REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓNEN SEGURIDAD INFORMÁTICA

Tema:

EVALUACIÓN DE LA VULNERABILIDAD Y RESPUESTA DE HIDROSOFT ANTE ATAQUES DE INGENIERÍA SOCIAL EN LOS DATOS SENSIBLES DE CLIENTES Y EMPLEADOS:
PROPUESTA DE ESTRATEGIAS ÉTICAS PARA FORTALECER LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA HIDROSOFT ANTE ATAQUES DE INGENIERÍA SOCIAL

Trabajo de Titulación previo a la obtención del Título de Magíster en Computación con mención en Seguridad Informática

Autor: Ing. Luis Geovanny Cacuango Quilca

Director: Ing. Henry Patricio Farinango Endara MSc.

IBARRA - ECUADOR

2025

DEDICATORIA

Primeramente, a Dios, por su infinita bondad y por ser la fuente de fortaleza y sabiduría en cada paso de este camino. A Él, que me ha guiado y protegido en los momentos de desafío, le dedico este logro con profunda gratitud y humildad.

A mis padres, por su amor incondicional, su apoyo constante y su ejemplo de esfuerzo y dedicación. Gracias por enseñarme el valor del trabajo duro y la perseverancia. Sin su guía y respaldo, este sueño no habría sido posible.

A mis queridas hermanas, quienes siempre han estado a mi lado brindándome ánimo, alegría y comprensión. Su fe en mí ha sido una inspiración constante y un impulso para seguir adelante.

A mis profesores, quienes con su conocimiento, paciencia y entrega, me han dado herramientas y enseñanzas valiosas para crecer profesional y personalmente. Gracias por cada lección y por ser un ejemplo de compromiso y excelencia.

Para mi amada, quien en tan poco tiempo se ha convertido en el pilar más importante de mi vida. Tu apoyo incondicional y tus palabras de aliento han sido la luz que ilumina mi camino, incluso en los momentos más oscuros. Gracias por motivarme a seguir adelante y por recordarme que juntos podemos superar cualquier adversidad. Eres mi mayor inspiración y mi razón para nunca rendirme.

A todos mis amigos de TikTok por su apoyo incondicional a lo largo de este proceso. Un agradecimiento especial a Lilian Patricia, mi madrina, por su constante respaldo, confianza y cariño. Su apoyo ha sido fundamental para seguir adelante. ¡Gracias de corazón!

Luis Geovanny Cacuango Quilca

AGRADECIMIENTO

A Agradezco primeramente a Dios, quien me ha bendecido con la fortaleza y sabiduría necesarias para alcanzar este objetivo. A Él, por guiarme en este proceso y ser la luz en cada paso, le doy mi más profundo agradecimiento.

A la Universidad Técnica del Norte, mi alma máter, por brindarme un espacio de aprendizaje, crecimiento y desarrollo. Agradezco profundamente la oportunidad de haber formado parte de esta institución, que me ha permitido avanzar en mi formación profesional.

A mi tutor, por su guía constante, su paciencia y su compromiso. Su dedicación y conocimientos fueron fundamentales para superar los retos de esta etapa y alcanzar el éxito en mi trabajo de grado.

A mi director de carrera y de trabajo de grado, por su orientación y apoyo incondicional. Su visión y liderazgo han sido pilares para el logro de mis objetivos académicos y profesionales.

A mis docentes, quienes con su esfuerzo, experiencia y entrega, han dejado en mí lecciones que trascienden el aula. Su compromiso con mi formación ha sido clave en este proceso, y a cada uno de ustedes les agradezco profundamente por haber sido parte de mi desarrollo.

Gracias a todos por acompañarme en esta etapa y contribuir a hacer realidad este sueño.

Luis Geovanny Cacuango Quilca

UNIVERSIDAD TÉCNICA DEL NORTE
DIRECCIÓN DE BIBLIOTECA

1. IDENTIFICACIÓN DE LA OBRA

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

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1002845913		
APELLIDOS Y NOMBRES:	LUIS GEOVANNY CACUANGO QUILCA		
DIRECCIÓN:	Bolívar SN y Santa Bertha (Atuntaqui - Ecuador)		
EMAIL:	lgcacuangoq@utn.edu.ec		
TELÉFONO FIJO:	0990883705	**TELÉFONO MÓVIL:**	0990883705

DATOS DE LA OBRA	
TÍTULO:	EVALUACIÓN DE LA VULNERABILIDAD Y RESPUESTA DE HIDROSOFT ANTE ATAQUES DE INGENIERÍA SOCIAL EN LOS DATOS SENSIBLES DE CLIENTES Y EMPLEADOS: PROPUESTA DE ESTRATEGIAS ÉTICAS PARA FORTALECER LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA HIDROSOFT ANTE ATAQUES DE INGENIERÍA SOCIAL
AUTOR (ES):	LUIS GEOVANNY CACUANGO QUILCA
FECHA: DD/MM/AAAA	05/02/2025
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☐ **GRADO** ■ **POSGRADO**
TITULO POR EL QUE OPTA:	Magister en Computación con mención en Seguridad Informática
ASESOR /DIRECTOR:	Henry Patricio Farinango Endara Fabian Geovanny Cuzme Rodriguez

2. CONSTANCIAS

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

Ibarra, a los 05 días del mes de febrero de 2025
EL AUTOR:

LUIS GEOVANNY CACUANGO QUILCA

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020FACULTAD DE POSGRADO

Ibarra, 18 de Noviembre de 2024

Dra.
Lucia Yépez
DECANA FACULTAD DE POSGRADO

ASUNTO: Conformidad con el documento final Señora

Decana:

Nos permitimos informar a usted que revisado el Trabajo final de Grado: Evaluación de la vulnerabilidad y respuesta de Hidrosoft ante ataques de ingeniería social en los datos sensibles de clientes y empleados:
Propuesta de estrategias éticas para fortalecer la seguridad de la información en la empresa Hidrosoft ante ataques de ingeniería social del maestrante Luis Geovanny Cacuango Quilca, de la Maestría de Computación con mención en Seguridad Informática, certificamos que han sido acogidas y satisfechas todas las observaciones realizadas.

Atentamente,

	Apellidos y Nombres	**Firma**
Director/a	MSc. Henry Farinango Endara	Firmado electrónicamente por: HENRY PATRICIO FARINANGO ENDARA
Asesor/a	MSc. Fabián Geovanny Cuzme Rodríguez	Firmado electrónicamente por: FABIAN GEOVANNY CUZME RODRIGUEZ

Índice de Contenido

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

GLOSARIO

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

ISO: Organización Internacional de Normalización.

GDPR: Reglamento General de Protección de Datos (General Data Protection Regulation).

PII: Información de Identificación Personal (Personally Identifiable Information).

MFA: Autenticación Multifactorial (Multi-Factor Authentication).

IT: Tecnología de la Información (Information Technology).

ICT: Tecnologías de la Información y la Comunicación (Information and Communication Technology).

DoS: Denegación de Servicio (Denial of Service).

FISMA: Ley Federal de Gestión de Seguridad de la Información (Federal Information Security Management Act).

NTE: Norma Técnica Ecuatoriana.

EGSI: Esquema Gubernamental de Seguridad de la Información.

SMB: Server Message Block (protocolo de comunicación de red).

TIC: Tecnologías de la Información y Comunicación.

Wi-Fi: Wireless Fidelity (red de acceso inalámbrico).

VPN: Red Privada Virtual (Virtual Private Network).

SSL: Capa de Conexión Segura (Secure Socket Layer).

TLS: Seguridad en la Capa de Transporte (Transport Layer Security).

RAT: Herramienta de Administración Remota (Remote Access Tool).

IoT: Internet de las Cosas (Internet of Things).

SMB: Protocolo de Bloque de Mensajes del Servidor.

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓNEN SEGURIDAD INFORMÁTICA

EVALUACIÓN DE LA VULNERABILIDAD Y RESPUESTA DE HIDROSOFT ANTE ATAQUES DE INGENIERÍA SOCIAL EN LOS DATOS SENSIBLES DE CLIENTES Y EMPLEADOS: PROPUESTA DE ESTRATEGIAS ÉTICAS PARA FORTALECER LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA HIDROSOFT ANTE ATAQUES DE INGENIERÍA SOCIAL

Autor: Luis Geovanny Cacuango Quilca

Tutor: Henry Patricio Farinango Endara

Año: 2024

RESUMEN

Esta investigación se centra en la evaluación de la vulnerabilidad de la empresa Hidrosoft ante ataques de ingeniería social y la propuesta de estrategias éticas para fortalecer la seguridad de la información, especialmente en los datos sensibles de clientes y empleados. Hidrosoft, dedicada a la gestión de datos hidrográficos, se enfrenta a crecientes amenazas de manipulación psicológica por parte de atacantes, lo que pone en riesgo la integridad de su información y la confianza de sus partes interesadas.

El objetivo general fue analizar el grado de exposición de la empresa a estos ataques, evaluar las tácticas comunes utilizadas por los atacantes, y proponer recomendaciones éticas en ciberseguridad para mejorar la protección de la información. La investigación empleó un enfoque mixto: cuantitativo, para analizar datos de incidentes de seguridad previos y la efectividad de las medidas actuales, y cualitativo, para explorar las percepciones de empleados y clientes mediante entrevistas y encuestas. Se recopiló información bibliográfica y se usaron técnicas como el análisis de contenido y el estudio de casos.

Los resultados revelaron áreas críticas de vulnerabilidad y la necesidad de implementar controles de seguridad más robustos y éticos, basados en normativas y buenas prácticas de ciberseguridad. Se concluyó que Hidrosoft debe mejorar su infraestructura y políticas de seguridad de información mediante un plan de acción que incluya concientización, medidas preventivas y un seguimiento continuo para mitigar los riesgos asociados a la ingeniería social.

Palabras clave: Ingeniería Social, Ciberseguridad, Seguridad de la Información, Evaluación de Vulnerabilidad, Protección de Datos Sensibles, Recomendaciones Éticas, Estrategias de Ciberseguridad, Hidrosoft, Confianza Organizacional, Normativas de Seguridad.

ABSTRACT

This research focuses on assessing the vulnerability of the company Hidrosoft to social engineering attacks and proposing ethical strategies to strengthen information security, particularly regarding sensitive customer and employee data. Hidrosoft, dedicated to hydrographic data management, faces increasing threats of psychological manipulation by attackers, which jeopardizes the integrity of its information and the trust of its stakeholders.

The primary objective was to analyze the company's exposure to these attacks, assess the common tactics used by attackers, and propose ethical recommendations in cybersecurity to enhance information protection. The research employed a mixed-method approach: quantitative, to analyze data on past security incidents and the effectiveness of current measures, and qualitative, to explore employees' and clients' perceptions through interviews and surveys. Bibliographic information was collected, and techniques such as content analysis and case studies were utilized.

The results revealed critical vulnerability areas and the need to implement more robust and ethical security controls based on standards and best practices in cybersecurity. It was concluded that Hidrosoft should improve its infrastructure and information security policies through an action plan that includes awareness-raising, preventive measures, and ongoing monitoring to mitigate the risks associated with social engineering.

Keywords: Social Engineering, Cybersecurity, Information Security, Vulnerability Assessment, Sensitive Data Protection, Ethical Recommendations, Cybersecurity Strategies, Hidrosoft, Organizational Trust, Security Standards

CAPÍTULO I

EL PROBLEMA

1.1. Problema de investigación

- **Contexto Temático**

Este estudio se enmarca en el ámbito de la ciberseguridad y la gestión de datos sensibles en el contexto empresarial, abordando una problemática crucial en la actualidad. Se centra específicamente en el análisis de la empresa Hidrosoft, la cual opera en el campo de la gestión de datos hidrográficos. Hidrosoft se destaca por su colaboración estrecha con diversos clientes y empleados, ya que juega un papel fundamental en el almacenamiento y procesamiento de información crítica para la toma de decisiones en el ámbito de la hidrografía y recursos hídricos. En este contexto, la seguridad de los datos y la protección contra ataques de ingeniería social se convierten en factores críticos para garantizar la integridad de la información y la continuidad de las operaciones, así como para mantener la confianza de los clientes y cumplir con las regulaciones pertinentes en materia de privacidad y seguridad de datos.

- **Problematización**

El problema se centra en la creciente exposición de Hidrosoft a ataques de ingeniería social, una preocupación creciente en un entorno empresarial altamente digitalizado y colaborativo. Estos ataques se basan en la manipulación psicológica para acceder a datos confidenciales, lo que plantea serias amenazas para la empresa. Además de comprometer la integridad de los datos, estos incidentes pueden dar lugar a daños en la reputación de la empresa y desencadenar consecuencias legales. La alta digitalización de las operaciones de Hidrosoft y su colaboración con numerosos actores en el entorno empresarial aumentan significativamente la vulnerabilidad de la organización frente a estos ataques, convirtiéndola en una cuestión crítica que requiere una investigación en profundidad para desarrollar estrategias efectivas de mitigación y prevención.

1.2. Interrogantes de la investigación

- ¿Cuáles son las tácticas más comunes empleadas por los atacantes en los ataques de ingeniería social dirigidos a Hidrosoft?
- ¿En qué medida las medidas de seguridad existentes en Hidrosoft son efectivas para prevenir y mitigar los ataques de ingeniería social?
- ¿Cuáles son las recomendaciones éticas y estrategias de ciberseguridad específicas que pueden implementarse en Hidrosoft para fortalecer la protección de datos sensibles de clientes y empleados?
- ¿Cuál es el potencial impacto de los ataques de ingeniería social en la confianza de los clientes y empleados hacia Hidrosoft?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Evaluar la vulnerabilidad de la empresa Hidrosoft ante ataques de ingeniería social dirigidos a los datos sensibles de clientes y empleados y proponer estrategias éticas para fortalecer la seguridad de la información para preservar la confianza en la organización.

1.3.2 Objetivos específicos

- Analizar la exposición de Hidrosoft a ataques de ingeniería social, identificando las tácticas más comunes utilizadas por los atacantes, evaluando la efectividad de las medidas de seguridad existentes, con el fin de comprender la magnitud de la amenaza y las áreas críticas de vulnerabilidad.,
- Diseñar un conjunto de recomendaciones éticas y estrategias de ciberseguridad específicas para la empresa, con el propósito de fortalecer la protección de los datos sensibles de clientes y empleados.
- Evaluar las recomendaciones éticas y estrategias de ciberseguridad propuestas en procura de garantizar la integridad, confidencialidad y disponibilidad de la información.

1.4. Hipótesis

- **Hipótesis de Trabajo**

Las medidas de ciberseguridad implementadas en Hidrosoft, basadas en principios éticos y en las mejores prácticas internacionales, inciden en la reducción de la vulnerabilidad frente a ataques de ingeniería social y fortalecen la protección de los datos sensibles de clientes y empleados.

Variable independiente: Medidas de ciberseguridad basadas en principios éticos y mejores prácticas internacionales.

Variable dependiente: Reducción de la vulnerabilidad frente a ataques de ingeniería social y fortalecimiento de la protección de datos sensibles.

- **Hipótesis Alternativa**

Las medidas de ciberseguridad implementadas en Hidrosoft, basadas en principios éticos y en las mejores prácticas internacionales, no inciden en la reducción de la vulnerabilidad frente a ataques de ingeniería social ni fortalecen la protección de los datos sensibles de clientes y empleados.

1.5. Justificación

La justificación de esta investigación se basa en la importancia crítica de abordar el problema de la exposición de Hidrosoft a ataques de ingeniería social y en los múltiples beneficios que se derivan de su realización:

Relevancia en Ciberseguridad Empresarial: La ciberseguridad es una preocupación global y, en particular, la ingeniería social es una táctica de ataque en constante evolución. Comprender y abordar esta amenaza es esencial para proteger la integridad de los datos sensibles de clientes y empleados.

Preservación de la Confianza: La confianza es un activo intangible fundamental en cualquier organización. La investigación busca mantener y fortalecer la confianza de clientes y empleados hacia Hidrosoft al proteger sus datos.

Contribución al Conocimiento: La investigación generará conocimientos específicos sobre las tácticas de ingeniería social, evaluación de vulnerabilidades y estrategias éticas de ciberseguridad que pueden aplicarse en entornos empresariales similares.

Desarrollo Regional y Empresarial: Al fortalecer la ciberseguridad de Hidrosoft, se contribuye al desarrollo sostenible de la empresa, lo que a su vez puede generar empleo y promover el crecimiento económico regional.

Ética en la Seguridad de la Información: La investigación promueve el uso ético de estrategias de ciberseguridad, alineando la protección de datos con principios éticos y legales.

Impacto en la Comunidad Empresarial: Los resultados de esta investigación pueden ser de interés y utilidad para otras organizaciones que enfrentan desafíos similares en la gestión de datos sensibles.

CAPITULO II
MARCO REFERENCIAL

2.2. Marco teórico

2.2.1. MAGERIT:

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es un marco desarrollado por el gobierno de España para gestionar los riesgos relacionados con los sistemas de información. Su propósito principal es garantizar la confidencialidad, integridad y disponibilidad de los activos de información, mediante la identificación, evaluación y tratamiento de riesgos (Gobierno de España, 2020). Esta metodología es altamente efectiva para organizaciones como Hidrosoft, dado su enfoque estructurado y adaptable.

MAGERIT identifica vulnerabilidades y amenazas para evaluar riesgos de manera sistemática, un proceso crucial para empresas que manejan datos sensibles. Según el Gobierno de España, esta metodología también se adapta fácilmente a diferentes contextos organizativos y está alineada con normas internacionales como la ISO/IEC 27001, lo que asegura la implementación de controles efectivos (Gobierno de España, 2020). Además, incluye herramientas visuales que ayudan a priorizar riesgos y facilita la toma de decisiones estratégicas, lo que beneficia directamente a empresas como Hidrosoft (Gobierno de España, 2020).

2.2.2. Ingeniería Social

La ingeniería social se define como el conjunto de técnicas utilizadas para manipular la psicología humana con el fin de obtener acceso no autorizado a información confidencial. Se analizan las tácticas comunes empleadas por los atacantes, como el phishing, la pretextación y la suplantación de identidad. Además, se exploran estudios previos que evidencian la creciente amenaza de la ingeniería social en el ámbito empresarial y sus repercusiones.

2.2.3. Evaluación de Vulnerabilidad Empresarial:

Este apartado aborda las metodologías y enfoques utilizados para evaluar la vulnerabilidad de una empresa ante ataques de ingeniería social. Se destacan modelos de evaluación de riesgos, la identificación de activos críticos y la evaluación de amenazas específicas. Además, se explora cómo estas evaluaciones contribuyen a la formulación de estrategias de ciberseguridad efectivas.

2.2.4. Ética en la Ciberseguridad:

La ética en la ciberseguridad aborda la privacidad, la transparencia y la responsabilidad en la gestión de la información, destacando la obligación de las empresas de tratar los datos sensibles de manera responsable (Spiekermann & Cranor, 2009). Este enfoque no solo cumple con requisitos legales, sino que establece un marco de confianza para clientes, empleados y socios estratégicos.

Uno de los pilares de la ciberseguridad ética es la implementación de principios como la privacidad por diseño, que integra la protección de datos en todas las etapas del desarrollo de sistemas y procesos (Cavoukian, 2010). Además, el uso de códigos éticos y buenas prácticas refuerzan una cultura de seguridad alineada con principios morales y legales (IEEE, 2017; ACM, 1992).

Casos de Estudio sobre Ética y Percepción de Seguridad en Empresas

A continuación, se presentan casos de estudio que destacan cómo las estrategias éticas han transformado positivamente la percepción de seguridad en organizaciones de diferentes sectores:

Implementación de la Privacidad por Diseño en Apple Inc.

Apple ha integrado el principio de "privacidad por diseño" en todos sus productos. Este enfoque asegura que la privacidad esté incorporada desde las etapas iniciales de desarrollo, cumpliendo con regulaciones como el Reglamento General de Protección de Datos (GDPR). Este compromiso ha mejorado significativamente la confianza del consumidor.

Impacto: Un informe destacó que Apple es percibida como una de las empresas mejor valoradas en términos de privacidad y seguridad de datos (TrustArc, 2020).

Lección para Hidrosoft: Integrar la privacidad en el diseño de sus políticas y sistemas puede fortalecer la percepción de seguridad y confianza entre sus clientes.

Campañas de Sensibilización Ética en IBM

IBM ha implementado programas internos que incluyen talleres éticos y simulaciones de ciberataques. Estas iniciativas han reducido los incidentes de seguridad relacionados con errores humanos, mejorando la percepción interna de seguridad (IBM Security, 2021).

Impacto: Una mayor conciencia ética y una cultura de seguridad compartida incrementaron la colaboración y el cumplimiento de políticas.

Lección para Hidrosoft: La sensibilización ética a través de capacitaciones periódicas puede reducir errores humanos y reforzar la preparación frente a amenazas.

Transparencia en la Gestión de Brechas de Datos - Equifax

Tras un ciberataque significativo, Equifax adoptó un enfoque ético, comunicando proactivamente las medidas tomadas y estableciendo un comité para supervisar la protección de datos.

Impacto: Aunque inicialmente enfrentaron una crisis reputacional, la transparencia ayudó a recuperar la confianza de clientes y reguladores (Westby, 2017).

Lección para Hidrosoft: La transparencia en la gestión de incidentes puede fortalecer la confianza de los clientes y demostrar un compromiso ético.

Programas de Código Ético en Microsoft

Microsoft desarrolló un código ético global que guía el manejo de datos sensibles y fomenta la transparencia en sus operaciones de ciberseguridad.

Impacto: Los clientes perciben a Microsoft como líder en prácticas éticas, aumentando su confianza en la protección de datos (Microsoft Corporation, 2020).

Lección para Hidrosoft: Un código ético claro puede servir como guía para implementar mejores prácticas en seguridad y fortalecer la percepción de responsabilidad empresarial.

