación puede darse de tres formas diferentes, en las que se puede romper la cadena de confianza, como se indica a continuación: - En primer lugar, es posible que la parte superior de la cadena de certificados enviada por el servidor no descienda de una autoridad de	Media	Menor	Medio	Compre o genere un certificado SSL adecuado para este servicio.

	certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido o cuando faltan certificados intermedios que conectarían la parte superior de la cadena de certificados con una autoridad de certificación pública conocida. - En segundo lugar, la cadena de certificados puede contener un certificado que no sea válido en el momento del análisis. Esto puede ocurrir cuando el análisis se realiza antes de una de las fechas 'notBefore' del certificado o después de una de las fechas 'notAfter' del certificado.				
10	No se puede confiar en el certificado X.509 del servidor. Esta situación puede darse de tres formas diferentes, en las que se puede romper la cadena de confianza, como se indica a continuación: - En primer lugar, es posible que la parte superior de la cadena de certificados enviada por el servidor no descienda de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido o cuando faltan certificados intermedios que conectarían la parte superior de la cadena de certificados con una autoridad de certificación pública conocida. - En segundo lugar, la cadena de certificados puede contener un certificado que no sea válido en el momento del análisis. Esto puede ocurrir cuando el análisis se realiza antes de una de las fechas "no antes" del certificado o después de una de las fechas 'notAfter' del certificado. - En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o no se pudo verificar. Las firmas incorrectas se pueden solucionar haciendo que su emisor vuelva a firmar el certificado con la firma incorrecta. Las firmas que no se pudieron verificar son el resultado de que el emisor del certificado utilizó un algoritmo de firma que Nessus no admite o no reconoce. Si el host remoto es un host público en producción, cualquier interrupción en la cadena dificulta que los usuarios verifiquen la autenticidad y la identidad del servidor web. Esto podría facilitar la realización de ataques de intermediario contra el host remoto.	Media	Moderado	Medio	Compre o genere un certificado SSL adecuado para este servicio.
11	El host remoto admite el uso de RC4 en uno o más conjuntos de cifrado.	Medio	Crítico	Medio	Vuelva a configurar la aplicación afectada, si es posible, para evitar el uso de cifrados RC4. Considere usar

	El cifrado RC4 tiene fallas en la generación de un flujo pseudoaleatorio de bytes, de modo que se introduce una amplia variedad de pequeños sesgos en el flujo, lo que disminuye su aleatoriedad. Si el texto sin formato se cifra repetidamente (por ejemplo, cookies HTTP) y un atacante puede obtener muchos (es decir, decenas de millones) de textos cifrados, es posible que pueda derivar el texto sin formato.				TLS 1.2 con suites AES-GCM sujetas a la compatibilidad del navegador y del servidor web.
12	La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL ya que cualquiera podría establecer un ataque de intermediario contra el host remoto. Tenga en cuenta que este complemento no busca cadenas de certificados que terminen en un certificado que no esté autofirmado, pero que esté firmado por una autoridad certificadora no reconocida.	Media	Moderado	Medio	Compre o genere un certificado SSL adecuado para este servicio
13	El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 tiene varios defectos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más nuevas de TLS, como 1.2 y 1.3, están diseñadas contra estos defectos y deben usarse siempre que sea posible. A partir del 31 de marzo de 2020, los puntos finales que no estén habilitados para TLS 1.2 y versiones posteriores ya no funcionarán correctamente con los principales navegadores web ni con los principales proveedores. PCI DSS v3.2 requiere que TLS 1.0 esté completamente deshabilitado antes del 30 de junio de 2018, excepto para los terminales POS POI (y los puntos de terminación SSL/TLS a los que se conectan) que se puede verificar que no son susceptibles a ningún exploit conocido.	Medio	Menor	Medio	Habilite la compatibilidad con TLS 1.2 y 1.3 y deshabilite la compatibilidad con TLS 1.0.