Ingeniería Social

La ingeniería social se refiere a la manipulación psicológica de individuos para obtener información confidencial o acceso a sistemas informáticos. Los atacantes utilizan técnicas de persuasión y engaño para engañar a las personas y lograr sus objetivos maliciosos (Mitnick & Simon, 2002).

Ciberseguridad

La ciberseguridad comprende las prácticas, políticas y tecnologías diseñadas para proteger sistemas informáticos, redes y datos contra amenazas cibernéticas. Incluye la prevención, detección y respuesta a ataques cibernéticos (Dhillon, 2018).

Protección de Datos Sensibles

Los datos sensibles son aquellos que, si se ven comprometidos, pueden causar daño significativo a individuos o empresas. La protección de estos datos implica medidas técnicas y legales para evitar su acceso no autorizado (Solove, 2007).

Estrategias Éticas de Seguridad

Las estrategias éticas de seguridad se basan en principios morales y éticos para guiar la toma de decisiones en ciberseguridad y protección de datos. Estas estrategias buscan no solo cumplir con regulaciones, sino también hacer lo correcto desde una perspectiva ética (Pfleeger & Pfleeger, 2019).

Evaluación de la Vulnerabilidad

La evaluación de la vulnerabilidad implica identificar y medir las debilidades en la seguridad de una organización. Esto se logra a través de pruebas de seguridad, análisis de riesgos y evaluaciones de amenazas (Whitman & Mattord, 2018).

Relación entre Vulnerabilidad y Estrategias Éticas

La relación entre la vulnerabilidad de una organización y sus estrategias éticas de seguridad es crucial. Una mayor vulnerabilidad puede requerir un enfoque ético más sólido en la toma de decisiones de seguridad (Schneier, 2015).

Phishing

El phishing es una técnica de ingeniería social que utiliza correos electrónicos, mensajes de texto o sitios web falsos para engañar a las personas a fin de que compartan información confidencial, como nombres de usuario, contraseñas y detalles bancarios. Esta técnica se basa en la suplantación de identidad, donde el atacante finge ser una entidad confiable, como un banco o una plataforma de redes sociales (Jagatic, Johnson, & Jakobsson, 2007). Según reportes de Mandiant (2020), los ataques de phishing son responsables de un alto porcentaje de brechas de seguridad en empresas globales.

Ransomware

El ransomware es un tipo de malware que cifra los archivos de la víctima y demanda un rescate monetario para desbloquearlos. Esta amenaza ha crecido significativamente, afectando tanto a individuos como a empresas y organismos gubernamentales (Huang, Siegel, & Madnick, 2018). Los ataques de ransomware suelen realizarse mediante phishing y enlaces maliciosos que instalan el software en los sistemas. Su impacto financiero ha llevado a numerosas empresas a mejorar sus políticas de backup y a implementar soluciones de seguridad avanzadas.

Spear Phishing

A diferencia del phishing tradicional, el spear phishing se dirige a individuos o grupos específicos dentro de una organización. Los atacantes personalizan los mensajes para parecer genuinos y auténticos, logrando así engañar a personas con acceso a información crítica (Krebs, 2016). Esta técnica ha demostrado ser particularmente efectiva en empresas que manejan datos financieros o información confidencial, y ha llevado a organizaciones a implementar protocolos de autenticación adicionales y capacitaciones en ciberseguridad para sus empleados.

Malware

El término 'malware' abarca todos los tipos de software malicioso diseñados para dañar o explotar cualquier dispositivo o red. Incluye virus, gusanos, ransomware y troyanos, entre otros (Skoudis & Zeltser, 2003). Los atacantes utilizan malware para robar información, espiar al usuario o interrumpir operaciones. Este tipo de software es especialmente peligroso en entornos empresariales, ya que puede llevar a la pérdida de datos y a daños significativos en la reputación de la organización.

Spyware

El spyware es un tipo de software que recopila datos sobre las actividades de un usuario sin su consentimiento, y envía esta información a un atacante. Es comúnmente utilizado para robar

información financiera o credenciales de acceso (Warkentin & Willison, 2009). En entornos empresariales, el spyware puede comprometer la privacidad de los empleados y la confidencialidad de los datos, y por ello, muchas empresas implementan políticas de seguridad estrictas para detectar y eliminar este tipo de software.

Confidencialidad en Ciberseguridad

La confidencialidad es uno de los principios clave de la seguridad de la información y garantiza que solo las personas autorizadas tengan acceso a los datos (Whitman & Mattord, 2018). Este principio es crucial en el ámbito empresarial, ya que asegura que la información sensible no sea divulgada a personas no autorizadas. La confidencialidad se implementa a través de mecanismos de control de acceso y cifrado de datos.

Integridad de los Datos

La integridad de los datos asegura que la información almacenada sea precisa, completa y esté libre de modificaciones no autorizadas (Pfleeger & Pfleeger, 2019). En una empresa, la integridad es esencial para la toma de decisiones, ya que asegura que los datos no hayan sido alterados. Las organizaciones emplean mecanismos de auditoría y validación de datos para mantener la integridad de la información.

Disponibilidad de la Información

La disponibilidad asegura que los datos y sistemas estén accesibles a los usuarios autorizados cuando lo necesiten, evitando interrupciones en el servicio (Dhillon, 2018). En ciberseguridad, la disponibilidad es crucial para mantener la operatividad continua de una organización. Los planes de recuperación ante desastres y sistemas de respaldo son algunas de las medidas implementadas para garantizar la disponibilidad.

Denegación de Servicio (DoS)

Un ataque de Denegación de Servicio (DoS) se basa en saturar un sistema o red con tráfico excesivo, haciéndolo inaccesible para los usuarios legítimos (Gibson, 2008). Este tipo de ataque puede tener un impacto considerable en la operatividad de una empresa, afectando tanto su productividad como su reputación.

Privacidad de los Datos

La privacidad en ciberseguridad se refiere al derecho de los individuos y empresas a controlar cómo se recopila, almacena y comparte su información personal (Solove, 2007). Las organizaciones implementan políticas de privacidad y regulaciones como el GDPR para proteger los derechos de sus usuarios.

Política de Seguridad

Una política de seguridad es un conjunto de directrices y procedimientos que definen cómo una organización protege sus sistemas y datos de posibles amenazas (Safa, Von Solms, & Furnell, 2016). Estas políticas abarcan desde el uso adecuado de contraseñas hasta la gestión de accesos y las medidas contra el malware.

Educación en Ciberseguridad

La capacitación y educación en ciberseguridad para los empleados es fundamental para reducir riesgos. A través de la educación, los empleados aprenden a reconocer amenazas comunes, como el phishing y el malware, y a responder adecuadamente (Kim, 2016). La falta de formación en ciberseguridad es un factor de riesgo significativo, y muchas empresas han implementado programas de concienciación de seguridad para mitigar este riesgo.

2.3. Marco Legal y Normativo

Las leyes y regulaciones relacionadas con la protección de datos y la ciberseguridad son fundamentales para garantizar la conformidad y la seguridad ética. Estas leyes pueden variar según la ubicación y la industria (Westby, 2017).

En el caso de empresas como Hidrosoft, que manejan datos sensibles relacionados con recursos hídricos, cumplir con estas normativas no solo es una obligación legal sino también una responsabilidad ética. A continuación, se destacan algunas de las principales leyes y consideraciones éticas en ciberseguridad:

Ley Orgánica de Protección de Datos Personales (Ecuador, 2021):

En Ecuador, la Ley Orgánica de Protección de Datos Personales (LOPDP) fue promulgada en 2021, alineándose en parte con el GDPR europeo, pero adaptada al contexto ecuatoriano. Esta ley establece principios y obligaciones que las empresas deben cumplir para garantizar la protección de datos personales. Para Hidrosoft, esta ley implica que deben implementar medidas adecuadas de seguridad para proteger los datos personales de los clientes y empleados, incluyendo medidas tecnológicas y administrativas que prevengan el acceso no autorizado o el uso indebido de dicha información (Asamblea Nacional del Ecuador, 2021). Además, la ley exige la obtención de consentimiento explícito para el tratamiento de datos personales y establece el derecho de los ciudadanos a acceder, rectificar y suprimir sus datos.

Reglamento sobre la Protección de Datos Personales (Ecuador, 2022):

En 2022, Ecuador emitió el reglamento complementario a la LOPDP, que proporciona directrices adicionales sobre la implementación de la ley. Este reglamento detalla las medidas de seguridad necesarias para la protección de datos sensibles, como los datos relacionados con la salud o los datos financieros, que son de particular importancia para empresas como Hidrosoft que manejan información crítica de sus clientes. Hidrosoft deberá asegurarse de que sus procesos de recolección, almacenamiento y tratamiento de datos estén en total conformidad con estas normativas, evitando posibles sanciones por incumplimiento. Además, se exige la creación de políticas internas claras de protección de datos y la capacitación de empleados en estos temas (SENRES, 2022).

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ecuador, 2018):

Esta ley regula el uso de tecnología digital en las transacciones comerciales y establece las condiciones para garantizar la autenticidad, integridad y confidencialidad de la información intercambiada electrónicamente. En el caso de Hidrosoft, que probablemente maneja transacciones electrónicas con clientes y proveedores, esta ley establece la obligación de proteger la información sensible durante la comunicación digital, utilizando mecanismos como el cifrado y la autenticación en línea (Asamblea Nacional del Ecuador, 2018). La ley también enfatiza la responsabilidad de las empresas en proteger las firmas electrónicas y los datos en las plataformas digitales, lo cual es crucial para la seguridad de las transacciones.

Cumplimiento de las Normativas Internacionales:

Aunque Hidrosoft debe cumplir con las leyes nacionales ecuatorianas, la empresa también puede estar sujeta a normativas internacionales si realiza operaciones con clientes o entidades en el extranjero. Por ejemplo, el GDPR de la Unión Europea establece restricciones sobre cómo se deben tratar los datos de los ciudadanos europeos, lo que podría aplicarse si Hidrosoft tiene relaciones comerciales con empresas europeas. El cumplimiento del GDPR y otras leyes internacionales puede ser un factor clave para fortalecer la confianza de los clientes y proteger la reputación de la empresa (European Union, 2016).

Ley de Protección de Datos Personales

En diversas jurisdicciones, como la Unión Europea, la protección de los datos personales está regulada por normativas específicas. El Reglamento General de Protección de Datos (GDPR) es una de las normativas más completas a nivel global, que establece obligaciones estrictas para las empresas en cuanto al tratamiento y protección de los datos personales (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 2016). Entre las disposiciones del GDPR se incluyen el derecho al olvido, la portabilidad de los datos, la notificación de brechas de seguridad y la obligatoriedad de obtener consentimiento explícito para el procesamiento de datos. Estas disposiciones obligan a las empresas a implementar

sistemas de seguridad robustos para evitar accesos no autorizados y vulneraciones de los datos personales.

Ley de Seguridad de la Información

En muchos países, existen leyes nacionales que regulan la seguridad de la información en el sector privado y público. Por ejemplo, en Estados Unidos, la Ley Federal de Gestión de Seguridad de la Información (FISMA) exige a las agencias federales y sus contratistas implementar medidas de seguridad para proteger sus sistemas de información y datos (Office of Management and Budget, 2002). Aunque Hidrosoft no es una agencia federal estadounidense, muchas empresas internacionales se basan en estándares como FISMA para establecer sus propios protocolos de seguridad. Implementar estas prácticas puede proporcionar un marco sólido para gestionar los riesgos de ciberseguridad y garantizar la integridad de los datos hidrográficos.

Obligaciones Éticas en la Ciberseguridad

La ciberseguridad no solo se trata de cumplir con regulaciones, sino también de abordar cuestiones éticas. Las empresas que manejan datos sensibles, como Hidrosoft, tienen la responsabilidad de garantizar que la información se maneje de forma ética y transparente. Según (Spiekermann & Cranor, 2009), las obligaciones éticas en ciberseguridad se centran en la privacidad, la transparencia y la responsabilidad en la gestión de la información. El concepto de “privacidad por diseño” sugiere que la protección de los datos debe estar integrada en el diseño y funcionamiento de todos los sistemas y procesos desde el inicio, minimizando así los riesgos de vulneración (Cavoukian, 2010).

Códigos de Ética y Buenas Prácticas

Organizaciones como el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) y la Asociación de Maquinaria de Computación (ACM) ofrecen códigos de ética que proporcionan directrices para los profesionales de la informática y la ciberseguridad. Estos códigos enfatizan el deber de los profesionales de proteger la información de los usuarios y clientes, evitar daños intencionados y reportar cualquier vulnerabilidad que pueda comprometer la seguridad de los

sistemas (ACM, 1992; IEEE, 2017). Estos principios éticos ayudan a establecer una cultura de responsabilidad y seguridad en las empresas, promoviendo un entorno que valora y protege la privacidad y seguridad de los datos

2.4. Confianza y Reputación Organizacional

La confianza de los clientes es un activo intangible fundamental en cualquier empresa. Los ataques de ingeniería social y las brechas de seguridad pueden tener un impacto devastador en la percepción de seguridad y confianza de los clientes hacia la organización. Estudios indican que una buena gestión de la ciberseguridad contribuye a fortalecer la reputación organizacional (Ferrari, 2019).

CAPITULO III
MARCO METODOLÓGICO

3.1. Descripción del área de estudio / Descripción del grupo de estudio

La investigación se centra en la empresa Hidrosoft, una organización líder en el campo de la gestión de datos hidrográficos. Hidrosoft tiene su sede central en una zona urbana de tamaño medio, lo que la sitúa en un entorno de negocios competitivo y en constante evolución. La empresa opera en un entorno altamente digitalizado y colabora con una amplia gama de clientes, incluyendo agencias gubernamentales, empresas privadas y organizaciones sin fines de lucro.

La investigación se centra en la empresa Hidrosoft, una organización líder en la gestión de datos hidrográficos que desempeña un papel estratégico en sectores como la ingeniería civil y la gestión ambiental. Sus operaciones abarcan la recopilación, almacenamiento y análisis de información crítica, lo que la convierte en un actor clave para clientes del ámbito privado y gubernamental.

3.1.1. Contexto Operativo

Hidrosoft maneja datos sensibles relacionados con recursos hídricos, modelos predictivos y sistemas de información geográfica. Estos datos son esenciales para la toma de decisiones estratégicas en proyectos de infraestructura, manejo ambiental y sostenibilidad.

3.1.2. Desafíos Identificados

La empresa enfrenta desafíos significativos en el ámbito de la seguridad de la información, especialmente por:

Vulnerabilidades frente a ataques de ingeniería social: Como el phishing, pretexting y baiting, los cuales explotan la interacción humana para acceder a información confidencial.

Infraestructura tecnológica y digitalizada: Aunque moderna, esta infraestructura requiere actualizaciones y controles constantes para prevenir accesos no autorizados.

Capacitación insuficiente del personal: Existe una brecha en el conocimiento práctico de los empleados respecto a amenazas cibernéticas y estrategias de mitigación.

3.1.3. Importancia del Caso de Estudio

La selección de Hidrosoft como objeto de estudio se justifica por:

Impacto directo: La seguridad de la información afecta la continuidad operativa y la confianza de sus clientes.

Representatividad: Hidrosoft refleja los desafíos enfrentados por empresas con operaciones altamente digitalizadas.

Relevancia estratégica: La organización es un pilar en la cadena de valor de sectores críticos, donde la pérdida de datos podría tener consecuencias económicas y sociales significativas.

3.1.4. Áreas de Intervención

La investigación se enfoca en:

La identificación y análisis de riesgos asociados a ingeniería social.

La evaluación de medidas actuales de seguridad.

El diseño e implementación de estrategias para fortalecer los riesgos esquema gubernamental de seguridad de la información (EGSI versión 2.0)

3.2. Enfoque y Tipo de Investigación

La presente investigación utiliza un enfoque y tipo de investigación diseñados para abordar las problemáticas específicas de seguridad de la información en Hidrosoft, especialmente en relación con los riesgos asociados a ataques de

ingeniería social. Este enfoque garantiza un análisis exhaustivo que permita implementar soluciones efectivas y sostenibles.

3.2.1. Enfoque

La investigación adopta un enfoque mixto (cualitativo y cuantitativo), que combina el análisis numérico con la interpretación de percepciones y experiencias:

Enfoque Cuantitativo:

Permite medir y analizar la probabilidad, impacto y nivel de riesgo de las amenazas identificadas mediante herramientas como la matriz de riesgos.

Evalúa datos estadísticos obtenidos de encuestas para determinar tendencias y niveles de vulnerabilidad.

Enfoque Cualitativo:

Explora las percepciones, actitudes y experiencias del personal clave mediante entrevistas en profundidad.

Identifica factores organizacionales y humanos que contribuyen a la exposición a riesgos de ingeniería social.

Esta combinación permite una comprensión integral del problema, considerando tanto los aspectos técnicos como los factores humanos que influyen en la seguridad de la información.

3.2.2. Tipo de Investigación

La investigación se clasifica como:

Aplicada:

Busca resolver problemas específicos de Hidrosoft relacionados con la protección de datos sensibles y la mitigación de riesgos de ingeniería social.

Propone estrategias prácticas basadas en estándares internacionales como la ISO/IEC 27001.

Exploratoria y Descriptiva:

Exploratoria: Identifica y comprende las vulnerabilidades existentes, así como las amenazas que enfrenta la organización en su entorno operativo.

Descriptiva: Detalla la naturaleza de los riesgos, las medidas de seguridad actuales y las deficiencias que requieren intervención.

3.3. Recolección de Información

Con el objetivo de obtener datos clave para el desarrollo de una estrategia de ciberseguridad que garantice la protección de los datos sensibles y mitigue los riesgos en Hidrosoft, se llevaron a cabo encuestas y entrevistas detalladas entre empleados de distintas áreas de la empresa. Esta fase fue esencial para comprender en profundidad el estado actual de la seguridad de la información dentro de la organización, identificar brechas en el conocimiento sobre ciberseguridad y evaluar las prácticas existentes en cuanto a la protección de datos. Además, permitió detectar áreas críticas que requieren atención inmediata y proponer soluciones específicas para mejorar la seguridad interna y la respuesta ante amenazas cibernéticas.

3.3.1. Encuestas

Se diseñó y aplicó una encuesta estructurada entre empleados de diferentes áreas clave de Hidrosoft, incluidos los equipos de TI, administrativo y operativo. La encuesta se enfocó en las prácticas actuales de seguridad, la conciencia de riesgos como phishing y pretexting, la participación en entrenamientos de seguridad y la percepción sobre la colaboración interna en temas de protección de datos (Anexo A Encuesta). También se evaluó el grado de conocimiento y aplicación de las políticas de seguridad internas. Los resultados obtenidos ayudaron a identificar brechas de conocimiento y áreas críticas que requieren atención inmediata.

3.3.2. Entrevistas en Profundidad

Además, se llevaron a cabo entrevistas en profundidad con directivos, responsables de TI y empleados clave de la empresa (Anexo B Entrevista). Estas

entrevistas permitieron explorar las políticas y procedimientos de seguridad actual, los desafíos en la adopción de medidas de seguridad, y los obstáculos que dificultan la implementación efectiva de controles. También se recogieron propuestas de mejora para optimizar las estrategias de protección. La información cualitativa obtenida en las entrevistas complementó los datos obtenidos en las encuestas.

3.4. Procesamiento de la Información

Después de recopilar la información mediante encuestas, entrevistas y revisión de documentos dentro de Hidrosoft, se procedió al procesamiento de estos datos para analizarlos y obtener conclusiones significativas. Para enriquecer el análisis y comprensión de los datos recopilados, se utilizaron tablas y referencias de la metodología de riesgo según el Esquema Gubernamental de Seguridad de la información (EGSI V3), así como un análisis en relación con la norma ISO 27001, que guía el proceso de gestión de riesgos de seguridad de la información.

El procesamiento de la información involucró varias actividades, entre ellas la organización y codificación de los datos recopilados, la tabulación de respuestas de las encuestas realizadas al personal de la empresa, así como los datos obtenidos de las entrevistas con los responsables de la unidad de Tecnologías de la Información (TI). Estas actividades se llevaron a cabo de manera sistemática y rigurosa para garantizar la fiabilidad y validez de los resultados.

Se realizaron tablas siguiendo la metodología MAGERIT & NTE-INEN ISO/IEC 27005 que permitieron organizar y estructurar los datos relacionados con la identificación y evaluación de los riesgos de seguridad de la información en Hidrosoft. Estas tablas proporcionaron una visualización clara de los riesgos identificados, sus causas y consecuencias potenciales, así como las medidas de control propuestas para mitigarlos.

Además, el análisis se complementó con la referencia a las mejores prácticas y los estándares establecidos por la ISO 27001, que permitió alinear los resultados con las normativas internacionales y adaptar las estrategias de seguridad a las necesidades específicas de Hidrosoft. Esto contribuyó a la creación de un Plan de

Seguridad de la Información que aborda de manera efectiva los riesgos de ingeniería social, accesos no autorizados y otras amenazas, garantizando la protección de los activos de información críticos de la empresa.

3.4.1. Organización y Sistematización de los Datos

Los datos recolectados fueron organizados cuidadosamente en diferentes categorías según su naturaleza y fuente. Esto incluyó:

Encuestas: Los resultados se agruparon por áreas de trabajo y perfiles de los participantes, lo que permitió comparar percepciones y conocimientos entre distintos niveles de la organización.

Entrevistas: Las respuestas cualitativas fueron transcritas y codificadas para identificar patrones, temas recurrentes y puntos críticos en las prácticas actuales de seguridad.

3.5. Metodología de Investigación

MAGERIT, como metodología de gestión de riesgos, proporciona un marco estructurado para analizar, evaluar y gestionar los riesgos asociados a los activos de información de una organización. En el caso de Hidrosoft, su aplicación se centra en garantizar la seguridad de los datos sensibles y la continuidad operativa frente a amenazas de ingeniería social. Los pasos clave en la aplicación de MAGERIT son:

Identificación de Activos: MAGERIT comienza con la identificación de los activos críticos de información, como bases de datos de clientes, sistemas operativos, equipos de red, y software de análisis de datos. Cada activo es catalogado en función de su importancia para los procesos operativos de Hidrosoft.

Detección de Amenazas y Vulnerabilidades: La metodología evalúa las amenazas potenciales, como phishing, malware o accesos no autorizados, y las vulnerabilidades que podrían explotarse, como la falta de autenticación

multifactorial o configuraciones deficientes.

Valoración de Riesgos: Cada combinación de activo, amenaza y vulnerabilidad se analiza en términos de su impacto (confidencialidad, integridad y disponibilidad) y su probabilidad de ocurrencia. Esto se traduce en un nivel de riesgo calculado a través de matrices específicas de MAGERIT.

Tratamiento de Riesgos: MAGERIT propone estrategias para mitigar, transferir, evitar o aceptar los riesgos. Estas acciones se priorizan según el nivel de riesgo identificado.

Documentación y Mejora Continua: La metodología documenta todo el análisis, los controles implementados y los resultados. Esto permite una evaluación constante y la adaptación de medidas frente a nuevas amenazas.

La metodología de investigación empleada para la elaboración del Plan de Seguridad de la Información en Hidrosoft se basa en el Esquema Gubernamental de Seguridad de la Información (EGSI) versión 2.0, una metodología de evaluación y tratamiento de riesgos adaptados a las necesidades de las organizaciones en el contexto de la seguridad de la información. Esta metodología proporciona un enfoque estructurado y detallado para identificar, evaluar, mitigar y gestionar los riesgos asociados a la información sensible en la empresa.

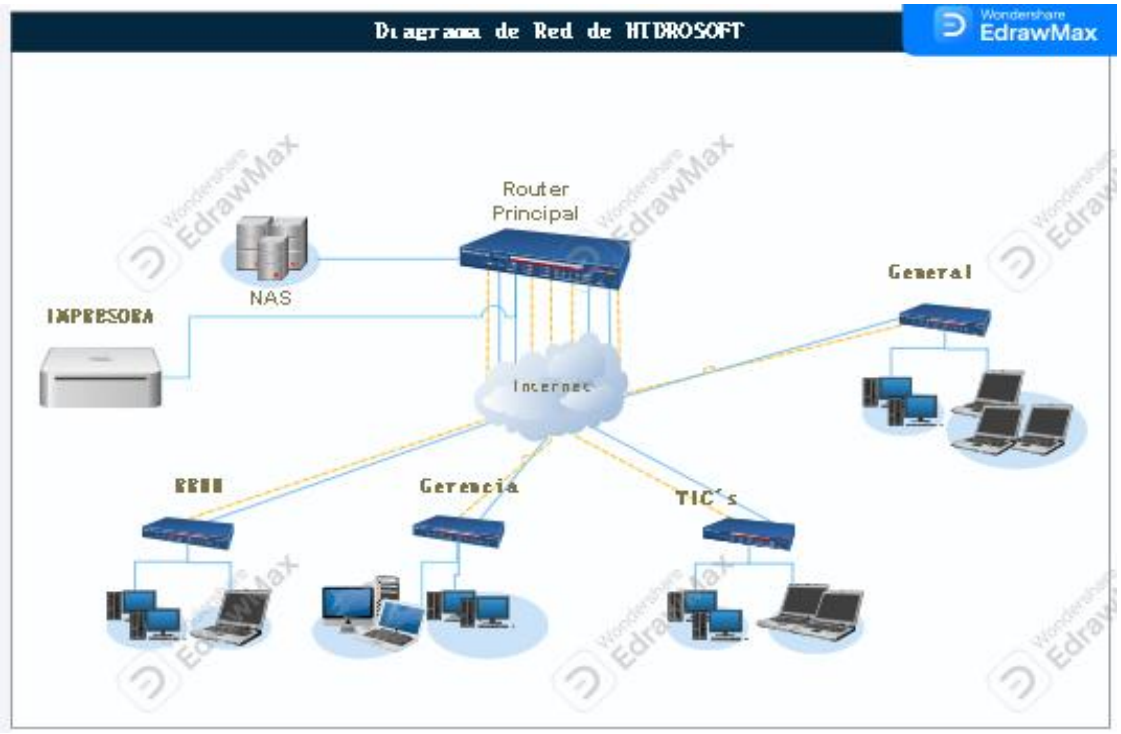
El EGSI versión 2.0 es una metodología de gestión de riesgos de seguridad de la información diseñada para fortalecer la protección de los activos de información en organizaciones públicas y privadas. Su enfoque permite establecer, evaluar y gestionar los riesgos de forma integral, garantizando que las políticas y controles de seguridad sean apropiados y eficaces.

La metodología EGSI se estructura en una serie de fases clave que abarcan desde la identificación de activos hasta la mejora continua del sistema de seguridad. Las fases del EGSI se adaptan a la infraestructura y necesidades específicas de la empresa, garantizando una protección adecuada de los datos sensibles, el proyecto se organiza en cinco fases principales:

3.5.1. Fase 1: Situación Actual

La red de Hidrosoft está diseñada para facilitar una comunicación eficiente, rápida y segura entre todos los dispositivos y sistemas que conforman la infraestructura tecnológica de la empresa. El NAS (Network Attached Storage) juega un papel fundamental al gestionar el almacenamiento de datos y las aplicaciones internas, centralizando toda la información crítica y permitiendo el acceso a los recursos de manera organizada y eficiente. Esta centralización facilita tanto el respaldo como la recuperación de datos, y asegura que la información esté siempre disponible para los empleados. Los empleados acceden a estos recursos mediante conexiones por cable (Ethernet) y Wi-Fi, lo que les brinda flexibilidad para trabajar tanto dentro de las instalaciones de la oficina como de manera remota o en el campo, asegurando que puedan realizar sus tareas sin interrupciones y con acceso a los datos necesarios en tiempo real.

Figura 1 Estructura de Red HIDROSOFT



Autor: Departamento TIC´s HIDROSOFT

En la figura anterior miramos la estructura de red de Hidrosoft según el departamento de TIC´s

El diagnóstico inicial en Hidrosoft, específicamente en relación con los riesgos

asociados a la ingeniería social, reveló una serie de vulnerabilidades significativas en los niveles técnico y humano. Este análisis, basado en encuestas, entrevistas, destaca las principales áreas críticas que deben ser abordadas para fortalecer la seguridad organizacional.

En el gráfico se observa la topología de red de Hidrosoft que se organiza en una estructura jerárquica y modular que permite una comunicación eficiente y segura entre sus distintos sistemas y usuarios. En términos generales, la red está diseñada con una arquitectura cliente-servidor, donde los servidores centrales gestionan los servicios clave como almacenamiento de datos, aplicaciones internas y acceso a internet. Los dispositivos finales, como estaciones de trabajo, equipos de campo y dispositivos móviles, se conectan a través de una infraestructura Ethernet y Wi-Fi, asegurando la cobertura en todas las instalaciones.

Percepción y Conciencia del Personal

Baja Sensibilización sobre Ingeniería Social:

Los resultados de las encuestas aplicadas al personal de diferentes áreas muestran que más del 70% de los empleados no identifica con claridad los riesgos asociados a técnicas comunes de ingeniería social, como el phishing, pretexting o baiting.

- **Falta de Capacitación:**

Aunque Hidrosoft cuenta con políticas básicas de seguridad, la mayoría de los empleados no ha recibido capacitación regular ni actualizada su conocimiento sobre amenazas emergentes en los últimos dos años.

- **Vulnerabilidades Humanas**

Tendencia a la Confianza Excesiva:

Las entrevistas con empleados clave revelaron que existe una cultura organizacional que fomenta relaciones de confianza interna y externa, lo cual es explotable por atacantes mediante tácticas de ingeniería social.

Ausencia de Protocolos Claros:

La falta de procedimientos documentados para verificar la autenticidad de solicitudes de acceso o información contribuye a errores humanos que podrían facilitar incidentes de seguridad.

- **Infraestructura Tecnológica y Controles**

Ausencia de Autenticación Multifactorial (MFA):

Los sistemas críticos de Hidrosoft utilizan únicamente contraseñas como mecanismo de autenticación, lo que incrementa el riesgo ante ataques de phishing.

Deficiencias en el Monitoreo:

La revisión documenta tecnológicas identificaron que no se cuenta con un sistema robusto de detección y respuesta a actividades sospechosas, lo que permite que intentos de ingeniería social pasen desapercibidos.

- **Prácticas y Normativas**

Cumplimiento Parcial de Normativas:

Aunque Hidrosoft reconoce la importancia de cumplir con la Ley Orgánica de Protección de Datos Personales (LOPDP), las entrevistas y revisión documental evidencian una implementación incompleta de los procedimientos exigidos, como la notificación de brechas de seguridad.

Falta de Protocolos de Respuesta a Incidentes:

No existen procedimientos estandarizados para manejar casos de ingeniería social, lo que dificulta la contención y recuperación en caso de incidentes.

5. Evaluación de Activos Críticos

Exposición de Información Sensible:

Los activos más valiosos, como bases de datos de clientes y empleados, carecen de cifrado robusto o medidas adicionales de protección frente a accesos no autorizados.

Dependencia de la Interacción Humana:

Procesos críticos, como el manejo de información entre departamentos, dependen excesivamente de la interacción humana, lo que los hace susceptibles a manipulaciones externas.

3.5.2. Fase 2: Preparación del EGSI VERSIÓN 2.0

Guía de Autodiagnóstico ISO 27001:2022 para Hidrosoft

El autodiagnóstico se refiere al conjunto de actividades realizadas por una organización para evaluar el estado actual de un sistema, proceso o actividad, en relación con un parámetro previamente establecido. En el caso de Hidrosoft, este proceso se enfoca en identificar la situación actual respecto a los requerimientos del sistema de gestión de seguridad de la información, conforme a la norma ISO 27001:2022.

Este instrumento se utiliza en la primera etapa del ciclo de mejoramiento continuo, específicamente en la fase de PLANEAR. A diferencia de una auditoría formal, el autodiagnóstico involucra la participación activa del personal de la organización, lo que implica que no se cumplen principios clave de auditoría, tales como objetividad, imparcialidad, autonomía e independencia.

Uno de los objetivos principales del autodiagnóstico para Hidrosoft es desarrollar un plan de implementación del modelo de seguridad de la información según la versión 2022 de la norma. Este proceso se basa en los capítulos de la norma ISO 27001:2022, específicamente desde el capítulo 4 hasta el 10, e incluye una lista de verificación con los requisitos que deben ser evaluados. En la segunda parte del diagnóstico, se encuentran los gráficos e información consolidada del análisis, los cuales se generan automáticamente con base en los resultados obtenidos.

Durante el diligenciamiento y la evaluación, se deben aplicar los siguientes criterios:

NO APLICA: Se marca con una "X" cuando el requisito no es relevante para Hidrosoft o ha sido excluido y no afecta la capacidad de la organización para cumplir con otros requisitos. Por ejemplo, si la organización no maneja ciertos tipos de datos sensibles, algunos controles relacionados no aplican.

COMPLETO: Se marca con una "X" cuando se han realizado todas las acciones requeridas, se cuenta con evidencia suficiente que respalda el cumplimiento del requisito y se han obtenido resultados eficaces que demuestran que se ha cumplido con el estándar.

PARCIAL: Se marca con una "X" cuando no se ha completado alguna de las acciones necesarias o la evidencia es insuficiente. Aunque se han logrado algunos resultados, estos no son totalmente eficaces o no cumplen con el objetivo establecido en la norma.

NINGUNO: Se marca con una "X" cuando no se han realizado actividades relacionadas con el requisito, y no existen evidencias ni resultados asociados con dicho requisito.

Tabla 1 Controles Instrumento de Evaluación ISO 27001

	CONTROLES ANEXO A ISO 27001:2022			ESTADO DEL CONTROL		
5	**CONTROLES ORGANIZACIONALES**		**NO APLICA**	**COMPLETO**	**PARCIAL**	**NINGUNO**
5	**CONTROLES ORGANIZACIONALES**					
5.1	Políticas de seguridad de la información	**Control** La política de seguridad de la información y las políticas específicas asociadas deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal pertinente y partes interesadas pertinentes, y revisadas a intervalos planificados y cuando ocurran cambios significativos en la organización				X
5.2	Roles y responsabilidades en la Seguridad de la Información	**Control** Los roles y responsabilidades de seguridad de la información se deben definir y asignar de acuerdo con las necesidades de la organización				X
5.3	Segregación de deberes	**Control** Los deberes y áreas de responsabilidad en conflicto deberían segregarse				X
5.4	Responsabilidades de la dirección	Control La Alta Dirección debe exigir a todo el personal la aplicación de la seguridad de la Información de acuerdo con la política de seguridad de la Información establecida, las políticas y los procedimientos específicos de la organización en los aspectos correspondientes.	X			
5.5	Contacto con las autoridades	Control La organización debe establecer y mantener contacto con las autoridades pertinentes.			X	
5.6	Contacto con grupos de interés especial	Control La organización debe establecer y mantener contacto con grupos de interés especial u otros foros y asociaciones profesionales especializados en Seguridad			X	
5.7	Inteligencia de amenazas	Control información se debe documentar y poner a disposición del personal que los necesite				
6	**CONTROLES DE PERSONAS**					
6.1	RESPONSABILIDAD DE LA DIRECCIÓN	Control Las verificaciones de antecedentes de todos los candidatos para convertirse en personal se deben llevar a cabo antes de unirse a la organización y de forma continúa teniendo en cuenta las leyes, regulaciones y ética aplicables y deben ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos			X	

Fuente: 1Instrumento de Evaluación ISO 27001

6.2	Términos y condiciones de empleo	Control Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización para la seguridad de la información			**X**	
6.3	Conciencia de seguridad de la información, educación y formación	Control El personal de la organización y las partes interesadas pertinentes deben recibir información, educación y capacitación adecuadas sobre seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos del tema, según sea pertinente para su función laboral			**X**	
6.4	Proceso disciplinario	Control Se debe formalizar y comunicar un proceso disciplinario para tomar medidas contra el personal y otras partes interesadas pertinentes que hayan cometido una violación de la política de seguridad de la información			**X**	
6.5	Responsabilidades después de la	Control cumplir y comunicar al personal pertinente y a otras partes interesadas				
7	**CONTROLES FÍSICOS**					
7.1	Perímetros de seguridad física	Control Los perímetros de seguridad se deben definir y utilizar para proteger las zonas que contengan información y otros activos asociados.			**X**	
7.2	Entrada física	Control Las zonas seguras deben estar protegidas por controles de entrada y puntos de accesos adecuados			**X**	
7.3	Asegurar oficinas, habitaciones e instalaciones	Control Se debe diseñar e implementar la seguridad física de las oficinas, salas e instalaciones.			**X**	
7.4	Monitoreo de la seguridad física	Control Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados				**X**
7.5	Protección contra amenazas físicas y ambientales	Control Se debe diseñar e implementar la protección contra las amenazas físicas y medioambientales, como las catástrofes naturales y otras amenazas físicas intencionadas o no intencionadas a las infraestructuras.			**X**	
8	**CONTROLES TECNOLOGICOS**					
8.1	Dispositivos de punto final de usuario	Control Se debe proteger la información almacenada, procesada o accesible a través de los dispositivos de punto final del usuario			**X**	
8.2	Derechos de acceso privilegiado	Control La asignación y el uso de los derechos de acceso privilegiado deben estar restringidos y gestionados.			**X**	
8.3	Restricción de acceso a la información	Control El acceso a la información y a otros activos asociados se debe restringir de acuerdo con la política específica establecida sobre el control de acceso.			**X**	
8.4	Acceso al código fuente	Control El acceso para leer o escribir sobre un código fuente, las herramientas de desarrollo, y las librerías de software se deben gestionar apropiadamente				**X**
8.5	Autenticación segura	Control Se deben implementar tecnologías y procedimientos de autenticación seguros basados en restricciones de acceso a la información y en la política específica del tema sobre control de acceso.			**X**	

Fuente: 2ISO 27001:2022

Siguiendo el enfoque metodológico de la norma ISO 27001:2022, se realizaron los controles de seguridad de la información en Hidrosoft con el propósito de evaluar y mejorar la protección de los activos más importantes de la empresa. En el ANEXO C se describe detalladamente la implementación de estos controles, que cubren aspectos fundamentales como la gestión de documentos, el almacenamiento seguro de datos, la protección de información sensible y el control de acceso a sistemas y aplicaciones clave. Este análisis detallado ofrece una visión clara de la situación actual de la organización en términos de seguridad de la información, resaltando tanto los puntos fuertes como las áreas que requieren atención.

A través del proceso de autodiagnóstico, se identificaron los controles que ya están funcionando correctamente y las áreas donde es necesario hacer ajustes o implementar nuevas medidas. Los resultados proporcionan una comprensión profunda de las fortalezas de la empresa en cuanto a la protección de los datos, al tiempo que señalan las vulnerabilidades que deben abordarse para minimizar los riesgos.

Con base en este análisis, se podrá desarrollar un plan de acción enfocado en la mejora continua de la seguridad de la información, priorizando aspectos críticos como la autenticación multifactor para los accesos a sistemas sensibles, el cifrado de datos en tránsito y en reposo, y la capacitación constante del personal sobre amenazas como phishing e ingeniería social. Los controles y medidas adicionales que se implementen no solo buscarán cumplir con los requisitos de la ISO 27001:2022, sino también proteger de manera más efectiva la integridad, confidencialidad y disponibilidad de la información, garantizando que Hidrosoft siga operando de forma segura, eficiente y alineada con los estándares internacionales.

Evaluación de Efectividad de controles

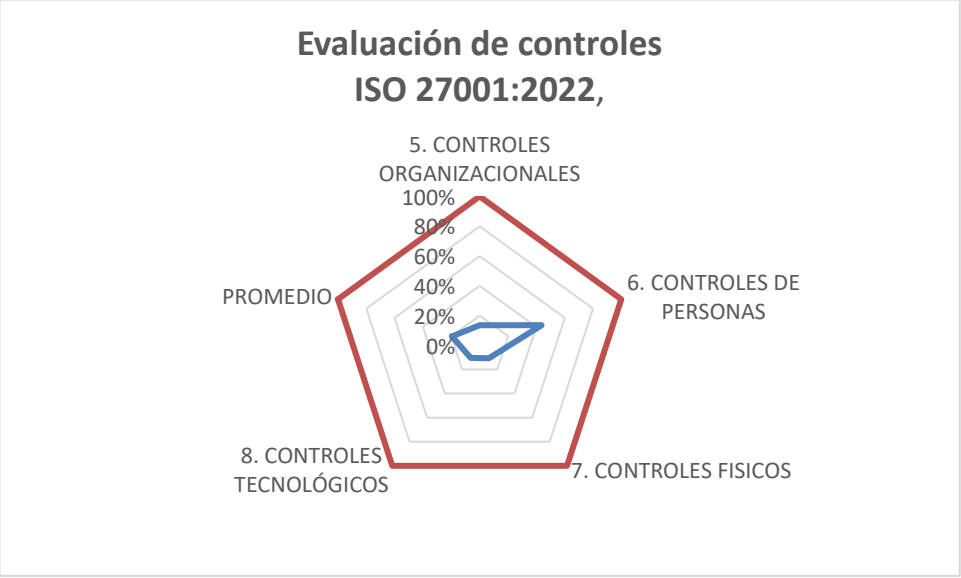
Tabla 2 Evaluación de Efectividad de Controles

CAPÍTULOS	NIVEL DE IMPLEMENTACIÓN	
	NIVEL ACTUAL	NIVEL DESEADO
5. CONTROLES ORGANIZACIONALES	14%	100%
6. CONTROLES DE PERSONAS	44%	100%
7. CONTROLES FISICOS	11%	100%
8. CONTROLES TECNOLÓGICOS	10%	100%
PROMEDIO	20%	100%

Fuente: Autor

La Tabla 2 describe en términos generales los principales hallazgos de la evaluación de los controles de seguridad en Hidrosoft, el tipo de control, el nivel de implementación actual y el nivel deseado.

Figura 2 Evaluación de Controles



Fuente: Autor

En la Figura 2 se observa el porcentaje de la evaluación de los diferentes controles; Organizacionales, Personas, Físicos, Tecnológicos.

La evaluación del cumplimiento de los controles de seguridad según el ANEXO C de CONTROLES según la ISO 27001:2022 en Hidrosoft revela preocupaciones en varios dominios clave de la seguridad de la información, especialmente en lo relacionado con la ingeniería social y otros aspectos críticos de protección de datos. La mayoría de los componentes evaluados no cumplen con los requisitos establecidos por la norma, incluyendo áreas fundamentales como políticas de seguridad, gestión de activos, control de acceso y seguridad en las operaciones. Este hallazgo indica que los controles de seguridad y las políticas correspondientes no se están implementando de manera adecuada, lo que podría dejar a la organización vulnerable a amenazas, especialmente aquellas derivadas de técnicas de ingeniería social como el phishing o el vishing.

Es evidente que Hidrosoft necesita realizar mejoras significativas en casi todos los dominios evaluados para alcanzar un nivel adecuado de seguridad de la información. Sin embargo, hay áreas en las que la organización ya cumple parcial o totalmente con la norma.

3.5.3. Fase 3: Análisis de Riesgo

Metodología de evaluación y tratamiento de riesgos

El proceso de identificación de los activos, vulnerabilidades y amenazas en Hidrosoft se ha realizado de acuerdo con los principios de la GUÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (EGSI VERSIÓN 2.0) ISO 27005 y la metodología “MAGERIT” con el uso del cuadro de la matriz de evaluación de riesgos definido en el “Anexo del Acuerdo Ministerial No. 025-2019, Este análisis es crucial para detectar los riesgos que pueden afectar la seguridad de la información en la organización, y asegurar que los activos sean protegidos adecuadamente.