Tabla 4

Flujo de trabajo

Tiempo	Usuario	Archivo	Tipo de destino	Destino	Información sensible	Fuente	Aplicación	Acción	Riesgo
22.03.2024 21:25:16	USUARIO@DESKTOP-VS0A1L9	GUIA GENERO[4559] (1).docx	Unidad en la nube	C:\Users\USUARIO\OneDrive\Escritorio\GUIA GENERO[4559] (1).docx	No	C:\Users\USUARIO\Downloads\GUIA GENERO[4559] (1).docx	Explorador de Windows (explorer.exe)	Solo registrar	No
22.03.2024 21:24:45	USUARIO@DESKTOP-VS0A1L9	189-Texto del artículo-669-1-10-20230804.pdf	Unidad en la nube	C:\Users\USUARIO\OneDrive\Escritorio\189-Texto del artículo-669-1-10-20230804.pdf	No	C:\Users\USUARIO\Downloads\189-Texto del artículo-669-1-10-20230804.pdf	Explorador de Windows (explorer.exe)	Solo registrar	No
22.03.2024 21:22:46	USUARIO@DESKTOP-VS0A1L9	Document (1) (1).docx	Unidad en la nube	C:\Users\USUARIO\OneDrive\Documentos\Document (1) (1).docx	No	C:\Users\USUARIO\OneDrive\Escritorio\Document (1) (1).docx	Explorador de Windows (explorer.exe)	Solo registrar	No
22.03.2024 21:16:57	Roci@DESKTOP-H9E6EL5	PROYECCION 2024.xls	Ruta local	C:\Users\Roci\Desktop\PROYECCION 2024.xls	No	C:\Users\Roci\Downloads\PROYECCION 2024.xls	Explorador de Windows (explorer.exe)		No
22.03.2024 21:16:25	Roci@DESKTOP-H9E6EL5	PROYECCION 2024.xls	-		No	C:\Users\Roci\Downloads\PROYECCION 2024.xls	Microsoft Excel (EXCEL.EXE)		No
22.03.2024 21:16:15	Roci@DESKTOP-H9E6EL5	PROYECCION 2024.xls	-		No	C:\Users\Roci\Downloads\PROYECCION 2024.xls	Microsoft Excel (EXCEL.EXE)		No
22.03.2024 21:14:53	Roci@DESKTOP-H9E6EL5	PROYECCION 2024.xls	Ruta local	C:\Users\Roci\Downloads\PROYECCION 2024.xls	No	web.whatsapp.com	Google Chrome (chrome.exe)		No
22.03.2024 21:07:49	Roci@DESKTOP-H9E6EL5	INFORME.pdf	Webmail	outlook.live.com/mail/0/	No	C:\Users\Roci\Downloads\INFORME.pdf	Google Chrome (chrome.exe)	Solo registrar	No
22.03.2024 21:07:48	Roci@DESKTOP-H9E6EL5	ORGANIGAMA INFORC.pdf	Webmail	outlook.live.com/mail/0/	No	C:\Users\Roci\Downloads\ORGANIGAMA INFORC.pdf	Google Chrome (chrome.exe)	Solo registrar	No

22.03.2024 21:07:46	Roci@DESKTOP-H9E6EL5	ORGANIGRAMA.xls	Webmail	outlook.live.com/mail/0/	No	C:\Users\Roci\Downloads\ORGANIGRAMA.xls	Google Chrome (chrome.exe)	Solo registrar	No
22.03.2024 21:07:46	Roci@DESKTOP-H9E6EL5	Informe Técnico Sophos Email COAC CHONE LTDA - signed.pdf	Webmail	outlook.live.com/mail/0/	No	C:\Users\Roci\Downloads\Informe Técnico Sophos Email COAC CHONE LTDA - signed.pdf	Google Chrome (chrome.exe)	Solo registrar	No
22.03.2024 21:07:40	Roci@DESKTOP-H9E6EL5	[INFECU]Actualización_de_consola_ESET_Nucleo de Solca Machala.docx	Webmail	outlook.live.com/mail/0/	No	C:\Users\Roci\Downloads\[INFECU]Actualización_de_consola_ESET_Nucleo de Solca Machala.docx	Google Chrome (chrome.exe)	Solo registrar	No
22.03.2024 21:07:07	Roci@DESKTOP-H9E6EL5	[INFECU]Actualización_de_consola_ESET_Nucleo de Solca Machala.docx	Ruta local	C:\Users\Roci\Downloads\[INFECU]Actualización_de_consola_ESET_Nucleo de Solca Machala.docx	No	web.whatsapp.com	Google Chrome (chrome.exe)		No
22.03.2024 21:07:00	Roci@DESKTOP-H9E6EL5	ORGANIGRAMA.xls	Ruta local	C:\Users\Roci\Downloads\ORGANIGRAMA.xls	No	web.whatsapp.com	Google Chrome (chrome.exe)		No
22.03.2024 21:06:57	Roci@DESKTOP-H9E6EL5	Informe Técnico Sophos Email COAC CHONE LTDA - signed.pdf	Ruta local	C:\Users\Roci\Downloads\Informe Técnico Sophos Email COAC CHONE LTDA - signed.pdf	No	web.whatsapp.com	Google Chrome (chrome.exe)		No
22.03.2024 21:06:49	Roci@DESKTOP-H9E6EL5	ORGANIGAMA INFORC.pdf	Ruta local	C:\Users\Roci\Downloads\ORGANIGAMA INFORC.pdf	No	web.whatsapp.com	Google Chrome (chrome.exe)		No
22.03.2024 21:06:15	Roci@DESKTOP-H9E6EL5	CarteraPorCobrar (2).xls	-		No	C:\Users\Roci\Downloads\CarteraPorCobrar (2).xls	Google Chrome (chrome.exe)	Solo registrar	No