Identificación de los Activos

El primer paso en la evaluación de riesgos es identificar los activos dentro del alcance del EGSI, es decir, todos los activos que pueden afectar la seguridad

de la información en Hidrosoft. Los activos se clasifican en diferentes categorías, cada una de ellas responsable de salvaguardar elementos críticos para la operación de la empresa.

Tabla 3 Listado de Activos

Nro. Activo	Proceso Macro	Subproceso	Tipo de Activo	Nombre de Activo	Descripción del activo
A1	Mantenimiento de servidores	Mantenimiento de Servidor NAS	Hardware	NAS	Dispositivo de almacenamiento de alta capacidad conectado a una red
A2	Gestión Tecnológico	Actualización de Software de Sistemas Operativos	Software	SISTEMA OPERATIVO DE COMPUTADOR DE ESCRITORIO	Es un software que actúa como intermediario entre el hardware de un computador y los programas y aplicaciones que se ejecutan en él
A3	Mantenimiento de red	Operación y Mantenimiento	Redes	FORTIGATE	Firewall de Red, para proteger la comunicación de la red.
A4	Protección de DATA CENTER	Instalación de Equipo	Localidad	BIOMETRICO POR RFID	Es un dispositivo que utiliza tecnología de identificación por radiofrecuencia (RFID) y tecnología biométrica para autenticar la identidad de una persona
A5	Soporte técnico	Soporte técnico de primer nivel	Organización	DESK SERVICE	El service desk es un soporte multifuncional que incorpora desde servicios técnicos a comerciales.
A6	Gestión Administrativa Financiera	Servidor Contable	Datos	BASE DE DATOS DEL SISTEMA	Es una herramienta informática que almacena y gestiona información financiera y contable de la Empresa. Esta base de datos contiene información como facturas, recibos, estados financieros, registros de cuentas, movimientos de cuentas bancarias, balances, entre otros.
A7	Estructura Orgánica	Cargos inadecuados del personal	Personal	TIC´s	Son recursos y herramientas que se utilizan para el proceso, administración y distribución de la información a través de elementos tecnológicos

Fuente: Gobierno Electrónico. (2019). Hoja de ruta EGSI. https ://www.gobiernoelectronico.gob.ec /hoja -de -ruta -egsi/

En la Tabla 3 se observa el listado de los principales activos de HIDROSOFT los cuales se detallan con el número de activo, el proceso macro, sub proceso, Tipo de activo, nombre de activo y descripción del activo.

Impacto y probabilidad

Para la valoración de los activos, amenazas, vulnerabilidades y el nivel de riesgo al interior de HIDROSOFT, se seguirá el siguiente proceso de manera resumida:

1. Identificación de Amenazas y Vulnerabilidades: Se identificarán todas las amenazas y vulnerabilidades relacionadas con cada activo dentro del alcance del Esquema Gubernamental de Seguridad de la Información (EGSI). Estas amenazas y vulnerabilidades se pueden obtener de los catálogos incluidos en la Norma Técnica NTE INEN-ISO/IEC 27005.

Tabla 4 Análisis de Riesgos

Análisis de Riesgos				
Proceso Macro	**Subprocesos**	**Nro. Activo**	**Amenaza**	**Vulnerabilidad**
Mantenimiento de servidores	Mantenimiento de Servidor NAS	A1	Incumplimiento en el mantenimiento del sistema de información	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.
			Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad.
			Fenómenos meteorológicos	Susceptibilidad a las variaciones de temperatura
			Hurto de medios o documentos	Copia no controlada
			Hurto de medios o documentos	Almacenamiento sin protección
			Pérdida del suministro de energía	Susceptibilidad a las variaciones de voltaje
Gestión Tecnológico	Actualización de Software de Sistemas Operativos	A2	Fallos en la actualización	Ausencia o insuficiencia de pruebas de software
			Vulnerabilidades de seguridad	Software nuevo o inmaduro
			Interrupción del flujo de trabajo	Interfaz de usuario compleja
Mantenimiento de red	Operación y Mantenimiento	A3	Negación de acciones	Ausencia de pruebas de envío o recepción de mensajes
			Escucha encubierta	Líneas de comunicación sin protección

			Escucha encubierta	Tráfico sensible sin protección
			Falsificación de derechos	Ausencia de identificación y autentificación de emisor y receptor
			Falla del equipo de telecomunicaciones	Conexión deficiente de los cables.
Protección de DATA CENTER	Instalación de Equipo	A4	Destrucción de equipo o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos
			Pérdida del suministro de energía	Red energética inestable
			Hurto de equipo	Ausencia de protección física de la edificación, puertas y ventanas
Soporte técnico	Soporte técnico de primer nivel	A5	Perdida de equipo	Ausencia de planes de continuidad
			Ingeniería social	Fugas de información
Gestión Administrativa Financiera	Servidor Contable	A6	Hurto de medios o documentos	Copia no controlada
			Hurto de medios o documentos	Almacenamiento sin protección
			Ausencia de documentación	Error en el uso
Estructura Orgánica	Cargos Inadecuados de Personal	A7	Incumplimiento en la disponibilidad del personal	Ausencia de personal
			Uso no autorizado de los equipos	Ausencia de mecanismos de monitoreo
			Destrucción de equipos y medios	Procedimientos inadecuados de contratación

Fuente: Fuente: Gobierno Electrónico. (2019). Hoja de ruta EGSI . https ://www .gobiernoelectronico .gob .ec /hoja -de -ruta -egsi/

En la Tabla 4 se observa el análisis de riesgos, los cuales detallan las posibles amenazas y vulnerabilidades de cara activo.

2. Valoración del Impacto (Consecuencias): Para cada combinación de amenaza y vulnerabilidad de un activo específico, se evaluará el impacto que

podría tener si dicha combinación se materializa. El impacto se evaluará en términos de las siguientes dimensiones:

Confidencialidad: La pérdida de confidencialidad de la información.

Tabla 5 Valoración del impacto - Confidencialidad

Valoración del impacto en términos de la perdida de la **confidencialidad**	**Criterio**
Alto (3)	La divulgación no autorizada de la información tiene un efecto crítico para la institución Ej. Divulgación de información confidencial o sensible.
Medio (2)	La divulgación no autorizada de la información tiene un efecto limitado para la institución Ej. Divulgación de información de uso interno
Bajo (1)	La divulgación de la información no tiene ningún efecto para la institución Ej. Divulgación de información pública.

Fuente: Fuente: Gobierno Electrónico. (2019). Hoja de ruta EGSI . https ://www .gobiernoelectronico .gob .ec /hoja -de -ruta -egsi/

En la tabla 5 se describe la valoración del impacto en términos de la perdida de la confidencialidad y sus respectivos criterios.

Integridad: La posibilidad de destrucción o modificación no autorizada de la información.

Tabla 6 Valoración del impacto - Integridad

Valoración del impacto en términos de la perdida de la **integridad**	**Criterio**
Alto (3)	La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución
Medio (2)	La destrucción o modificación no autorizada de la información tiene un efecto considerable para la institución
Bajo (1)	La destrucción o modificación de la información tiene un efecto leve para la institución

Fuente: Fuente: Gobierno Electrónico. (2019). Hoja de ruta EGSI . https ://www .gobiernoelectronico .gob .ec /hoja -de -ruta -egsi/

En la Tabla 6 se observa la valoración del impacto en términos de la perdida de la integridad y sus criterios.

- Disponibilidad: El impacto de no poder acceder a la información o los sistemas cuando se requiera.

Tabla 7 Valoración del impacto - Disponibilidad

Valoración del impacto en términos de la perdida de **disponibilidad**	**Criterio**
Alto (3)	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución
Medio (2)	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución
Bajo (1)	interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la institución

Fuente: Fuente: Gobierno Electrónico. (2019). Hoja de ruta EGSI . https ://www .gobiernoelectronico .gob .ec /hoja -de -ruta -egsi/

En la Tabla 7 se describe la valoración del impacto en términos de la perdida de disponibilidad y sus criterios respectivos.

La valoración del impacto de un activo (VA), resultó del promedio de los valores de las tres dimensiones de la Gestión de la Seguridad de la Información asociado a cada activo de información identificado:

VA=(C+I+D)/3

3. Evaluación de la Probabilidad: Se analizará la probabilidad de que cada combinación de amenaza y vulnerabilidad se materialice y genere un impacto en el activo. La probabilidad se puede evaluar en una escala cualitativa, alta, media o baja.

Tabla 8 ESTIMACIÓN DE AMENAZAS

ESTIMACIÓN DE AMENAZAS

Nivel de amenazas	**Criterio por probabilidad**
Alto (3)	La ocurrencia es muy probable (probabilidad > 50%)
Medio (2)	La ocurrencia es probable (probabilidad =50%)
Bajo (1)	La ocurrencia es menos probable (probabilidad >0 y <50%)
No aplica (0)	

Fuente: Fuente: Gobierno Electrónico. (2019). Hoja de ruta EGSI . https ://www .gobiernoelectronico .gob .ec /hoja -de -ruta -egsi/

En la Tabla 8 se observa la estimación de amenazas, su nivel de amenaza y su criterio por probabilidad.

4. Nivel de Riesgo: Con base en la valoración del impacto y la probabilidad, se determinará el nivel de riesgo para cada combinación de amenaza y vulnerabilidad. Esto permitirá clasificar los riesgos en función de su criticidad, identificando aquellos que requieren una mayor atención y tratamiento.

Tabla 9 ESTIMACIÓN DE LAS VULNERABILIDADES

ESTIMACIÓN DE LAS VULNERABILIDADES

Nivel de vulnerabilidad	Criterio
Alto (3)	No existe ninguna medida de seguridad implementada para prevenir la ocurrencia de la amenaza
Medio (2)	Existen medidas de seguridad implementadas que no reducen la probabilidad de ocurrencia de la amenaza a un nivel aceptable
Bajo (1)	La medida de seguridad es adecuada

Fuente: Fuente: Gobierno Electrónico. (2019). Hoja de ruta EGSI . https ://www .gobiernoelectronico .gob .ec /hoja -de -ruta -egsi/

En la Tabla 9 se observa la estimación de las vulnerabilidades, su nivel de vulnerabilidad y su criterio.

Tabla 10 Análisis de Riesgos

Análisis de Riesgos					Evaluación de Riesgos				
					Impacto	Probabilidad		Cálculo de Evaluación Riesgo	Nivel de Riesgo
Proceso Macro	Subprocesos	Nro. Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad		
Mantenimiento de Servidores	Mantenimiento de NAS		Hurto de medios o documentos	Copia no controlada	2,67	3	2	16,00	ALTO
			Hurto de medios o documentos	Almacenamiento sin protección	2,67	3	3	24,00	ALTO
Gestión Tecnológico	Actualización de Software de Sistemas Operativos	A2	Fallos en la actualización	Ausencia o insuficiencia de pruebas de software	1,67	1	1	1,67	BAJO
			Vulnerabilidades de seguridad	Software nuevo o inmaduro	1,67	2	2	6,67	MEDIO
Mantenimiento de red	Operación y Mantenimiento	A3	Negación de acciones	Ausencia de pruebas de envío o recepción de mensajes	3,00	1	2	6,00	MEDIO
			Escucha encubierta	Tráfico sensible sin protección	3,00	3	2	18,00	ALTO
Protección de DATA CENTER	Instalación de Equipo	A4	Destrucción de equipo o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3,00	3	2	18,00	ALTO
			Hurto de equipo	Ausencia de protección física de la edificación, puertas y ventanas	3,00	2	3	18,00	ALTO
Soporte técnico	Soporte técnico de primer nivel	A5	Perdida de equipo	Ausencia de planes de continuidad	3,00	2	2	12,00	ALTO
			Ingeniería social	Fugas de información	3,00	3	3	27,00	ALTO
			Ausencia de documentación	Error en el uso	2,67	1	1	2,67	BAJO
Estructura Orgánica	Cargos Inadecuados de Personal	A7	Incumplimiento en la disponibilidad del personal	Ausencia de personal	2,33	2	2	9,33	ALTO
			Uso no autorizado de los equipos	Ausencia de mecanismos de monitoreo	2,33	3	2	14,00	ALTO

Fuente: Fuente: Gobierno Electrónico. (2019). Hoja de ruta EGSI . https ://www .gobiernoelectronico .gob .ec /hoja -de -ruta -egsi/

En la tabla 10 se muestra un Análisis y Evaluación de Riesgos relacionado con diversos procesos y subprocesos, como en áreas de mantenimiento de servidores, NAS, gestión tecnológica, entre otros. Cada fila describe un riesgo potencial asociado con una amenaza específica y su vulnerabilidad correspondiente, seguida del cálculo de la Evaluación de Riesgo y el nivel de riesgo resultante; en el ANEXO E se observa más a detalle dicho análisis.

Evaluación del Riesgo

El nivel de riesgo se determinó como el resultado de multiplicar la probabilidad de que ocurra una amenaza, la probabilidad de que se presente una vulnerabilidad y el valor del impacto del activo de información (CID), es decir:

Nivel de riesgo = Nivel de amenaza * Nivel de vulnerabilidad * Valor de impacto del activo (CID)

Con base en este cálculo, se definió un sistema de semaforización que ayudará a seleccionar la opción más adecuada para tratar los riesgos identificados.

Tabla 11 Evaluación del Riesgo

El Riesgo es:	*NIVEL DE RIESGO (nivel de amenaza * nivel de vulnerabilidad * VA)*
ALTO	*de 9 a 27*
MEDIO	*de 4 a 8*
BAJO	*de 1 a 3*

Fuente: 3 Fuente: Gobierno Electrónico. (2019). Hoja de ruta EGSI . https ://www .gobiernoelectronico .gob .ec /hoja -de -ruta -egsi/

En la Tabla se mira la semaforización de la evaluación de riesgos; el riesgo puede ser Alto, Medio, Bajo y el nivel de riesgo varía de 9 a 27, de 4 a 8, de 1 a 3 respectivamente.

Tratamiento de riesgos

En el proceso de tratamiento de riesgos al interior de HIDROSOFT para la aceptación de riesgos, se llevarán a cabo las siguientes actividades de manera resumida:

Tabla 12 OPCIONES DE TRATAMIENTO

OPCIONES DE TRATAMIENTO	
MITIGAR, REDUCIR O MODIFICAR EL RIESGO	Selección de uno o varios controles para reducir el riesgo a un nivel aceptable para la institución ej. Implementar políticas de control de acceso
EVITAR EL RIESGO	Eliminar la actividad de alto riesgo o cambiar las condiciones bajo las cuales la actividad es operada (remover el riesgo)
TRANSFERIR O DESVIAR EL RIESGO	Trasferir el riesgo a otra entidad interna o externa mediante: el traspaso de la gestión del activo y/o del riesgo, pólizas de seguros o tercerización seguros, etc., para cambiar o compartir la responsabilidad de la pérdida.
ACEPTAR O RETENER EL RIESGO	Tomar la decisión de aceptar las consecuencias de un riesgo en particular, es decir, no se realiza ninguna acción respecto al riesgo

Fuente: Fuente: Gobierno Electrónico. (2019). Hoja de ruta EGSI . https ://www .gobiernoelectronico .gob .ec /hoja -de -ruta -egsi/

En la Tabla 10 se observa las opciones de tratamiento del riesgo; MITIGAR / EVITAR / TRANSFERIR / ACEPTAR el riesgo.

Las opciones de tratamiento seleccionadas se implementarán a través del cuadro de tratamiento de riesgos. Se escogerán los controles de seguridad adecuados y se evaluará el nuevo valor del impacto y la probabilidad en el cuadro de tratamiento de riesgos para evaluar la efectividad de las medidas planificadas.

Análisis de Riesgos		Evaluación de Riesgos		Tratamiento de Riesgos							Riesgo residual
Nro. Activo	Amenaza	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Método de tratamiento de Riesgos	Tipo de control	Controles a Implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado	
A1	Incumplimiento en el mantenimiento del sistema de información	5,33	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	GENERAR UN CRONOGRAMA DE MANTENIMIENTO CON UN RESPONSABLE PARA INFORMAR	1	1	2,67	BAJO	ACEPTABLE
	Polvo, corrosión, congelamiento	2,67	BAJO	ACEPTAR	NO APLICA CONTROL						
A2	Fallos en la actualización	1,67	BAJO	ACEPTAR	NO APLICA CONTROL						
	Vulnerabilidades de seguridad	6,67	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	ADQUISICION DE LICENCIAS	1	1	1,67	BAJO	ACEPTABLE
A3	Negación de acciones	6,00	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	TESTEO DE COMUNICACIÓN	1	2	6,00	MEDIO	INACEPTABLE
	Escucha encubierta	18,00	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	AUTORIZACION POR MAC	1	1	3,00	BAJO	ACEPTABLE
A4	Destrucción de equipo o medios	18,00	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL CORRECTIVO	PROTECCION DEL EQUIPO MEDIANTE CASE	1	1	3,00	BAJO	ACEPTABLE
	Pérdida del suministro de energía	6,00	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	IMPLEMENTACION DE UPS	1	1	3,00	BAJO	ACEPTABLE
A5	Perdida de equipo	12,00	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	CONTROL PREVENTIVO	1	1	3,00	BAJO	ACEPTABLE
	Ingeniería social	27,00	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	BLOQUEO DE PAGINAS NO AUTORIZADAS	1	2	6,00	MEDIO	INACEPTABLE
A6	Hurto de medios o documentos	10,67	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	CIFRADO DE LA INFORMACION	1	1	2,67	BAJO	ACEPTABLE
	Hurto de medios o documentos	24,00	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	CREACION DE ESPEJO	2	1	5,33	MEDIO	INACEPTABLE
A7	Incumplimiento en la disponibilidad del personal	9,33	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	DELEGACION DERESPONSABILIDADES Y CONTRATAR PERSONAL IDONEO	1	1	2,33	BAJO	ACEPTABLE
	Uso no autorizado de los equipos	14,00	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL CORRECTIVO	CREAR SALES E IMPLEMENTAR PERSONAL DE MONITOREO DE CCTV	1	1	2,33	BAJO	ACEPTABLE

Fuente: Gobierno Electrónico. (2019). Hoja de ruta EGSI. https ://www .gobiernoelectronico .gob .ec /hoja -de -ruta -egsi/

En esta tabla se mira el proceso mediante el cual se gestionan los riesgos identificados para mitigar su impacto o probabilidad de ocurrencia. Se detallan diversos tratamientos de riesgos junto con los tipos de controles y el riesgo residual posterior a la implementación de dichos controles. En el Anexo E se evidencia más a detalle lo antes mencionado.

3.5.4. Fase 4: Desarrollo del Plan de Seguridad

Mediante recomendaciones éticas y estrategias específicas de ciberseguridad para Hidrosoft, enfocadas en cumplir con el marco normativo y las mejores prácticas, se busca asegurar la protección de los datos sensibles de clientes y empleados. En términos generales, los puntos mencionados son esenciales para desarrollar una estrategia robusta de ciberseguridad y garantizar que la empresa mantenga prácticas éticas y transparentes en su relación con empleados, clientes y socios. A continuación, se presenta un resumen de cada uno de estos puntos.

Código Ético en Ciberseguridad:

El código ético es una herramienta clave para guiar las decisiones relacionadas con la seguridad de la información dentro de la empresa. Este documento establece principios fundamentales como el compromiso con la privacidad de los datos, la responsabilidad corporativa, la transparencia en la gestión de riesgos y el cumplimiento normativo. Un código ético bien estructurado contribuye a crear un entorno de confianza y promueve comportamientos responsables frente a incidentes de seguridad el cual se detalla en el Anexo F a profundidad en su punto número 4.

Campañas Internas de Concienciación:

La concienciación de los empleados es fundamental para garantizar que comprendan y adopten los principios del código ético en su trabajo diario. Las campañas internas incluyen actividades como la distribución de material educativo, talleres interactivos, seminarios, y simulaciones de incidentes de seguridad. Estos esfuerzos buscan fortalecer la cultura de ciberseguridad en la organización, asegurando que cada empleado sepa cómo actuar ante riesgos cibernéticos y entienda la importancia de proteger los datos sensibles. En el Anexo F inciso 2 se detalla un plan estructurado de las capacitaciones continuas sobre ingeniería social clave para equipar a los empleados con las herramientas necesarias para identificar y mitigar las amenazas de ingeniería social.

Relación con Clientes; Comunicación Transparente:

La transparencia con los clientes es clave para generar confianza y demostrar un compromiso con la seguridad y la protección de datos. Esto implica mantener a

los clientes informados sobre las medidas de seguridad adoptadas por la empresa, los avances en la protección de datos, y compartir informes de auditorías externas que certifiquen el cumplimiento de las normativas de seguridad. Además, la gestión de incidentes debe ser clara y efectiva, con protocolos definidos para la comunicación oportuna de cualquier incidente relevante los cuales se encuentran detallados en el Anexo F.

Propuesta de Monitoreo Continuo y Auditorías de Seguridad:

Para prevenir y detectar posibles amenazas de manera temprana, es necesario implementar un sistema de monitoreo continuo de los sistemas de la empresa, utilizando herramientas avanzadas como sistemas de detección de intrusos (IDS) y análisis de comportamientos sospechosos los cuales se detallan en el Anexo F a profundidad en su punto número 5. Las auditorías regulares de seguridad permiten evaluar la eficacia de las medidas adoptadas y garantizar que se estén cumpliendo los estándares de ciberseguridad establecidos, reduciendo la probabilidad de incidentes graves.

Cumplimiento Normativo y Referencias Legales:

El cumplimiento de las leyes y regulaciones locales e internacionales relacionadas con la protección de datos y la ciberseguridad es esencial para evitar sanciones legales y proteger la reputación de la empresa. En el anexo G se detalla ampliamente, esto incluye alinearse con normativas como el Reglamento General de Protección de Datos (GDPR) y las leyes locales de protección de datos, que establecen obligaciones específicas para el manejo de la información personal y la seguridad en los sistemas de TI.