22.03.2024 21:06:14	Roci@DESKTOP-H9E6EL5	CarteraPorCobrar (2).xls	Compartir archivos	wetransfer.com	No	C:\Users\Roci\Downloads\CarteraPorCobrar (2).xls	Google Chrome (chrome.exe)	Solo registrar	Sí
22.03.2024 21:06:14	Roci@DESKTOP-H9E6EL5	INFORME.pdf	Compartir archivos	wetransfer.com	No	C:\Users\Roci\Downloads\INFORME.pdf	Google Chrome (chrome.exe)	Solo registrar	Sí
22.03.2024 21:05:11	Roci@DESKTOP-H9E6EL5	INFORME.pdf	Ruta local	C:\Users\Roci\Downloads\INFORME.pdf	No	google.com/search%3Fq%3Dwetra%26oq%3Dwetra%26gs_lcrp%3DEgZjaHJvbWUyCQgAEEUYORiABDITCAEQLhiDARjHARixAxjRAxiABDIHCAIQABiABDINCAMQABiDARixAxiABDIHCAQQABiABDINCAUQABiDARixAxiABDIHCAYQABiABDIGCAcQBRhA0gEIMjkxNWowajeoAgiwAgE%26sourceid%3Dchrome%26ie%3DUTF-8	Google Chrome (chrome.exe)		No
22.03.2024 20:55:19	arogel	[INFECU]Actualización_de_consola_ESET_Nucleo de Solca Machala.docx	Mensajería instantánea	WhatsApp.exe	No	C:\Users\arogel\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalState\tmp\media.tmp\6fa35fe6e01e2439068c0fbf8e908822264d08c8\[INFECU]Actualización_de_consola_ESET_Nucleo de Solca Machala.docx	WhatsApp.exe	Solo registrar	No
22.03.2024 20:55:17	arogel	[INFECU]Ampliación_Licenciamiento_de_consola_ESET_GAD PROVINCIAL	Mensajería instantánea	WhatsApp.exe	No	C:\Users\arogel\OneDrive - INFORC ECUADOR\Respaldo Alfredo\Respados Esc_actusl\[INFECU]Ampliación_Licenciamiento_de_consola_ESET_GAD	WhatsApp.exe	Solo registrar	No

		DE NAPO.docx				PROVINCIAL DE NAPO.docx			
22.03.2024 20:55:17	arogel	[INFECU]Ampliación_Licenciamiento_de_consola_ESET_GAD PROVINCIAL DE NAPO.pdf	Mensajería instantánea	WhatsApp.exe	No	C:\Users\arogel\OneDrive - INFORC ECUADOR\Respaldo Alfredo\Respados Esc_actusl\[INFECU]Ampliación_Licenciamiento_de_consola_ESET_GAD PROVINCIAL DE NAPO.pdf	WhatsApp.exe	Solo registrar	No
22.03.2024 20:55:17	arogel	[INFECU]Actualización_de_consola_ESET_Banco Ecuatoriano de la Vivienda.docx	Mensajería instantánea	WhatsApp.exe	No	C:\Users\arogel\OneDrive - INFORC ECUADOR\Respaldo Alfredo\Respados Esc_actusl\[INFECU]Actualización_de_consola_ESET_Banco Ecuatoriano de la Vivienda.docx	WhatsApp.exe	Solo registrar	No
22.03.2024 20:51:13	arogel	Registros DLP_2024_3_22.xls	-		No	D:\Informacion conf\Registros DLP_2024_3_22.xls	Microsoft Excel (EXCEL.EXE)		No
22.03.2024 20:51:09	arogel	Registros DLP_2024_3_22.xls	USB	D:\Informacion conf\Registros DLP_2024_3_22.xls	No	\\DESKTOP-4AUCK06\Users\safetica\Desktop\test\Registros DLP_2024_3_22.xls	Explorador de Windows (explorer.exe)	Solo registrar	Sí
22.03.2024 20:51:09	arogel	Registros DLP_2024_3_22.pdf	USB	D:\Informacion conf\Registros DLP_2024_3_22.pdf	No	\\DESKTOP-4AUCK06\Users\safetica\Desktop\test\Registros DLP_2024_3_22.pdf	Explorador de Windows (explorer.exe)	Solo registrar	Sí
22.03.2024 20:47:39	arogel	ORGANIGAMA INFORC.pdf	-		No	C:\Users\arogel\Downloads\ORGANIGAMA INFORC.pdf	Google Chrome (chrome.exe)	Solo registrar	No
22.03.2024 20:47:39	arogel	comprobante (3).pdf	-		No	C:\Users\arogel\Downloads\comprobante (3).pdf	Google Chrome (chrome.exe)	Solo registrar	No
22.03.2024 20:47:39	arogel	Gastos Viaje.xlsx	-		No	C:\Users\arogel\Downloads\Gastos Viaje.xlsx	Google Chrome (chrome.exe)	Solo registrar	No

22.03.2024 20:47:37	arogel	LEY DE PROTECCIÓN DE DATOS ECUADOR V2.pptx	Compartir archivos	wetransfer.com	No	C:\Users\arogel\Downloads\LEY DE PROTECCIÓN DE DATOS ECUADOR V2.pptx	Google Chrome (chrome.exe)	Solo registrar	Sí
22.03.2024 20:47:37	arogel	ORGANIGAMA INFORC.pdf	Compartir archivos	wetransfer.com	No	C:\Users\arogel\Downloads\ORGANIGAMA INFORC.pdf	Google Chrome (chrome.exe)	Solo registrar	Sí
22.03.2024 20:47:37	arogel	Informe Técnico Sophos Email COAC CHONE LTDA - signed.pdf	Compartir archivos	wetransfer.com	No	C:\Users\arogel\Downloads\Informe Técnico Sophos Email COAC CHONE LTDA - signed.pdf	Google Chrome (chrome.exe)	Solo registrar	Sí
22.03.2024 20:47:37	arogel	Informe Técnico Sophos Email COAC CHONE LTDA - signed.pdf	-		No	C:\Users\arogel\Downloads\Informe Técnico Sophos Email COAC CHONE LTDA - signed.pdf	Google Chrome (chrome.exe)	Solo registrar	No
22.03.2024 20:47:37	arogel	LEY DE PROTECCIÓN DE DATOS ECUADOR V2.pptx	-		No	C:\Users\arogel\Downloads\LEY DE PROTECCIÓN DE DATOS ECUADOR V2.pptx	Google Chrome (chrome.exe)	Solo registrar	No
22.03.2024 20:47:37	arogel	comprobante (3).pdf	Compartir archivos	wetransfer.com	No	C:\Users\arogel\Downloads\comprobante (3).pdf	Google Chrome (chrome.exe)	Solo registrar	Sí
22.03.2024 20:47:37	arogel	Gastos Viaje.xlsx	Compartir archivos	wetransfer.com	No	C:\Users\arogel\Downloads\Gastos Viaje.xlsx	Google Chrome (chrome.exe)	Solo registrar	Sí
22.03.2024 20:46:30	arogel	Informe Técnico Sophos Email COAC CHONE LTDA - signed.pdf	Mensajería instantánea	WhatsApp.exe	No	C:\Users\arogel\Downloads\Informe Técnico Sophos Email COAC CHONE LTDA - signed.pdf	WhatsApp.exe	Solo registrar	Sí