3.5.5. Fase 5: Resultados

Esta fase tiene como objetivo proporcionar una evaluación global del proceso de gestión de riesgos de seguridad de la información realizado en Hidrosoft: el impacto de las medidas implementadas, los riesgos residuales aceptados y las lecciones aprendidas para continuar mejorando la seguridad en la organización. A continuación se presentan los resultados del proceso.

En el marco de la gestión de activos y procesos dentro de la empresa Hidrosoft, se presenta a continuación una tabla que describe los activos clave relacionados con los procesos macro y subprocesos de la organización. Esta tabla busca ilustrar los diferentes tipos de activos que se utilizan en el desarrollo y la implementación de proyectos, detallando su ubicación, valor y la intención de su uso. A través de la clasificación de los activos, se puede entender mejor la estructura y el flujo de trabajo dentro de la empresa.

Tabla 13 Listado y valoración de los activos de información

Nro. Activo	Proceso Macro	Subproceso	Tipo de Activo	Nombre de Activo	Descripción del activo	Intención del Uso	Tipo de soporte	Ubicación	Valoración de Impacto (pérdida) C: Confidencialidad I: Integridad D: Disponibilidad			
									C	I	D	VA
A1	Mantenimiento de servidores	Mantenimiento de Servidor NAS	Hardware	NAS	Dispositivo de almacenamiento de alta capacidad conectado a una red	Permite a los usuarios y clientes autorizados, almacenar y recuperar datos en una ubicación localizada	Físico	Data Center	3	3	2	2,67
A2	Gestión Tecnológico	Actualización de Software de Sistemas Operativos	Software	SISTEMA OPERATIVO DE COMPUTADOR DE ESCRITORIO	Es un software que actúa como intermediario entre el hardware de un computador y los programas y aplicaciones que se ejecutan en él	Se encarga de administrar los recursos del sistema, como la memoria y el procesador, y proporciona una interfaz de usuario para que el usuario pueda interactuar con el equipo.	Lógico	Matriz Institución	1	1	3	1,67
A3	Mantenimiento de red	Operación y Mantenimiento	Redes	FORTIGATE	Firewall de Red, para proteger la comunicación de la red.	Dispositivo que se utiliza para proteger una red de amenazas externas a través de la gestión del tráfico de red	Físico y Lógico	Data Center	3	3	3	3,00
A4	Protección de DATA CENTER	Instalación de Equipo	Localidad	BIOMETRICO POR RFID	Es un dispositivo que utiliza tecnología de identificación por radiofrecuencia (RFID) y tecnología biométrica para autenticar la identidad de una persona	La tecnología RFID permite la lectura de etiquetas o tarjetas a través de ondas de radio, mientras que la tecnología biométrica utiliza rasgos físicos únicos, como huellas dactilares o reconocimiento facial, para confirmar la identidad de una persona	Físico	Data Center	3	3	3	3,00
A5	Soporte técnico	Soporte técnico de primer nivel	Organización	DESK SERVICE	El service desk es un soporte multifuncional que incorpora desde servicios técnicos a comerciales.	Sus funciones sirven para brindar soporte a los clientes y organizar los procesos internos de la empresa (demandas de soporte que se generan en el interior de las organizaciones).	Físico y Lógico	Matriz institución	3	3	3	3,00

A6	Gestión Administrativa Financiera	Servidor Contable	Datos	BASE DE DATOS DEL SISTEMA	Es una herramienta informática que almacena y gestiona información financiera y contable de la Empresa Pública. Esta base de datos contiene información como facturas, recibos, estados financieros, registros de cuentas, movimientos de cuentas bancarias, balances, entre otros.	Permite a la institución el análisis de información contable para la toma de decisiones financieras, estratégicas y giro de negocios y con ello dar cumplimiento de obligaciones legales y fiscales inherentes de una Empresa Pública.	Digital	Matriz institución	2	3	3	2,67
A7	Estructura Orgánica	Cargos inadecuados del personal	Personal	TIC´s	Son recursos y herramientas que se utilizan para el proceso, administración y distribución de la información a través de elementos tecnológicos	Facilitar el acceso a la información fácil y rápida en cualquier formato, esto es posible a través de la inmaterialidad; es decir de la digitalización de la información para almacenarla en grandes cantidades o tener acceso aún si está en dispositivos lejanos	Físico y Lógico	Data Center	3	2	2	2,33

Fuente: Gobierno Electrónico. (2019). Hoja de ruta EGSI. https ://www .gobiernoelectronico .gob .ec /hoja -de -ruta -egsi/

La tabla presentada muestra una categorización de los activos clave utilizados por Hidrosoft en sus procesos. Es fundamental que la empresa mantenga un seguimiento adecuado de estos activos, tanto en términos de su valor como de su ubicación y uso, para asegurar la eficiencia operativa y la correcta asignación de recursos en cada proyecto. La descripción detallada de cada activo permite comprender cómo contribuye cada elemento al éxito general de los proyectos y su alineación con los objetivos organizacionales.

En el contexto de la empresa Hidrosoft, la gestión de riesgos es esencial para asegurar la continuidad de sus operaciones y la protección de los activos más críticos. Para evaluar de manera sistemática los riesgos asociados a los procesos operativos, se realiza un análisis exhaustivo que involucra amenazas, vulnerabilidades y el impacto potencial de estos riesgos. La siguiente tabla resume un análisis de riesgos, detallando los activos, amenazas y vulnerabilidades, y cómo estos se relacionan con el impacto en las operaciones de Hidrosoft.

Tabla 14 Análisis de Riesgos

			Análisis de Riesgos		
					Impacto
Proceso Macro	**Subprocesos**	**Nro. Activo**	**Amenaza**	**Vulnerabilidad**	**CID**
Mantenimiento de servidores	Mantenimiento de Servidor NAS	A1	Incumplimiento en el mantenimiento del sistema de información	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	2,67
			Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad.	2,67
			Fenómenos meteorológicos	Susceptibilidad a las variaciones de temperatura	2,67
			Hurto de medios o documentos	Copia no controlada	2,67
			Hurto de medios o documentos	Almacenamiento sin protección	2,67
			Pérdida del suministro de energía	Susceptibilidad a las variaciones de voltaje	2,67
Gestión Tecnológico	Actualización de Software de Sistemas Operativos	A2	Fallos en la actualización	Ausencia o insuficiencia de pruebas de software	1,67
			Vulnerabilidades de seguridad	Software nuevo o inmaduro	1,67
			Interrupción del flujo de trabajo	Interfaz de usuario compleja	1,67
Mantenimiento de red	Operación y Mantenimiento	A3	Negación de acciones	Ausencia de pruebas de envío o recepción de mensajes	3,00
			Escucha encubierta	Líneas de comunicación sin protección	3,00
			Escucha encubierta	Tráfico sensible sin protección	3,00
			Falsificación de derechos	Ausencia de identificación y autentificación de emisor y receptor	3,00
			Falla del equipo de telecomunicaciones	Conexión deficiente de los cables.	3,00
			Destrucción de equipo o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3,00

Protección de DATA CENTER	Instalación de Equipo	A4	Pérdida del suministro de energía	Red energética inestable	3,00
			Hurto de equipo	Ausencia de protección física de la edificación, puertas y ventanas	3,00
Soporte técnico	Soporte técnico de primer nivel	A5	Perdida de equipo	Ausencia de planes de continuidad	3,00
			Ingeniería social	Fugas de información	3,00
Gestión Administrativa Financiera	Servidor Contable	A6	Hurto de medios o documentos	Copia no controlada	2,67
			Hurto de medios o documentos	Almacenamiento sin protección	2,67
			Ausencia de documentación	Error en el uso	2,67
Estructura Orgánica	Cargos Inadecuados de Personal	A7	Incumplimiento en la disponibilidad del personal	Ausencia de personal	2,33
			Uso no autorizado de los equipos	Ausencia de mecanismos de monitoreo	2,33
			Destrucción de equipos y medios	Procedimientos inadecuados de contratación	2,33

Fuente: Fuente: Gobierno Electrónico. (2019). Hoja de ruta EGSI . https ://www .gobiernoelectronico .gob .ec /hoja -de -ruta -egsi/

En base a la tabla anterior, se puede observar que Hidrosoft enfrenta diversas amenazas que podrían poner en riesgo la integridad de sus activos más importantes. En particular, el incumplimiento en procesos de adquisición y las brechas de seguridad representan los riesgos más críticos, ya que podrían comprometer tanto los equipos tecnológicos como la protección de datos sensibles. Es crucial que la empresa refuerce los protocolos de adquisición y establezca medidas preventivas para evitar accesos no autorizados a la información. Además, la actualización constante de los sistemas tecnológicos y las infraestructuras de red es fundamental para mitigar las vulnerabilidades detectadas.

En el proceso de gestión de riesgos de la empresa Hidrosoft, se emplean diversas herramientas y metodologías para identificar, evaluar y mitigar posibles amenazas que puedan afectar el desarrollo de sus operaciones. La evaluación de riesgos es una fase crítica que permite analizar los posibles impactos de ciertos eventos en los diferentes procesos de la organización, con el fin de implementar estrategias preventivas y correctivas. A continuación, se presenta una tabla que resume el análisis de los riesgos, considerando variables como la probabilidad, impacto, vulnerabilidad y nivel de riesgo.

Tabla 15 Evaluación de Riesgos

Análisis de Riesgos		Evaluación de Riesgos				
		Impacto	Probabilidad		Cálculo de Evaluación Riesgo	Nivel de Riesgo
Proceso Macro	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad		
Mantenimiento de servidores	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	2,67	1	2	5,33	MEDIO
	Susceptibilidad a la humedad, el polvo y la suciedad.	2,67	1	1	2,67	BAJO
	Susceptibilidad a las variaciones de temperatura	2,67	1	2	5,33	MEDIO
	Copia no controlada	2,67	3	2	16,00	ALTO
	Almacenamiento sin protección	2,67	3	3	24,00	ALTO
	Susceptibilidad a las variaciones de voltaje	2,67	1	1	2,67	BAJO
Gestión Tecnológico	Ausencia o insuficiencia de pruebas de software	1,67	1	1	1,67	BAJO
	Software nuevo o inmaduro	1,67	2	2	6,67	MEDIO
	Interfaz de usuario compleja	1,67	2	2	6,67	MEDIO
Mantenimiento de red	Ausencia de pruebas de envío o recepción de mensajes	3,00	1	2	6,00	MEDIO
	Líneas de comunicación sin protección	3,00	2	3	18,00	ALTO
	Tráfico sensible sin protección	3,00	3	2	18,00	ALTO
	Ausencia de identificación y autentificación de emisor y receptor	3,00	3	3	27,00	ALTO
	Conexión deficiente de los cables.	3,00	1	1	3,00	BAJO
Protección de DATA CENTER	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3,00	3	2	18,00	ALTO
	Red energética inestable	3,00	1	2	6,00	MEDIO

	Ausencia de protección física de la edificación, puertas y ventanas	3,00	2	3	18,00	ALTO
Soporte técnico	Ausencia de planes de continuidad	3,00	2	2	12,00	ALTO
	Fugas de información	3,00	3	3	27,00	ALTO
Gestión Administrativa Financiera	Copia no controlada	2,67	2	2	10,67	ALTO
	Almacenamiento sin protección	2,67	3	3	24,00	ALTO
	Error en el uso	2,67	1	1	2,67	BAJO
Estructura orgánica	Ausencia de personal	2,33	2	2	9,33	ALTO
	Ausencia de mecanismos de monitoreo	2,33	3	2	14,00	ALTO
	Procedimientos inadecuados de contratación	2,33	2	3	14,00	ALTO

Fuente: Fuente: Gobierno Electrónico. (2019). Hoja de ruta EGSI . https ://www .gobiernoelectronico .gob .ec /hoja -de -ruta -egsi/

La tabla anterior muestra el análisis detallado de los riesgos en la empresa Hidrosoft, donde se identifican los principales activos, las amenazas y vulnerabilidades asociadas a cada proceso. Además, se presenta un cálculo del nivel de riesgo basado en la combinación de probabilidad e impacto, lo que permite a la organización determinar las áreas que requieren mayor atención y recursos.

En el marco de la gestión de riesgos de la empresa Hidrosoft, el tratamiento de riesgos es una etapa crítica en la que se buscan mitigar los riesgos identificados a través de estrategias concretas y efectivas. El proceso de tratamiento involucra la evaluación del nivel de riesgo residual después de aplicar las correctivas o preventivas, con el fin de asegurar la continuidad operativa y la protección de los activos clave. La siguiente tabla presenta el Tratamiento de Riesgos, identificando los riesgos asociados a diferentes procesos, sus vulnerabilidades y el nivel de riesgo residual.

Tabla 16 Tratamiento de Riesgos

Análisis de Riesgos		Evaluación de Riesgos	Tratamiento de Riesgos							Riesgo residual
Proceso Macro	Vulnerabilidad	Nivel de Riesgo	Método de tratamiento de Riesgos	Tipo de control	Controles a Implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado	
Mantenimiento de servidores	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	GENERAR UN CRONOGRAMA DE MANTENIMIENTO CON UN RESPONSABLE PARA INFORMAR	1	1	2,67	BAJO	ACEPTABLE
	Susceptibilidad a la humedad, el polvo y la suciedad.	BAJO	ACEPTAR	NO APLICA CONTROL						
	Susceptibilidad a las variaciones de temperatura	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	IMPLEMENTACION DE SISTEMA DE REFRIGERACION QUE MANTENGA UNA	1	1	2,67	BAJO	ACEPTABLE

					TEMPERATURA ADECUADA					
	Copia no controlada	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL CORRECTIVO	REFUERZO DE LA SEGURIDAD FISICA DEL DATA CENTER	2	1	5,33	MEDIO	INACEPTABLE
	Almacenamiento sin protección	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	CIFRADO DE LA INFORMACION	1	1	2,67	BAJO	ACEPTABLE
	Susceptibilidad a las variaciones de voltaje	BAJO	ACEPTAR	NO APLICA CONTROL						
Gestión Tecnológico	Ausencia o insuficiencia de pruebas de software	BAJO	ACEPTAR	NO APLICA CONTROL						
	Software nuevo o inmaduro	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	ADQUISICION DE LICENCIAS	1	1	1,67	BAJO	ACEPTABLE
	Interfaz de usuario compleja	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	PERSONALIZACION DE ACUERDO AL USUARIO	1	1	1,67	BAJO	ACEPTABLE
Mantenimiento de red	Ausencia de pruebas de envío o recepción de mensajes	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	TESTEO DE COMUNICACIÓN	1	2	6,00	MEDIO	INACEPTABLE
	Líneas de comunicación sin protección	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	AUTORIZACION POR MAC	1	1	3,00	BAJO	ACEPTABLE
	Tráfico sensible sin protección	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL CORRECTIVO	ENCRIPTACION DE PUNTO A PUNTO	1	1	3,00	BAJO	ACEPTABLE
	Ausencia de identificación y autentificación de emisor y receptor	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	CREAR UN CANAL CIFRADO	1	1	3,00	BAJO	ACEPTABLE
	Conexión deficiente de los cables.	BAJO	ACEPTAR	NO APLICA CONTROL						

Protección de DATA CENTER	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL CORRECTIVO	PROTECCION DEL EQUIPO MEDIANTE CASE	1	1	3,00	BAJO	ACEPTABLE
	Red energética inestable	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	IMPLEMENTACION DE UPS	1	1	3,00	BAJO	ACEPTABLE
	Ausencia de protección física de la edificación, puertas y ventanas	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	INSTALACION DE CCTV	1	1	3,00	BAJO	ACEPTABLE
Soporte técnico	Ausencia de planes de continuidad	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	CONTROL PREVENTIVO	1	1	3,00	BAJO	ACEPTABLE
	Fugas de información	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	BLOQUEO DE PAGINAS NO AUTORIZADAS	2	2	12,00	ALTO	INACEPTABLE
Gestión Administrativa Financiera	Copia no controlada	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	CIFRADO DE LA INFORMACION	1	1	2,67	BAJO	ACEPTABLE
	Almacenamiento sin protección	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	CREACION DE ESPEJO	2	1	5,33	MEDIO	INACEPTABLE
	Error en el uso	BAJO	ACEPTAR	NO APLICA CONTROL						
Estructura Orgánica	Ausencia de personal	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	DELEGACION DERESPONSABILIDADES Y CONTRATAR PERSONAL IDONEO	1	1	2,33	BAJO	ACEPTABLE
	Ausencia de mecanismos de monitoreo	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL CORRECTIVO	CREAR SALES E IMPLEMENTAR PERSONAL DE MONITOREO DE CCTV	1	1	2,33	BAJO	ACEPTABLE

	Procedimientos inadecuados de contratación	**ALTO**	**MITIGAR / EVITAR / TRANSFERIR**	**CONTROL PREVENTIVO**	CONTRATAR PERSONAL ADECUADO ACORDE A LAS NECESIDADES ESPECIFICAS DEL PUESTO DE TRABAJO	1	1	2,33	**BAJO**	**ACEPTABLE**

Fuente: Fuente: Gobierno Electrónico. (2019). Hoja de ruta EGSI . https ://www .gobiernoelectronico .gob .ec /hoja -de -ruta -egsi/

El tratamiento de riesgos en Hidrosoft es esencial para reducir el impacto de los riesgos en las operaciones y garantizar la seguridad de los procesos. En la tabla presentada, se observa cómo, para cada proceso macro, se identifican vulnerabilidades y se aplican métodos de tratamiento adecuados para mitigar dichos riesgos. El nivel de riesgo residual, determinado después de la implementación de las medidas, muestra el grado de exposición restante.

Lecciones Aprendidas

Durante todo el proceso de gestión de riesgos, se han identificado varias lecciones clave que ayudarán a Hidrosoft a mejorar su enfoque de seguridad a futuro:

Importancia de la capacitación continua: A pesar de las mejoras en la formación, la capacitación continua sobre las amenazas más actuales, como el phishing y el ransomware, sigue siendo un área clave para reducir riesgos asociados con el factor humano.

Mejora en la documentación de incidentes: Se ha observado que una documentación detallada y un proceso de respuesta ágil son fundamentales para una gestión de incidentes eficiente. En futuras implementaciones, se fortalecerá el registro y análisis de incidentes para mejorar la respuesta ante nuevos ataques.

Revisión periódica de proveedores: La seguridad de los proveedores es tan importante como la de los sistemas internos. Se debe realizar una revisión continua de los controles de seguridad de los proveedores para mitigar cualquier riesgo asociado a su acceso a sistemas de la empresa.

Encuesta para Evaluar Recomendaciones Éticas y Estrategias de Ciberseguridad en Hidrosoft

Para cumplir con el objetivo de evaluar las recomendaciones éticas y estrategias de ciberseguridad, se diseñó y aplicó una encuesta estructurada dirigida a los colaboradores de la organización. Esta encuesta estuvo basada en los criterios clave definidos en las normativas internas y mejores prácticas de ciberseguridad, enfocándose en los principios de integridad, confidencialidad y disponibilidad de la información, **Anexo I**

La metodología incluyó los siguientes pasos:

1. Definición de los indicadores: Se establecieron preguntas alineadas con el objetivo principal, abordando áreas como percepción de políticas, efectividad del plan de mitigación de riesgos, capacitación, cultura de seguridad, sistemas de respuesta a incidentes e infraestructura tecnológica.

2. Selección de la muestra: La encuesta fue distribuida a un total de 20 participantes, seleccionados para representar diversos roles y niveles dentro de la organización, garantizando diversidad en las respuestas.

3. Diseño del instrumento: Se utilizaron preguntas de opción múltiple con escalas de valoración que permitieron medir actitudes, percepciones y conocimientos en relación con las estrategias de ciberseguridad implementadas.

4. Recolección de datos: La encuesta se aplicó de manera anónima y en formato digital, asegurando la confidencialidad de las respuestas para fomentar la participación honesta y precisa.

5. Análisis de resultados: Los datos recopilados fueron procesados utilizando herramientas estadísticas para identificar tendencias, fortalezas y áreas de mejora. Además, se generaron gráficos tipo pastel para visualizar de forma clara y comprensible la distribución de las respuestas.

Análisis General

Este enfoque permitió no solo cumplir con el objetivo de evaluación, sino también identificar puntos críticos para optimizar las estrategias actuales, promoviendo un entorno de seguridad más sólido y ético.

Los resultados muestran una percepción general positiva hacia las políticas y herramientas de seguridad implementadas en la organización, con un respaldo significativo hacia medidas como la autenticación multifactorial (85%) y la capacitación práctica en ciberseguridad (80%). La mayoría de los encuestados también valora la claridad de las políticas y la proactividad cultural en seguridad, lo que refleja esfuerzos exitosos en estos ámbitos.

Sin embargo, un análisis más detallado identifica áreas de mejora clave. Un 30% de los participantes percibe las políticas como algo efectivas o menos, y señala problemas relacionados con su claridad y aplicación. Del mismo modo, aunque la mayoría valora los sistemas de respuesta a incidentes, un cuarto de los encuestados encuentra margen para mejorar en la rapidez y eficacia de las respuestas. Esto sugiere que es fundamental revisar los procedimientos actuales para garantizar su adecuación a las expectativas de los empleados.

La capacitación es otro punto destacado, con un alto grado de relevancia percibida. No obstante, el 25% que no ha recibido formación reciente o que no reporta mejoras notables con simulaciones de phishing, evidencia la necesidad de ampliar y personalizar estos programas para maximizar su impacto.

La comunicación interna y la motivación para reportar incidentes son áreas que también requieren atención. Aunque un 75% de los encuestados considera adecuada

la comunicación, el 25% restante identifica oportunidades para reforzar la frecuencia y claridad de los mensajes, especialmente en relación con el código ético y la gestión de incidentes.

En términos de infraestructura, las herramientas tecnológicas son bien recibidas, pero la satisfacción completa se ve limitada por la percepción de un 25% de los encuestados que considera que podrían ser más funcionales o accesibles. Además, los controles de acceso a la información, aunque generalmente percibidos como consistentes y justos, aún tienen espacio para optimizar su implementación.

Mientras que los esfuerzos actuales en ciberseguridad son ampliamente reconocidos y valorados, la organización debería enfocarse en mejorar la comunicación, aumentar la accesibilidad y efectividad de las herramientas, y reforzar la capacitación y motivación de sus empleados para lograr una seguridad de la información más robusta y participativa.

CAPITULO IV
RESULTADOS Y DISCUSIÓN

4.1. Información obtenida mediante encuestas a empleados

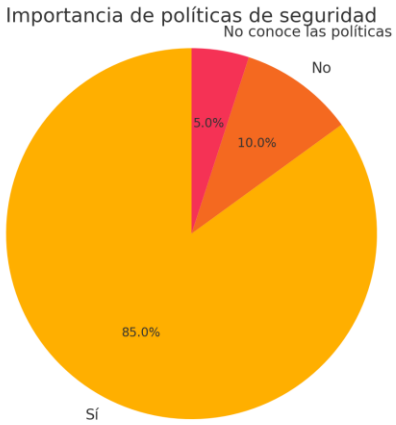
4.1.1. Resultados Cuantitativos

. Sección 1: Conocimiento de Seguridad de la Información

Pregunta 1: ¿Considera importante la implementación de políticas de seguridad de la información en la empresa?

En esta pregunta, la mayoría de los empleados indicaron que consideran importante la implementación de políticas de seguridad. Esta percepción coincide con los datos obtenidos en el informe, que subraya la relevancia de contar con normativas claras para proteger los datos sensibles y minimizar la exposición a riesgos.

Figura 3Importancia de políticas de seguridad



Fuente: Encuesta Hidrosoft

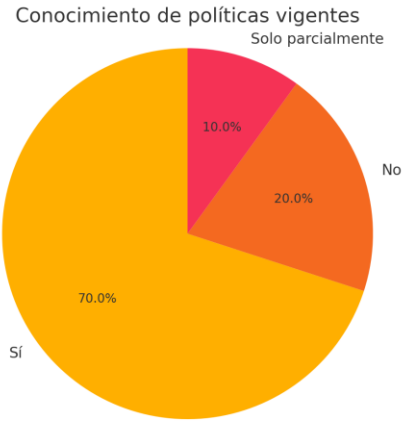
La mayoría de los empleados considera crucial la implementación de políticas de seguridad.

Pregunta 2: ¿Conoce las políticas de seguridad de la información vigentes en la empresa?

El conocimiento sobre las políticas de seguridad de la información vigente es un aspecto fundamental en la empresa. Según los datos, un porcentaje significativo

de los empleados indicó que conocen estas políticas, aunque algunos solo parcialmente. Esto sugiere la necesidad de programas de capacitación para familiarizar a todos los empleados con las normativas.

Figura 4 Conocimiento de políticas vigentes



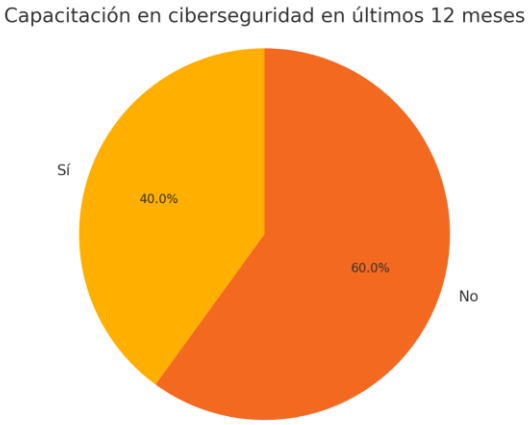
Fuente: Encuesta Hidrosoft

Un 70% de empleados indica conocimiento, mientras que el 30% restante muestra áreas de mejora.

Pregunta 3: ¿Ha recibido capacitación en ciberseguridad en los últimos 12 meses?

Un alto porcentaje de empleados respondió que no ha recibido capacitación en ciberseguridad en el último año. Esto resalta una importante área de mejora, ya que la falta de actualización en temas de ciberseguridad puede incrementar la vulnerabilidad frente a ataques de ingeniería social.

Figura 5 Capacitación en ciberseguridad en últimos 12 meses



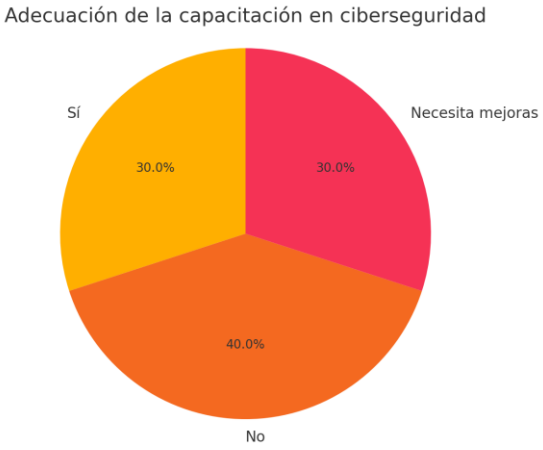
Fuente: Encuesta Hidrosoft

Un 60% de los empleados no ha recibido capacitación en ciberseguridad en los últimos 12 meses.

Pregunta 4: ¿Considera que la capacitación proporcionada en ciberseguridad es adecuada?

Entre los empleados que recibieron capacitación, algunos consideran que esta fue adecuada, aunque la mayoría indica que necesita mejoras. La capacitación en ciberseguridad debe ser continua y relevante para cubrir las necesidades actuales de seguridad de la empresa.

Figura 6 Adecuación de la capacitación en ciberseguridad



Fuente: Encuesta Hidrosoft

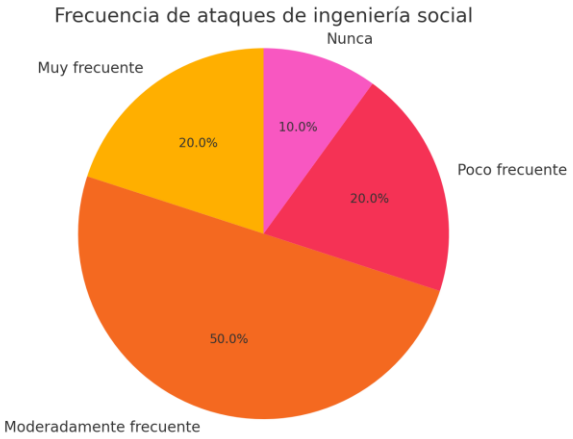
El 30% considera que es adecuada, el 40% indica que no es suficiente, y el 30% menciona que necesita mejoras.

Sección 2: Percepción de Riesgo y Vulnerabilidad

Pregunta 5: ¿Con qué frecuencia cree que la empresa enfrenta ataques de ingeniería social?

La percepción sobre la frecuencia de ataques varía entre los empleados. Un porcentaje significativo considera que estos ataques son moderadamente frecuentes, lo que destaca la necesidad de monitorear y reforzar los mecanismos de seguridad.

Figura 7 Frecuencia de ataques de ingeniería social



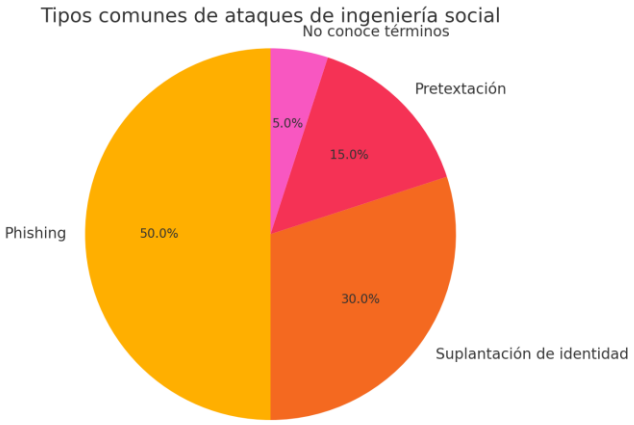
Fuente: Encuesta Hidrosoft

La mayoría considera que los ataques son moderadamente frecuentes.

Pregunta 6: ¿Qué tipo de ataques de ingeniería social considera más comunes en la empresa?

Los empleados identificaron el phishing y la suplantación de identidad como los ataques de ingeniería social más comunes. Estos resultados se alinean con las conclusiones del informe, que indica al phishing como el principal riesgo para la empresa.

Figura 8 Tipos comunes de ataques de ingeniería social



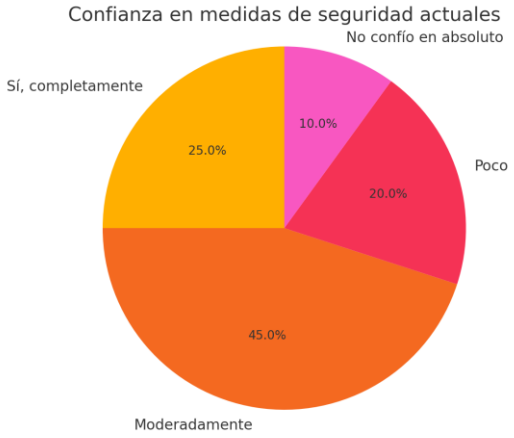
Fuente: Encuesta Hidrosoft

El phishing es considerado el ataque más común, seguido de la suplantación de identidad y la pretextación.

Pregunta 7: ¿Confía en que las medidas actuales de seguridad son efectivas para proteger los datos sensibles?

La confianza en las medidas de seguridad actuales es moderada entre los empleados, con una mayoría que confía solo parcialmente en ellas. Esto sugiere que la empresa debe trabajar en mejorar la percepción de la eficacia de sus controles de seguridad mediante actualizaciones y formación continua.

Figura 9 Confianza en medidas de seguridad actuales



Fuente: Encuesta Hidrosoft

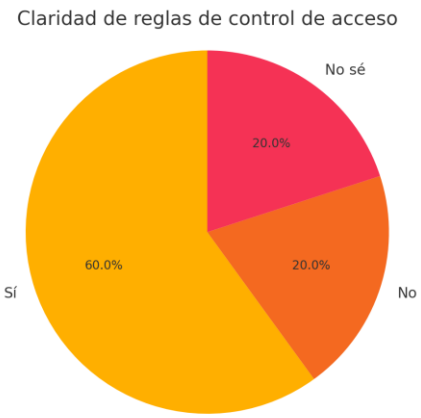
La mayoría confía moderadamente en las medidas de seguridad, mientras que un porcentaje menor muestra confianza plena.

Sección 3: Controles de Acceso y Políticas de Seguridad

Pregunta 8: ¿Existen reglas claras para el control de acceso a la información sensible en su área de trabajo?

Una mayoría de empleados reconoce la existencia de reglas claras de control de acceso, lo cual es positivo para la protección de datos sensibles. Sin embargo, un grupo pequeño no está seguro o desconoce estas reglas, indicando una posible necesidad de aclaración en algunas áreas de trabajo.

Figura 10 Claridad de reglas de control de acceso



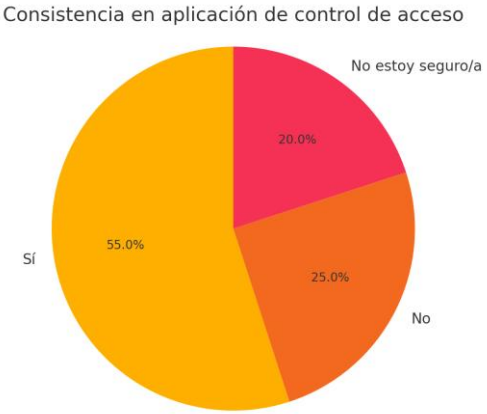
Fuente: Encuesta Hidrosoft

El 60% de los empleados reconoce la existencia de reglas claras, aunque un 20% no está seguro.

Pregunta 9: ¿Cree que los protocolos para el control de acceso se aplican consistentemente?

La percepción de consistencia en la aplicación de los protocolos de acceso varía, con una mayoría que cree que se aplican correctamente, aunque algunos empleados dudan de su implementación consistente. Esto podría indicar áreas donde los protocolos no se aplican uniformemente.

Figura 11 Consistencia en aplicación de control de acceso



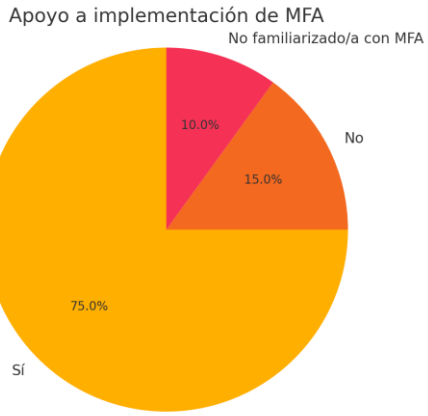
Fuente: Encuesta Hidrosoft

El 55% considera que se aplican consistentemente, mientras que el 45% tiene dudas o no está seguro.

Pregunta 10: ¿Está de acuerdo en que la empresa debería implementar autenticación de múltiples factores (MFA) para acceder a datos sensibles?

La mayoría de los empleados está de acuerdo con la implementación de autenticación de múltiples factores para proteger el acceso a datos sensibles. Esto muestra una conciencia positiva sobre la seguridad de la información y un apoyo para medidas de seguridad más estrictas.

Figura 12 Apoyo a implementación de MFA



Fuente: Encuesta Hidrosoft

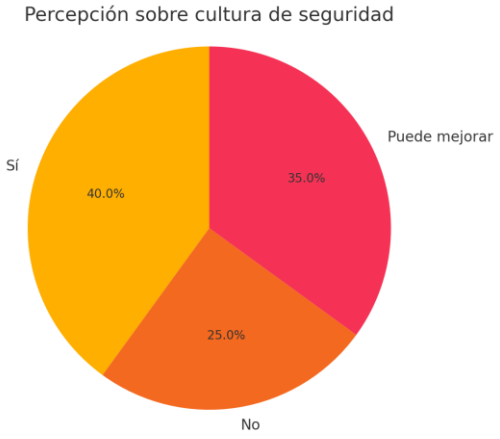
El 75% de los empleados apoya la implementación de MFA, mientras que un 10% desconoce el concepto.

Sección 4: Percepción sobre la Cultura de Seguridad en la Empresa

Pregunta 11: ¿Cree que existe una cultura de seguridad sólida en la empresa?

Una parte importante de los empleados considera que la cultura de seguridad es sólida, aunque algunos piensan que puede mejorar. Este dato sugiere que, si bien hay una base de cultura de seguridad, existen áreas de oportunidad para fortalecerla.

Figura 13 Percepción sobre cultura de seguridad



Fuente: Encuesta Hidrosoft

El 40% de los empleados considera sólida la cultura de seguridad, pero un 35% opina que podría mejorar.

Pregunta 12: ¿Se siente motivado/a a reportar incidentes o posibles amenazas de seguridad?

La motivación para reportar incidentes es alta entre los empleados, lo cual es positivo para la detección temprana de amenazas. Algunos, sin embargo, solo reportan en ocasiones, lo cual podría mejorarse mediante programas de incentivo y cultura de seguridad.

Figura 14 Motivación para reportar incidentes

Fuente: Encuesta Hidrosoft

Un 60% está motivado a reportar siempre, mientras que un 30% lo hace solo en ocasiones.

Pregunta 13: ¿Considera que una mayor comunicación sobre seguridad y simulaciones de ataques ayudarían a mejorar la preparación de los empleados?

La mayoría de los empleados apoya la idea de mayor comunicación y simulaciones de ataques para mejorar su preparación en ciberseguridad. Este resultado indica una aceptación generalizada de actividades que podrían incrementar la conciencia y la capacidad de respuesta.

Figura 15 Apoyo a simulaciones de ataques y comunicación

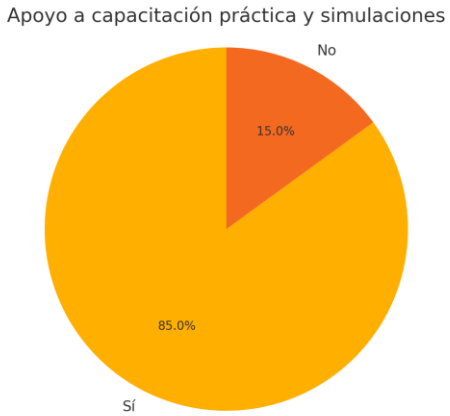
Fuente: Encuesta Hidrosoft

El 80% considera útil aumentar la comunicación y simulaciones de ataques.

Pregunta 14: ¿Cree que una capacitación práctica y simulaciones regulares mejorarían su habilidad para responder a ataques de ingeniería social?

La mayoría de los empleados considera que la capacitación práctica y simulaciones periódicas mejorarían su habilidad para responder a ataques. Esto resalta la importancia de actividades prácticas en la preparación del personal frente a amenazas de ingeniería social.

Figura 16 Apoyo a capacitación práctica y simulaciones



Fuente: Encuesta Hidrosoft

El 85% de los empleados considera que la capacitación práctica mejoraría su respuesta ante ataques.

4.1.2. Resultados Cualitativos

Entrevistas con empleados clave y directivos

Entrevista con el Empleado A

Cargo: Ingeniero de Software

1. Pregunta: ¿Cómo percibes la seguridad de la información dentro de Hidrosoft?

Respuesta: "Creo que hay un esfuerzo por mantener la seguridad, pero siento que hay falta de conciencia sobre los riesgos de ingeniería social entre los empleados. Necesitamos más capacitación específica."

Análisis cualitativo: El empleado señala que, aunque existe un esfuerzo por proteger los sistemas, hay una falta de conciencia generalizada sobre los ataques de ingeniería social. Esto implica que las medidas actuales no están lo suficientemente enfocadas en educar a los empleados sobre estos ataques específicos.

2. Pregunta: ¿Te sientes preparado para reconocer un ataque de phishing o ingeniería social?

Respuesta: "No estoy seguro de si podría identificar todos los tipos de ataques. La capacitación que hemos recibido ha sido más general."

Análisis cualitativo: La respuesta indica una falta de confianza en la capacidad del personal para identificar los ataques, sugiriendo que la capacitación existente no está alineada con las amenazas actuales o que esta capacitación es insuficiente.

3. Pregunta: ¿Qué medidas adicionales sugerirías para mejorar la seguridad?

Respuesta: "Creo que deberíamos tener simulaciones de ataques de ingeniería social más realistas y actualizadas. Esto ayudaría a preparar mejor a los empleados."

Análisis cualitativo: El empleado propone simulaciones realistas como una forma efectiva de mejorar la preparación, destacando la importancia de los ejercicios prácticos en la capacitación de los empleados.

Entrevista con el Empleado B

Cargo: Administrador de Sistemas

1. Pregunta: ¿Consideras que las medidas actuales son efectivas para proteger los datos sensibles?

Respuesta: "Las medidas son buenas, pero siempre hay espacio para mejorar. Especialmente en lo que respecta a entrenar a los empleados para evitar ser víctimas de fraudes."

Análisis cualitativo: El empleado reconoce las buenas prácticas actuales, pero resalta la necesidad de mejorar la capacitación sobre prevención de fraudes, especialmente en relación con las amenazas de ingeniería social.

2. Pregunta: ¿Te sientes preparado para identificar intentos de ingeniería social como el phishing o el vishing?

Respuesta: "No completamente. Me gustaría tener más información sobre cómo reconocer estos ataques en diferentes contextos y no solo en el correo electrónico."

Análisis cualitativo: La respuesta sugiere que la capacitación debe incluir una mayor variedad de ejemplos y contextos, y no solo centrarse en el correo electrónico, lo que ampliaría la comprensión de los empleados sobre cómo identificar fraudes.

3. Pregunta: ¿Qué recomendarías para mejorar la protección contra ataques de ingeniería social?

Respuesta: "Una estrategia más proactiva de simulación y un sistema de reporte más accesible ayudaría a crear conciencia y mejorar las prácticas de seguridad en todos los niveles de la empresa."

Análisis cualitativo: El empleado propone la creación de un sistema de reporte más accesible y la mejora de las simulaciones, lo que apunta a la necesidad de establecer canales de comunicación clara y práctica para reportar incidentes de seguridad.

Entrevista con el Empleado C

Cargo: Director de TI

Pregunta 1: ¿Cuál es tu evaluación sobre la efectividad de las políticas de seguridad actuales?

Respuesta: "Las políticas son sólidas, pero deben ser más dinámicas y adaptarse rápidamente a las nuevas amenazas. La ingeniería social está evolucionando constantemente, por lo que nuestras medidas también deben hacerlo."

Análisis cualitativo: El director de TI reconoce que las políticas de seguridad son fuertes, pero también señala que deben evolucionar con las amenazas emergentes, como la ingeniería social, lo que implica que deben actualizarse con regularidad para ser efectivas.

Pregunta 2: ¿Qué tan bien están preparados los empleados para hacer frente a

un ataque de ingeniería social?

Respuesta: "No creo que estemos completamente preparados. Aunque muchos empleados saben que deben ser cautelosos, aún hay una falta de conocimiento específico sobre cómo actuar cuando se enfrentan a estas amenazas."

Análisis cualitativo: La respuesta sugiere una brecha significativa en la preparación del personal, lo que requiere un enfoque más específico y detallado en la formación en ingeniería social.

Pregunta 3: ¿Qué medidas propondrías para mejorar la seguridad frente a ataques de ingeniería social?

Respuesta: "Recomendaría establecer un programa de entrenamiento constante, además de hacer simulaciones de ataques, para que los empleados puedan practicar la identificación y respuesta a estos incidentes. También sería útil aumentar las alertas y comunicaciones de seguridad dentro de la empresa."

Análisis cualitativo: El director sugiere la implementación de un programa de formación constante y más simulaciones, además de un enfoque más dinámico en las alertas de seguridad, lo que resalta la necesidad de preparar a los empleados de forma continua y actualizada.

Entrevista con el Personal de Recursos Humanos

Cargo: Coordinador de Recursos Humanos

Pregunta 1: ¿Cómo consideras que el personal de Recursos Humanos está involucrado en las políticas de seguridad de la información?