22.03.2024 20:46:30	arogel	ORGANIGAMA INFORC.pdf	Mensajería instantánea	WhatsApp.exe	No	C:\Users\arogel\Downloads\ORGANIGAMA INFORC.pdf	WhatsApp.exe	Solo registrar	Sí
22.03.2024 20:46:30	arogel	ORGANIGRAMA.xls	Mensajería instantánea	WhatsApp.exe	No	C:\Users\arogel\Downloads\ORGANIGRAMA.xls	WhatsApp.exe	Solo registrar	Sí
22.03.2024 20:45:42	arogel	ORGANIGRAMA.xls	USB	D:\Informacion conf\ORGANIGRAMA.xls	No	C:\Users\arogel\Downloads\ORGANIGRAMA.xls	Explorador de Windows (explorer.exe)	Solo registrar	Sí
22.03.2024 20:45:42	arogel	plan_de_seguridad__inventario_activos.xlsx	USB	D:\Informacion conf\plan_de_seguridad__inventario_activos.xlsx	No	C:\Users\arogel\Downloads\plan_de_seguridad__inventario_activos.xlsx	Explorador de Windows (explorer.exe)	Solo registrar	Sí
22.03.2024 20:45:42	arogel	CONVOCATORIA SEGURIDAD INFORMATICA.xlsx	USB	D:\Informacion conf\CONVOCATORIA SEGURIDAD INFORMATICA.xlsx	No	C:\Users\arogel\Downloads\CONVOCATORIA SEGURIDAD INFORMATICA.xlsx	Explorador de Windows (explorer.exe)	Solo registrar	Sí
22.03.2024 20:45:41	arogel	comprobante (3).pdf	USB	D:\Informacion conf\comprobante (3).pdf	No	C:\Users\arogel\Downloads\comprobante (3).pdf	Explorador de Windows (explorer.exe)	Solo registrar	Sí
22.03.2024 20:45:41	arogel	ORGANIGAMA INFORC.pdf	USB	D:\Informacion conf\ORGANIGAMA INFORC.pdf	No	C:\Users\arogel\Downloads\ORGANIGAMA INFORC.pdf	Explorador de Windows (explorer.exe)	Solo registrar	Sí
22.03.2024 20:45:40	arogel	LEY DE PROTECCIÓN DE DATOS ECUADOR V2.pptx	USB	D:\Informacion conf\LEY DE PROTECCIÓN DE DATOS ECUADOR V2.pptx	No	C:\Users\arogel\Downloads\LEY DE PROTECCIÓN DE DATOS ECUADOR V2.pptx	Explorador de Windows (explorer.exe)	Solo registrar	Sí
22.03.2024 20:39:21	arogel	security_installer.msi	USB	D:\security_installer.msi	No	C:\Proyectou\security_installer.msi	Explorador de Windows (explorer.exe)	Solo registrar	Sí
22.03.2024 20:37:34	arogel	ORGANIGAMA INFORC.pdf	Webmail	mail.google.com/mail/u/0/%23inbox%3Fcompose%3DGTvVlcSKh	No	C:\Users\arogel\Downloads\ORGANIGAMA INFORC.pdf	Google Chrome (chrome.exe)	Solo registrar	No

				phdPBhlfZBwnqwvffDCQzgZJWkLsHhpmScJjQdBwsXpwbdBghpcVzHCjDRQVFqDNhJNv					
22.03.2024 20:37:26	arogel	comprobante (3).pdf	Webmail	mail.google.com/mail/u/0/%23inbox%3Fcompose%3DGTvVlcSKhphdPBhlfZBwnqwvffDCQzgZJWkLsHhpmScJjQdBwsXpwbdBghpcVzHCjDRQVFqDNhJNv	No	C:\Users\arogel\Downloads\comprobante (3).pdf	Google Chrome (chrome.exe)	Solo registrar	No
22.03.2024 20:36:49	arogel	ORGANIGAMA INFORC.pdf	Mensajería instantánea	WhatsApp.exe	No	C:\Users\arogel\Downloads\ORGANIGAMA INFORC.pdf	WhatsApp.exe	Solo registrar	Sí

Identificados los riesgos y el flujo de trabajo se procede a hacer una matriz en donde se muestre la persona responsable y la política a implementarse para evitar o mitigar El riesgo encontrado.