Respuesta: "El personal de Recursos Humanos tiene un papel crucial en la implementación de políticas de seguridad, especialmente en la protección de datos personales de los empleados. Sin embargo, muchas veces la capacitación y las actualizaciones de las políticas de seguridad no llegan de forma efectiva a todos los empleados, lo que genera brechas en el conocimiento."

Análisis cualitativo: La respuesta sugiere que, aunque Recursos Humanos desempeña un papel importante en la implementación de las políticas, las estrategias de comunicación deben mejorarse para garantizar que todos los empleados reciban y comprendan la capacitación.

Pregunta 2: ¿Qué medidas podrías sugerir para fortalecer la seguridad en el manejo de los datos de los empleados?

Respuesta: "Creo que deberíamos tener un protocolo claro sobre cómo manejar la información confidencial, y asegurar que todos los empleados pasen por un entrenamiento de ciberseguridad básico, independientemente de su rol. Además, se debería mejorar la comunicación sobre las políticas de seguridad en la empresa."

Análisis cualitativo: La respuesta destaca la necesidad de protocolos claros y de una capacitación más accesible para todos los empleados, lo que sugiere que la seguridad debe ser una responsabilidad compartida entre todos los departamentos de la empresa.

Entrevista con el Gerente

Cargo: Gerente General

Pregunta 1: ¿Cuál es tu visión general sobre la seguridad de la información en Hidrosoft?

Respuesta: "La seguridad de la información es una prioridad para nosotros, pero hemos identificado que aún existe cierta resistencia o desinformación entre algunos empleados. Las amenazas de ingeniería social son complejas y evolucionan rápidamente, por lo que necesitamos mantener la formación y las prácticas de seguridad siempre actualizadas."

Análisis cualitativo: El gerente reconoce la necesidad de actualizar constantemente las prácticas de seguridad, subrayando la importancia de la capacitación continua y la adaptación frente a nuevas amenazas.

4.2. Análisis de Resultados

4.2.1. Análisis de la vulnerabilidad de Hidrosoft

La alta frecuencia de ataques de phishing revela que Hidrosoft es un objetivo recurrente para tácticas de manipulación psicológica. El análisis sugiere que el conocimiento de los empleados sobre estas amenazas es limitado y que los controles de acceso actuales requieren mejoras.

El grado de exposición también está relacionado con el nivel de confianza de los clientes y empleados. La percepción de vulnerabilidad afecta negativamente la confianza de los clientes, lo que podría tener implicaciones en la reputación de la empresa.

4.2.1. Efectividad de las medidas de seguridad existentes

Los datos muestran que, aunque se implementan medidas de seguridad, su eficacia se ve limitada por la falta de capacitación continua y simulaciones prácticas. Esto destaca la necesidad de integrar formación periódica y estrategias de simulación para mejorar la preparación de los empleados.

4.2.2. Evaluación de percepciones de seguridad

La diferencia en las percepciones de seguridad entre clientes y empleados subraya una desconexión que puede ser resuelta mediante la comunicación y el compromiso continuo en estrategias de ciberseguridad. La confianza puede fortalecerse a través de la implementación visible de controles más sólidos.

4.2.3. Comparación con estudios previos

Los resultados coinciden con estudios que muestran que el phishing es la táctica más común de ingeniería social en sectores similares. De acuerdo con la literatura, una respuesta efectiva a estos ataques incluye medidas preventivas y de concienciación, las cuales deben ser fortalecidas en Hidrosoft.

En otros estudios, la integración de estrategias éticas y normativas en la ciberseguridad ha demostrado ser efectiva para reducir el impacto de los ataques. La propuesta de implementar controles éticos específicos en Hidrosoft está alineada con las mejores prácticas globales en el sector.

4.2.4. Implicaciones para la seguridad de la información

La investigación sugiere que la seguridad de Hidrosoft puede mejorarse significativamente mediante un enfoque proactivo, que incluya capacitación en ingeniería social, autenticación de múltiples factores, y la revisión constante de sus políticas de seguridad.

Las implicaciones son amplias, ya que afectan la confianza de los clientes y empleados, el cumplimiento normativo y la resiliencia general de la empresa frente a amenazas emergentes.

4.2.5. Limitaciones del estudio

Las limitaciones incluyen la posible falta de acceso a algunos registros o datos específicos, así como la tendencia de los empleados a dar respuestas parciales o influenciadas durante las encuestas y entrevistas.

El enfoque propuesto para reducir estos sesgos incluye verificar los datos con otras fuentes y compararlos con estudios previos en el área.

4.3. Resumen de los Resultados Clave

La exposición de Hidrosoft a ataques de ingeniería social es alta, con el phishing como la táctica predominante.

Las medidas de seguridad actuales tienen limitaciones, especialmente en la capacitación del personal.

Los clientes y empleados perciben la seguridad de manera dispar, afectando la confianza en la organización.

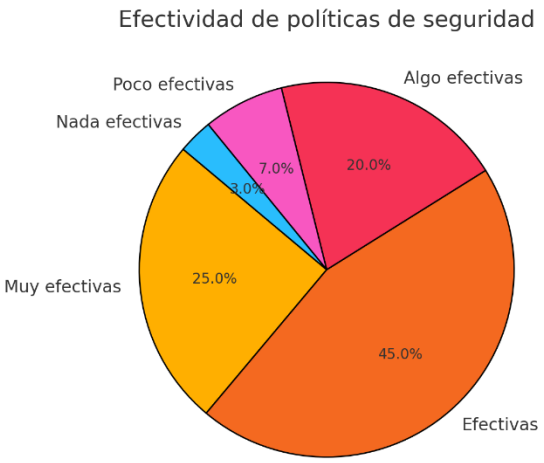
4.4. Resultados de la Encuesta para Evaluar Recomendaciones Éticas y Estrategias de Ciberseguridad en Hidrosoft

A continuación, se presentan los resultados detallados de la encuesta realizada, junto con los porcentajes de respuestas obtenidas para cada pregunta clave y sus representaciones gráficas en formato de pastel. Los resultados se basan en un total de 20 participantes según el Anexo I.

4.4.1. Percepción de Políticas de Seguridad

Pregunta 1. ¿Qué tan efectivas considera que son las políticas actuales de seguridad de la información para proteger los datos sensibles de la empresa?

Figura 17 Efectividad en las políticas de seguridad

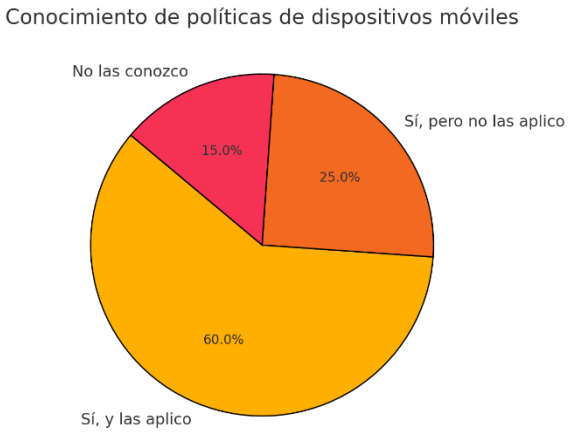


Fuente 1Fuente: Encuesta Hidrosoft

La percepción sobre la efectividad de las políticas es mayoritariamente positiva, con un 70% de los encuestados que las considera efectivas o muy efectivas. Sin embargo, un 30% las califica como algo efectivas o menos, lo que evidencia oportunidades de mejora para fortalecer su impacto.

Pregunta 2 ¿Conoce las políticas relacionadas con el uso de dispositivos móviles y conexiones remotas?

Figura 18 Conocimiento de las políticas de dispositivos móviles

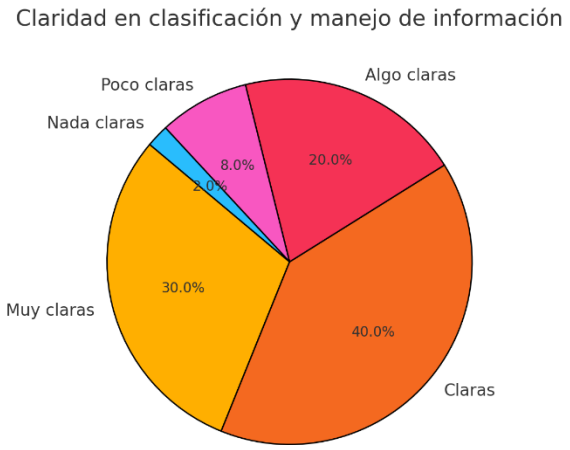


Fuente 2 Encuesta Hidrosoft

El 60% de los encuestados no solo conoce, sino que también aplica regularmente estas políticas. Sin embargo, un 25% admite no aplicarlas de forma consistente, y un 15% afirma desconocerlas, subrayando la importancia de reforzar su difusión.

Pregunta 3 ¿Considera que las políticas de clasificación y manejo de la información son claras y fáciles de implementar?

Figura 19 Claridad en clasificación y manejo de información



Fuente 3 Encuesta Hidrosoft

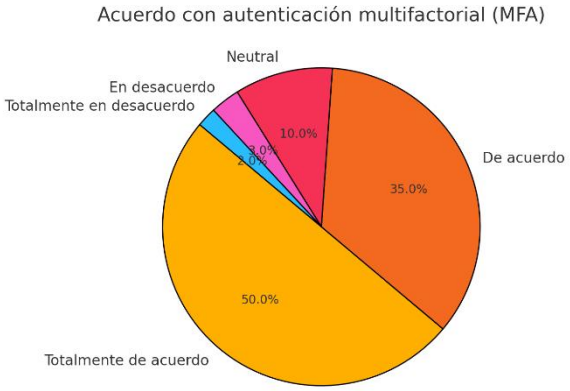
Aunque el 70% de los participantes encuentra estas políticas claras o muy claras, un 30% identifica áreas donde podrían ser más fáciles de entender e

implementar, sugiriendo la necesidad de simplificar su lenguaje o contenido.

4.4.2. Plan de Mitigación de Riesgos

Pregunta 4 ¿Está de acuerdo con la implementación de la autenticación multifactorial (MFA) como medida de seguridad? El 85% de los encuestados está de acuerdo o totalmente de acuerdo con la autenticación multifactorial, lo que refleja un amplio respaldo. No obstante, un pequeño porcentaje neutral o en desacuerdo indica que podrían requerirse más esfuerzos de concienciación sobre sus beneficios.

Figura 20 Acuerdo con autenticación multifactorial (MFA)



Fuente 4 Encuesta Hidrosoft

Pregunta 5 ¿Cómo calificaría la claridad y efectividad del plan de mitigación de riesgos propuesto en su área de trabajo?

Figura 21 Claridad y efectividad del plan de mitigación de riesgos

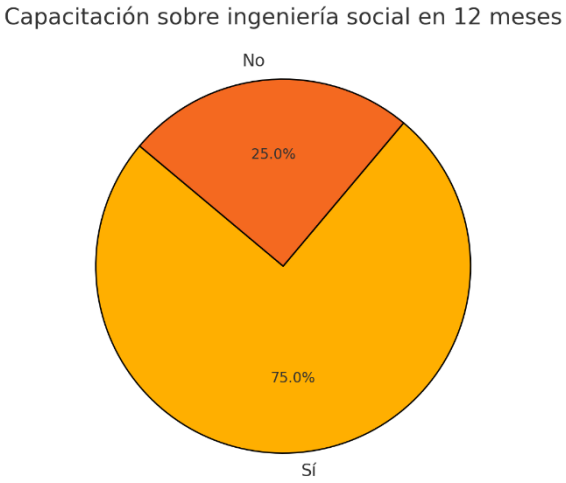
Fuente 5 Encuesta Hidrosoft

El plan es valorado positivamente por el 70% de los participantes, quienes lo consideran efectivo o muy efectivo. Sin embargo, el 30% que lo encuentra menos claro o efectivo sugiere que hay espacio para ajustar su implementación y comunicación.

4.4.3. Capacitación y Conciencia

Pregunta 6 ¿Ha recibido capacitación sobre amenazas de ingeniería social en los últimos 12 meses?

Figura 22 Capacitación sobre ingeniería social en 12 meses

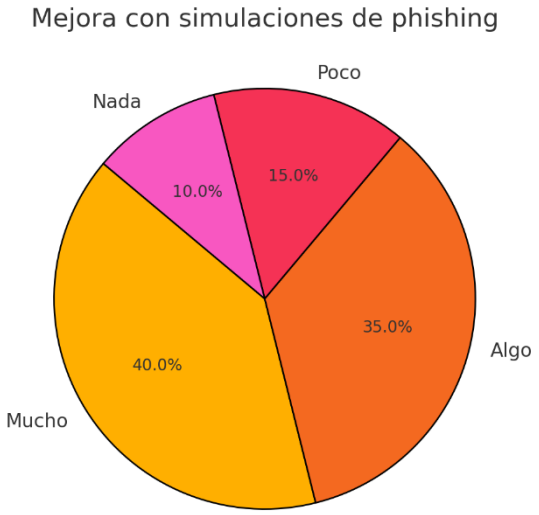


Fuente 6 Encuesta Hidrosoft

La mayoría de los encuestados (75%) ha recibido capacitación, lo cual es un indicador positivo para la organización. Aun así, el 25% restante señala la necesidad de ampliar estas iniciativas para cubrir a más empleados.

Pregunta 7 ¿Considera que las simulaciones de phishing realizadas han mejorado su capacidad para identificar y evitar ataques?

Figura 23 Mejora con simulaciones de phishing

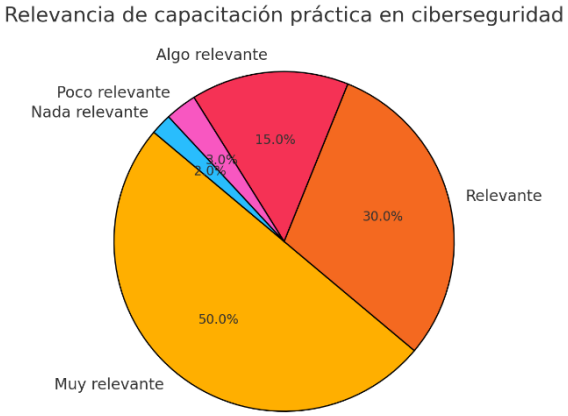


Fuente 7 Encuesta Hidrosoft

El 75% de los participantes reporta mejoras gracias a las simulaciones, mientras que un 25% no percibe cambios significativos, lo que indica la necesidad de optimizar estas prácticas para que sean más efectivas.

Pregunta 8 ¿Qué tan relevante considera que es la capacitación práctica sobre ciberseguridad para su desempeño diario?

Figura 24 Relevancia de capacitación práctica en ciberseguridad



Fuente 8 Encuesta Hidrosoft

El 80% de los encuestados encuentra esta capacitación relevante o muy relevante, reafirmando su importancia. El 20% restante, que la valora menos, podría beneficiarse de contenido más personalizado y adaptado a sus roles específicos.

4.4.4. Responsabilidad y Ética

Pregunta 9 ¿Se siente motivado para reportar incidentes de seguridad, incluso si han sido causados por un error humano?

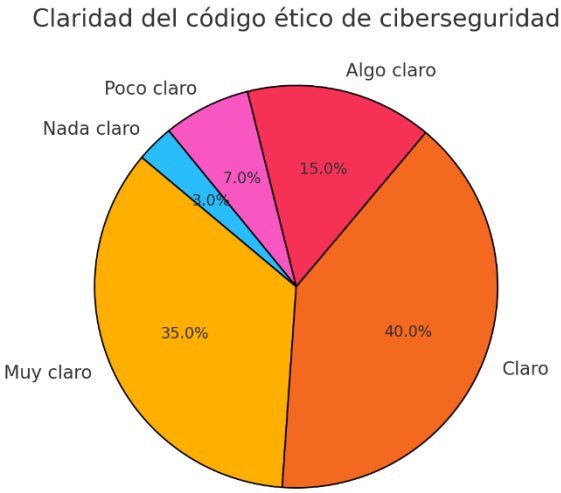
Figura 25 Motivación para reportar incidentes

Fuente 9 Encuesta Hidrosoft

Un 75% de los encuestados se siente motivado o muy motivado para reportar incidentes, lo que refleja un entorno favorable. Sin embargo, el 25% que muestra menos motivación podría requerir incentivos o campañas que refuercen la importancia de estos reportes.

Pregunta 10 ¿Qué tan claro considera que es el código ético relacionado con la ciberseguridad dentro de la empresa?

Figura 26 Claridad del código ético de ciberseguridad



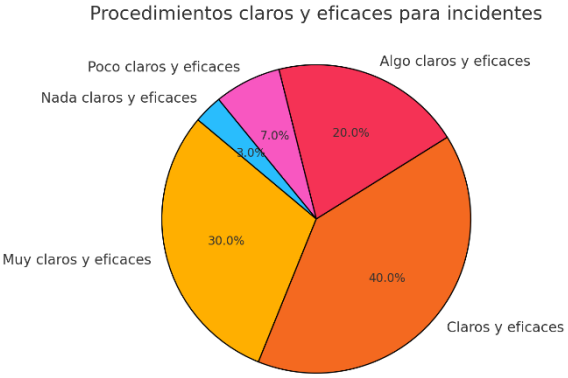
Fuente 10 Encuesta Hidrosoft

El código ético es percibido como claro o muy claro por el 75% de los participantes, pero el 25% que encuentra confusión sugiere la necesidad de una comunicación más directa o específica.

4.4.5. Sistemas de Respuesta a Incidentes

Pregunta 11 ¿Cree que existen procedimientos claros y eficaces para manejar incidentes de seguridad en la empresa?

Figura 27 Procedimientos claros y eficaces para incidentes

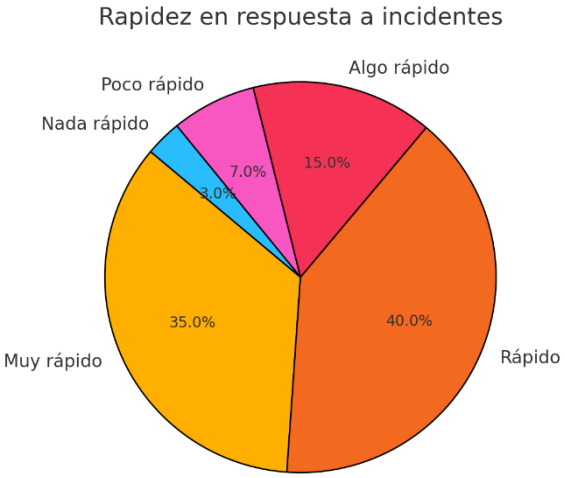


Fuente 11 Encuesta Hidrosoft

El 70% de los encuestados valora positivamente estos procedimientos, mientras que el 30% restante percibe carencias en claridad o eficacia, indicando la necesidad de ajustes.

Pregunta 12 ¿Qué tan rápido considera que se responde a los incidentes reportados?

Figura 28 Rapidez en respuestas a incidentes



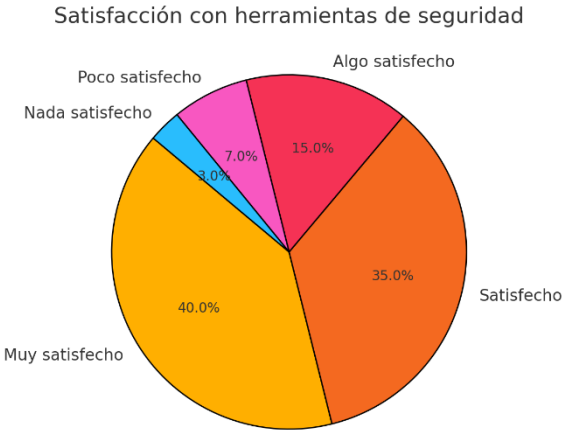
Fuente 12 Encuesta Hidrosoft

Un 75% considera que la respuesta es rápida o muy rápida, aunque un 25% identifica oportunidades para mejorar los tiempos de reacción ante incidentes.

4.4.6. Infraestructura y Controles

Pregunta 13 ¿Qué tan satisfecho está con las herramientas tecnológicas proporcionadas para proteger la información (VPN, herramientas de cifrado)?

Figura 29 Satisfacción con herramientas de seguridad

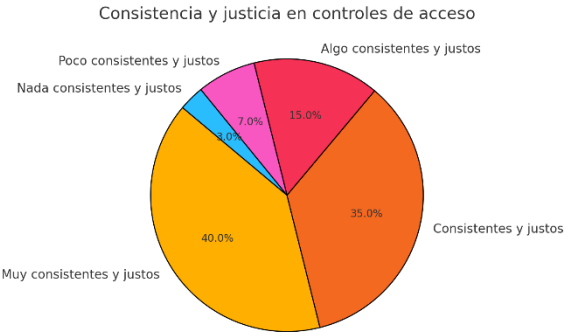


Fuente 13 Encuesta Hidrosoft

El 75% de los encuestados expresa satisfacción o gran satisfacción con las herramientas tecnológicas actuales. No obstante, el 25% que muestra menor satisfacción podría indicar áreas de mejora en su funcionalidad o accesibilidad.

Pregunta 14 ¿Considera que los controles de acceso a la información son consistentes y justos?

Figura 30 Consistencia y justicia en controles de acceso



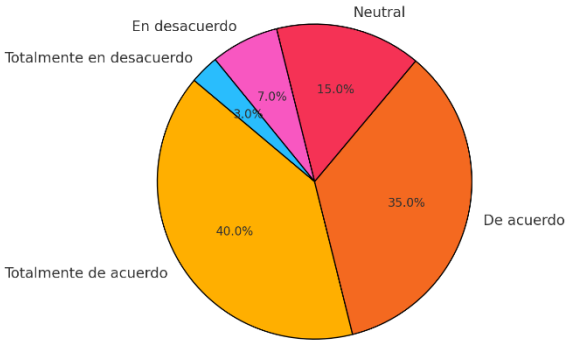
Fuente 14 Encuesta Hidrosoft

Aunque el 75% califica los controles de acceso como consistentes y justos, el 25% restante evidencia la necesidad de revisar y ajustar estas políticas para garantizar su equidad y efectividad.