Tabla 5

Plan DLP

			INFOC ECUADOR		
			Fecha de actualización:	**Versión:**	
			23/03/2024	**1**	
			ANÁLISIS		**Responsable**
	Riesgo	**Impacto**	**Tratamiento/Política**	**Fecha**	
1	Manejo de información no autorizada	Medio	Establecer políticas para el control de acceso a la información	23/03/2024	Jefe de TI
2	La cadena de certificados puede contener una firma que no coincide con la información del certificado o no se pueda verificar. Las firmas incorrectas se pueden solucionar haciendo que su emisor vuelva a firmar el certificado con la firma incorrecta.	Medio	Mantener actualizado el certificado de X.509 del servidor.	23/03/2024	Jefe de TI
3	Si el texto sin formato se cifra repetidamente (por ejemplo, cookies HTTP) y un atacante puede obtener muchos (es decir, decenas de millones) de textos cifrados, es posible que el atacante pueda derivar el texto sin formato.	Medio	Reconfigurar el host remoto de RC4 para conjunto de cifrados mensualmente.	23/03/2024	Jefe de TI
4	Si el host remoto es un host público en producción, esto anula el uso de SSL ya que cualquiera podría establecer un ataque de intermediario contra el host remoto.	Medio	La cadena de certificados X.509 debe estar firmada por una autoridad de certificación reconocida.	23/03/2024	Jefe de TI
5	El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 tiene varios defectos de diseño criptográfico.	Medio	Mantener instaladas las versiones más actuales de TLS	23/03/2024	Jefe de TI

6	El servicio remoto acepta conexiones cifradas mediante TLS 1.1. TLS 1.1 carece de soporte para los conjuntos de cifrado actuales y recomendados.	Medio	Mantener habilitada la compatibilidad con TLS 1.2 y/o 1.3 y deshabilitada la compatibilidad con TLS 1.1.	23/03/2024	Jefe de TI
7	El host remoto admite el uso de cifrados SSL que ofrecen cifrado de intensidad media.	Medio	Mantener configurado el cifrado SSL y verificarlo semanalmente	23/03/2024	Jefe de TI
8	Si el host remoto es un host público en producción, cualquier interrupción en la cadena dificulta que los usuarios verifiquen la autenticidad y la identidad del servidor web. Esto podría facilitar la realización de ataques de intermediario contra el host remoto.	Medio	Mantener configurado el cifrado SSL y verificarlo semanalmente	23/03/2024	Jefe de TI
9	En primer lugar, es posible que la parte superior de la cadena de certificados enviada por el servidor no descienda de una autoridad de certificación pública conocida. En segundo lugar, la cadena de certificados puede contener un certificado que no sea válido en el momento del análisis.	Medio	Comprar o generar un certificado SSL adecuado para X.509 del servidor	23/03/2024	Jefe de TI
10	El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 tiene varios defectos de diseño criptográfico.	Medio	Usar siempre versiones TLS 1,2 o 1,3 y mantener habilitada su compatibilidad con TLS 1.0	23/03/2024	Jefe de TI

CONCLUSIÓN

Del análisis del flujo de trabajo se concluye que aquellas actividades que poseen algún tipo de riesgo deben de ser controladas mediante la aplicación de políticas o estrategias que hagan que su desarrollo no sea riesgoso para la organización.

Eficacia en la Prevención de Pérdida de Datos/ indicadores:

- **Reducción en el número de incidentes de fuga de datos:**
  - Medición del porcentaje de disminución en la cantidad de casos de pérdida de información confidencial antes y después de la implementación de Safetica.
  - Análisis comparativo de la frecuencia e impacto de las fugas de datos en un período determinado.
- **Detección precisa de fugas de datos:**
  - Evaluación de la capacidad de Safetica para identificar y alertar sobre la pérdida de información sensible en tiempo real.
  - Análisis de la precisión y confiabilidad de las alertas generadas por el sistema.
- **Prevención de fugas intencionales y accidentales:**
  - Verificación de la eficacia de Safetica en la detección y bloqueo de intentos de exfiltración de datos, tanto por parte de usuarios internos como externos.
  - Evaluación de la capacidad del sistema para prevenir la pérdida de datos por errores humanos o negligencia.

Cumplimiento de Regulaciones:

- **Adaptación a las normas locales e internacionales:**
  - Verificación de que las funcionalidades de Safetica se ajustan a las regulaciones ecuatorianas y a los estándares internacionales de protección de datos como GDPR e ISO 27001.
  - Evaluación del cumplimiento de las políticas y procedimientos internos de Inforc con respecto a la seguridad de la información.

Integración con la Infraestructura Tecnológica:

- **Compatibilidad con sistemas existentes:**
  - Verificación de la compatibilidad de Safetica con los sistemas informáticos, hardware y software, utilizados en Inforc.
  - Evaluación de la capacidad del sistema para integrarse a la arquitectura tecnológica actual sin afectar su funcionamiento.

Facilidad de Uso y Administración:

- **Interfaz intuitiva y amigable para los usuarios:**
    - Evaluación de la facilidad de uso y comprensión de la interfaz de Safetica por parte de los empleados con diferentes niveles de experiencia tecnológica.
    - Análisis de la curva de aprendizaje y la necesidad de capacitación para el uso eficiente del sistema.

- **Administración eficiente por parte del equipo de IT:**
    - Verificación de la facilidad de gestión y configuración del sistema por parte del personal de TI de Inforc.
    - Evaluación de la disponibilidad de herramientas y recursos para la administración eficiente de Safetica.

Criterios Empresariales:

Retorno de la Inversión (ROI):

- **Reducción de costos asociados a la pérdida de datos:**
    - Análisis del impacto financiero de la implementación de Safetica en la prevención de fugas de información.
    - Cálculo del ROI a partir de la reducción de costos por multas, daños a la reputación y recuperación de datos.

- **Mejora en la productividad y eficiencia:**
    - Evaluación del impacto de Safetica en la optimización del tiempo y recursos empleados en la gestión de la seguridad de la información.
    - Análisis del aumento de la productividad por la disminución de interrupciones y tiempo de inactividad debido a incidentes de fuga de datos.

Aceptación y satisfacción de los usuarios:

- **Percepción positiva del sistema por parte de los empleados:**
    - Medición del nivel de satisfacción y aceptación de Safetica por parte de los usuarios finales.
    - Evaluación de la utilidad y facilidad de uso del sistema para el desempeño de las tareas cotidianas.

Fortalecimiento de la Cultura de Seguridad Informática:

- **Mayor conciencia sobre la importancia de la protección de datos:**
  - Evaluación del impacto de Safetica en la sensibilización y el compromiso de los empleados con la seguridad de la información.
  - Análisis del cambio en la cultura organizacional hacia una mayor responsabilidad en el manejo de datos sensibles.

Mejora en la Reputación de la Empresa:

- **Mayor confianza por parte de clientes y socios comerciales:**
  - Evaluación del impacto de la implementación de Safetica en la percepción de la empresa como una organización comprometida con la seguridad de la información.
  - Análisis del aumento en la confianza y fidelización de clientes y socios comerciales.

Criterios de Implementación:

Cumplimiento del Plan de Implementación:

- **Ejecución exitosa de las fases de planificación, implementación y monitoreo:**
  - Verificación del cumplimiento del cronograma y presupuesto establecidos para la implementación del proyecto.
  - Evaluación de la eficiencia en la gestión de recursos humanos, técnicos y financieros durante el proceso de implementación.

Capacitación Efectiva de los Usuarios:

- **Adquisición de habilidades y conocimientos para el uso de Safetica:**
  - Evaluación del nivel de conocimiento y comprensión del sistema por parte de los usuarios finales.
  - Análisis de la efectividad del programa de capacitación en la preparación de los empleados para utilizar Safetica de manera eficiente.

Soporte Técnico y Mantenimiento:

- **Disponibilidad de asistencia técnica oportuna y eficaz:**
  - Verificación de la existencia de un plan de soporte técnico para la resolución de problemas e incidentes relacionados con Safetica.
  - Evaluación de la capacidad del equipo de IT para brindar asistencia técnica eficiente a los usuarios.

Monitoreo y Evaluación Continua:

- **Análisis del rendimiento y la eficacia de Safetica:**
  - Implementación de un sistema de monitoreo para evaluar el desempeño del

sistema en la prevención de fugas de datos.

- Realización de evaluaciones periódicas para identificar oportunidades de mejora y optimizar la configuración del sistema.

Adaptación a Cambios y Actualizaciones:

- **Capacidad para ajustarse a nuevas necesidades y amenazas:**
  - Verificación de la flexibilidad del sistema para adaptarse a cambios en el entorno tecnológico y regulatorio.
  - Evaluación de la capacidad del equipo de IT para actualizar e implementar nuevas funcionalidades en Safetica.