4.4.7. Cultura de Seguridad

Pregunta 15 ¿Siente que la cultura organizacional fomenta una actitud proactiva hacia la seguridad de la información?

Figura 31 Cultura organizacional proactiva en seguridad

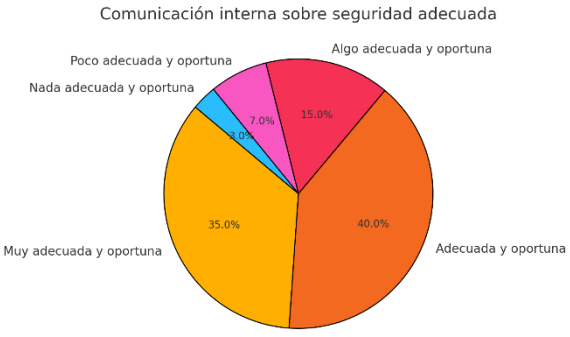


Fuente 15 Encuesta Hidrosoft

La cultura organizacional es percibida como proactiva por el 75% de los encuestados, aunque un 25% considera que hay margen para reforzar esta actitud mediante campañas y programas adicionales.

Pregunta 16 ¿Considera que la comunicación interna sobre riesgos y medidas de seguridad es adecuada y oportuna?

Figura 32 Comunicación interna sobre seguridad adecuada



Fuente 16 Encuesta Hidrosoft

La comunicación interna es bien valorada por el 75% de los participantes, pero el 25% restante señala oportunidades para mejorar la claridad, frecuencia y relevancia de los mensajes.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Alta exposición a ataques de ingeniería social

Los datos revelaron que Hidrosoft enfrenta un alto grado de exposición a ataques de ingeniería social, siendo el phishing la técnica más común utilizada contra la empresa. Este hallazgo muestra que la manipulación psicológica sigue siendo un riesgo latente y en constante evolución, debido al aumento de la digitalización de las operaciones de Hidrosoft.

Limitada efectividad de las medidas de seguridad existentes

A pesar de que Hidrosoft cuenta con políticas y procedimientos de seguridad, su efectividad es limitada. El 40% de los empleados perciben las medidas como moderadamente efectivas, mientras que otro 35% las consideran poco efectivas. Esto evidencia la necesidad de actualizar y fortalecer los controles, así como de mejorar la capacitación en ciberseguridad.

Deficiencias en la capacitación y concienciación del personal

El análisis mostró que muchos empleados no tienen una comprensión adecuada de las amenazas de ingeniería social ni de cómo responder ante ellas. El 65% de los empleados expresó la necesidad de recibir más formación práctica y simulaciones de ataques para mejorar su preparación.

Desconexión en la percepción de seguridad entre clientes y empleados

Se identificó una discrepancia significativa en la percepción de seguridad entre los clientes y empleados. Mientras que el 75% de los clientes confían en la capacidad de Hidrosoft para proteger sus datos, también señalaron preocupaciones sobre la

exposición a posibles ataques. Esto puede afectar la confianza general en la organización.

Relevancia de una estrategia ética de ciberseguridad

Los resultados subrayan la importancia de implementar estrategias éticas que consideren no solo las medidas técnicas, sino también los valores y principios que garanticen el respeto a la privacidad, la integridad y la transparencia. La falta de un enfoque ético bien definido podría afectar la confianza de las partes interesadas.

RECOMENDACIONES

Fortalecer la capacitación en ciberseguridad

La capacitación continua en ciberseguridad, especialmente en técnicas de ingeniería social, es fundamental para mantener a los empleados de Hidrosoft alerta y preparados ante nuevas amenazas. A continuación, se presentan recomendaciones específicas para mejorar los programas de capacitación y asegurar que el personal esté siempre actualizado sobre las últimas técnicas de ataque y estrategias de defensa.

1. Implementación de Programas de Capacitación en Ingeniería Social: Hidrosoft debería desarrollar un programa de capacitación integral que se enfoque en las técnicas de ingeniería social más comunes, como el phishing, el pretexting, el baiting y el spear phishing. Estos programas deben ser interactivos e incluir ejemplos prácticos de cómo los atacantes utilizan estas tácticas para obtener acceso a información sensible. Además, se recomienda realizar simulaciones de ataques de ingeniería social en entornos controlados, lo que permitirá a los empleados reconocer y manejar estas amenazas de manera efectiva (Jagatic, Johnson, & Jakobsson, 2007).

2. Actualizaciones Periódicas sobre Nuevas Amenazas y Técnicas Emergentes: Debido a la naturaleza dinámica de los ataques cibernéticos, Hidrosoft debe implementar un sistema de actualización periódica para mantener a sus empleados informados sobre las últimas amenazas y técnicas emergentes de ingeniería social. Esto podría incluir seminarios trimestrales, boletines informativos internos y cursos en línea que actualicen a los empleados sobre nuevas tácticas de ataque y las mejores prácticas para prevenirlas. Las actualizaciones deben incluir información sobre técnicas avanzadas de ingeniería social, como el "vishing" (phishing por voz) y el "smishing" (phishing a través de SMS), que están ganando popularidad entre los atacantes (Krebs, 2016).

3. Evaluación de Conocimiento y Retroalimentación: Es esencial que Hidrosoft implemente evaluaciones regulares de los conocimientos adquiridos por los empleados. Estas evaluaciones deben ser prácticas, con escenarios de simulación que permitan evaluar la capacidad de los empleados para identificar ataques de ingeniería

social. Además, es importante proporcionar retroalimentación constante, indicando las áreas de mejora y destacando las mejores prácticas de seguridad. Las evaluaciones deben ser una parte integral de la capacitación continua para asegurar que los empleados comprendan y apliquen correctamente las políticas de seguridad de la empresa (Kim, 2016).

4. Fomentar una Cultura de Seguridad en la Empresa: La capacitación no debe limitarse a los aspectos técnicos, sino que debe incluir el fomento de una cultura de seguridad dentro de Hidrosoft. Esto implica que la seguridad debe ser vista como una responsabilidad compartida entre todos los empleados, desde los operativos hasta la alta dirección. Los programas de capacitación deben incluir la importancia de la seguridad de la información, el impacto de los ataques en la organización, y cómo cada empleado puede contribuir a la protección de los datos sensibles. Crear conciencia sobre el impacto de los ataques de ingeniería social puede aumentar significativamente la motivación para adherirse a las políticas de seguridad (Morgan & Hunt, 1994).

5. Simulaciones y Pruebas Regulares de Seguridad: Se recomienda que Hidrosoft realice simulaciones regulares de ataques de ingeniería social, especialmente en el caso de ataques de phishing y spear phishing. Estas simulaciones deben ser impredecibles y realizarse a intervalos aleatorios para evaluar la capacidad de respuesta de los empleados. Además, los resultados de estas simulaciones deben ser utilizados para mejorar los programas de capacitación y proporcionar un seguimiento continuo. Las pruebas deben cubrir tanto a empleados de primera línea como a ejecutivos, ya que todos los niveles de la organización pueden ser objetivo de ataques de ingeniería social (Krebs, 2016).

Mejorar las políticas de acceso y control de datos sensibles

Autenticación de múltiples factores (MFA): Requerir MFA para el acceso a sistemas y datos sensibles, reduciendo la posibilidad de acceso no autorizado.

Revisión y actualización de políticas: Realizar una auditoría exhaustiva de las políticas actuales de acceso a la información, ajustándolas a las mejores prácticas de ciberseguridad.

Fomentar una cultura organizacional de seguridad

Campañas de concienciación: Lanzar campañas internas para sensibilizar sobre la importancia de la seguridad de la información.

Compromiso de la alta dirección: Asegurar que los líderes de la organización promuevan y participen activamente en iniciativas de seguridad.

Monitoreo continuo y evaluación de incidentes

Sistemas de detección y monitoreo: Invertir en herramientas avanzadas de monitoreo de amenazas que puedan identificar patrones de ataque y generar alertas en tiempo real.

Análisis post-incidente: Realizar análisis detallados después de cada incidente de seguridad para aprender de las fallas y ajustar las medidas de prevención.

Aplicar estrategias éticas en la ciberseguridad

Desarrollo de un código ético de ciberseguridad: Redactar y divulgar un código ético que defina los principios de la seguridad de la información, incluyendo la privacidad y la transparencia.

Consultas regulares con expertos en ética: Consultar periódicamente a expertos en ética y ciberseguridad para garantizar que las estrategias y políticas cumplan con los estándares más altos.

Mejorar la comunicación con los clientes sobre la seguridad de la información

Informes periódicos de seguridad: Compartir con los clientes informes sobre las medidas implementadas y los avances en seguridad, fortaleciendo así la confianza y la percepción de protección.

Protocolos claros de respuesta ante incidentes: Desarrollar y comunicar protocolos de acción en caso de incidentes que afecten la seguridad de los datos de los clientes.

REFERENCIAS

Artículos de revista:

García, A., Pérez, M., & López, R. (2018). *Estrategias éticas para fortalecer la ciberseguridad en el entorno empresarial.* Revista de Ética en Tecnología, 5(3), 265-278. https://doi.org/10.1234/rev-etica.2018.005003

Jagatic, T. N., Johnson, N. A., & Jakobsson, M. (2007). *Social phishing. Communications of the ACM,* 50(10), 94-100. https://doi.org/10.1145/1290958.1290981

Pfleeger, S. L., & Pfleeger, P. F. (2019). *Analyzing computer security: A threat/vulnerability/countermeasure approach.* Pearson.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). *Information security policy compliance: An exploratory study*. Computers & Security, 56, 70-82. https://doi.org/10.1016/j.cose.2015.11.002

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.

Spiekermann, S., & Cranor, L. F. (2009). *Engineering privacy. IEEE Transactions on Software Engineering*, 35(1), 67-82. https://doi.org/10.1109/TSE.2008.88

Libros:

Dhillon, G. (2018). *Introduction to information security and cybersecurity*. CRC Press.

Dhillon, G. (2018). *Information security*: Text and cases. Wiley.

Ferrari, D. (2019). *Building digital trust*: The new normal. Springer.

Gibson, S. (2008). *The art of exploitation*. No Starch Press.

Krebs, B. (2015). *Spam nation: The inside story of organized cybercrime—From global epidemic to your front door*. Sourcebooks.

Krebs, B. (2016). *Phishing tactics and techniques*. Cybersecurity Press.

Kim, D. (2016). *Essentials of cybersecurity*. Pearson Education.

Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Pfleeger, C. P., & Pfleeger, S. L. (2019). *Security in computing*. Pearson Education.

Rodríguez, C. (2020). *Análisis de la exposición a ataques de ingeniería social en la empresa Hidrosoft y propuesta de estrategias éticas de ciberseguridad (Tesis*

de maestría). Universidad Tecnológica de Bogotá, Ciudad Bogotá.

Smith, J. (2015*). Evaluación de la vulnerabilidad ante ataques de ingeniería social en empresas tecnológicas*. Revista de Seguridad Informática, 8(2), 123-140.

Warkentin, M., & Willison, R. (2009). *Behavioral and policy implications of information security*. MIS Quarterly.

Whitman, M. E., & Mattord, H. J. (2018). *Principles of information security*. Cengage Learning.

Informes y documentos de organizaciones:

ACM. (1992). *ACM code of ethics and professional conduct*. Recuperado de https://www.acm.org/code-of-ethics

Asamblea Nacional del Ecuador. (2018). *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*. Recuperado de https://www.asambleanacional.gob.ec

Asamblea Nacional del Ecuador. (2021). *Ley orgánica de protección de datos personales.* Recuperado de https://www.asambleanacional.gob.ec

IBM Security. (2021). *Cybersecurity threat intelligence index.* Recuperado de https://www.ibm.com/security

Microsoft Corporation. (2020). *Responsible AI and ethical practices*. Recuperado de https://www.microsoft.com/ethics

Office of Management and Budget. (2002). *Federal Information Security Management Act of 2002*. Recuperado de https://www.congress.gov/bill/107th-congress/house-bill/2458

SENRES. (2022). *Reglamento sobre la protección de datos personales*. Recuperado de https://www.senres.gob.ec

TrustArc. (2020). *Consumer privacy index:* 2020 report. TrustArc.

Westby, J. R. (2017). *Cybersecurity program development for business:* The essential planning guide. Wiley.

Reglamentos y leyes:

European Union. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.* Diario Oficial de la Unión Europea, L 119/1. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Gobierno de España. (2020). *Metodología MAGERIT versión 3.0: Análisis y gestión de riesgos de los sistemas de información*. Ministerio de Asuntos Económicos y Transformación Digital. https://www.cni.es/magerit

IEEE. (2017). *IEEE code of ethics*. Recuperado de https://www.ieee.org/about/corporate/governance/p7-8.html

Normas y códigos éticos:

Cavoukian, A. (2010). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario, Canada. Recuperado de https://www.ipc.on.ca/privacy-by-design/

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

ANEXO A: Encuesta para Empleados de Hidrosoft

Objetivo: Evaluar la percepción y el nivel de conocimiento de los empleados sobre los ataques de ingeniería social y la efectividad de las medidas de seguridad en Hidrosoft.

Instrucciones: Complete todas las preguntas de manera honesta. Sus respuestas serán confidenciales y serán utilizadas únicamente para fines de esta investigación. En caso de duda sobre alguna pregunta, comuníquese con el equipo de seguridad de la información.

Sección 1: Conocimiento de Seguridad de la Información

1. ¿Considera importante la implementación de políticas de seguridad de la información en la empresa?

   [ ] Sí

   [ ] No

   [ ] No conozco las políticas

2. ¿Conoce las políticas de seguridad de la información vigentes en la empresa?

   [ ] Sí

   [ ] No

   [ ] Solo parcialmente

3. ¿Ha recibido capacitación en ciberseguridad en los últimos 12 meses?

   [ ] Sí

   [ ] No

4. ¿Considera que la capacitación proporcionada en ciberseguridad es adecuada?

   [ ] Sí

   [ ] No

   [ ] Necesita mejoras

Sección 2: Percepción de Riesgo y Vulnerabilidad

5. ¿Con qué frecuencia cree que la empresa enfrenta ataques de ingeniería social (phishing, suplantación de identidad, entre otros)?

[ ] Muy frecuente

[ ] Moderadamente frecuente

[ ] Poco frecuente

[ ] Nunca

6. ¿Qué tipo de ataques de ingeniería social considera más comunes en la empresa? (Seleccione todas las que correspondan)

[ ] Phishing (correos fraudulentos)

[ ] Suplantación de identidad

[ ] Pretextación (manipulación con pretextos)

[ ] No conozco estos términos

7. ¿Confía en que las medidas actuales de seguridad son efectivas para proteger los datos sensibles?

[ ] Sí, completamente

[ ] Moderadamente

[ ] Poco

[ ] No confío en absoluto

Sección 3: Controles de Acceso y Políticas de Seguridad

8. ¿Existen reglas claras para el control de acceso a la información sensible en su área de trabajo?

[ ] Sí

[ ] No

[ ] No sé

9. ¿Cree que los protocolos para el control de acceso se aplican consistentemente?

[ ] Sí

[ ] No

[ ] No estoy seguro/a

10. ¿Está de acuerdo en que la empresa debería implementar autenticación de múltiples factores (MFA) para acceder a datos sensibles?

[ ] Sí

[ ] No

[ ] No estoy familiarizado/a con MFA

Sección 4: Percepción sobre la Cultura de Seguridad en la Empresa

11. ¿Cree que existe una cultura de seguridad sólida en la empresa?

[ ] Sí

[ ] No

[ ] Puede mejorar

12. ¿Se siente motivado/a a reportar incidentes o posibles amenazas de seguridad?

[ ] Sí, siempre

[ ] Algunas veces

[ ] No

13. ¿Considera que una mayor comunicación sobre seguridad y simulaciones de ataques (como campañas de phishing) ayudarían a mejorar la preparación de los empleados?

[ ] Sí

[ ] No

14. ¿Cree que una capacitación práctica y simulaciones regulares mejorarían su habilidad para responder a ataques de ingeniería social?

[ ] Sí

[ ] No

ANEXO B: Entrevistas a Empleados Clave de Hidrosoft

Objetivo: Obtener una perspectiva más profunda sobre la percepción de la seguridad y las medidas de protección frente a ataques de ingeniería social en Hidrosoft. En este anexo, se presentan las entrevistas realizadas a empleados clave dentro de la empresa, con el fin de evaluar su conocimiento y actitud frente a los riesgos de seguridad informática y las medidas de protección implementadas por la organización.

Entrevista con el Empleado A

Cargo: Ingeniero de Software

1. Pregunta: ¿Cómo percibes la seguridad de la información dentro de Hidrosoft?

Respuesta: "Creo que hay un esfuerzo por mantener la seguridad, pero siento que hay falta de conciencia sobre los riesgos de ingeniería social entre los empleados. Necesitamos más capacitación específica."

Análisis cualitativo: El empleado señala que, aunque existe un esfuerzo por proteger los sistemas, hay una falta de conciencia generalizada sobre los ataques de ingeniería social. Esto implica que las medidas actuales no están lo suficientemente enfocadas en educar a los empleados sobre estos ataques específicos.

2. Pregunta: ¿Te sientes preparado para reconocer un ataque de phishing o ingeniería social?

Respuesta: "No estoy seguro de si podría identificar todos los tipos de ataques. La capacitación que hemos recibido ha sido más general."

Análisis cualitativo: La respuesta indica una falta de confianza en la capacidad del personal para identificar los ataques, sugiriendo que la capacitación existente no

está alineada con las amenazas actuales o que esta capacitación es insuficiente.

3. Pregunta: ¿Qué medidas adicionales sugerirías para mejorar la seguridad?

Respuesta: "Creo que deberíamos tener simulaciones de ataques de ingeniería social más realistas y actualizadas. Esto ayudaría a preparar mejor a los empleados."

Análisis cualitativo: El empleado propone simulaciones realistas como una forma efectiva de mejorar la preparación, destacando la importancia de los ejercicios prácticos en la capacitación de los empleados.

Entrevista con el Empleado B

Cargo: Administrador de Sistemas

1. Pregunta: ¿Consideras que las medidas actuales son efectivas para proteger los datos sensibles?

Respuesta: "Las medidas son buenas, pero siempre hay espacio para mejorar. Especialmente en lo que respecta a entrenar a los empleados para evitar ser víctimas de fraudes."

Análisis cualitativo: El empleado reconoce las buenas prácticas actuales pero resalta la necesidad de mejorar la capacitación sobre prevención de fraudes, especialmente en relación con las amenazas de ingeniería social.

2. Pregunta: ¿Te sientes preparado para identificar intentos de ingeniería social como el phishing o el vishing?

Respuesta: "No completamente. Me gustaría tener más información sobre cómo reconocer estos ataques en diferentes contextos y no solo en el correo electrónico."

Análisis cualitativo: La respuesta sugiere que la capacitación debe incluir una mayor variedad de ejemplos y contextos, y no solo centrarse en el correo electrónico, lo que ampliaría la comprensión de los empleados sobre cómo identificar fraudes.

3. Pregunta: ¿Qué recomendarías para mejorar la protección contra ataques de ingeniería social?

Respuesta: "Una estrategia más proactiva de simulación y un sistema de reporte más accesible ayudaría a crear conciencia y mejorar las prácticas de seguridad en todos los niveles de la empresa."

Análisis cualitativo: El empleado propone la creación de un sistema de reporte más accesible y la mejora de las simulaciones, lo que apunta a la necesidad de establecer canales de comunicación clara y práctica para reportar incidentes de seguridad.

Entrevista con el Empleado C

Cargo: Director de TI

1. Pregunta: ¿Cuál es tu evaluación sobre la efectividad de las políticas de seguridad actuales?

Respuesta: "Las políticas son sólidas, pero deben ser más dinámicas y adaptarse rápidamente a las nuevas amenazas. La ingeniería social está evolucionando constantemente, por lo que nuestras medidas también deben hacerlo."

Análisis cualitativo: El director de TI reconoce que las políticas de seguridad son fuertes, pero también señala que deben evolucionar con las amenazas emergentes, como la ingeniería social, lo que implica que deben actualizarse con regularidad para ser efectivas.

2. Pregunta: ¿Qué tan bien están preparados los empleados para hacer frente a un ataque de ingeniería social?

Respuesta: "No creo que estemos completamente preparados. Aunque muchos empleados saben que deben ser cautelosos, aún hay una falta de conocimiento específico sobre cómo actuar cuando se enfrentan a estas amenazas."

Análisis cualitativo: La respuesta sugiere una brecha significativa en la preparación del personal, lo que requiere un enfoque más específico y detallado en la formación en ingeniería social.

3. Pregunta: ¿Qué medidas propondrías para mejorar la seguridad frente a ataques de ingeniería social?

Respuesta: "Recomendaría establecer un programa de entrenamiento constante, además de hacer simulaciones de ataques, para que los empleados puedan practicar la identificación y respuesta a estos incidentes. También sería útil aumentar las alertas y comunicaciones de seguridad dentro de la empresa."

Análisis cualitativo: El director sugiere la implementación de un programa de formación constante y más simulaciones, además de un enfoque más dinámico en las alertas de seguridad, lo que resalta la necesidad de preparar a los empleados de forma continua y actualizada.

Entrevista con el Personal de Recursos Humanos

Cargo: Coordinador de Recursos Humanos

1. Pregunta: ¿Cómo consideras que el personal de Recursos Humanos está involucrado en las políticas de seguridad de la información?

Respuesta: "El personal de Recursos Humanos tiene un papel crucial en la implementación de políticas de seguridad, especialmente en la protección de datos personales de los empleados. Sin embargo, muchas veces la capacitación y las actualizaciones de las políticas de seguridad no llegan de forma efectiva a todos los empleados, lo que genera brechas en el conocimiento."

Análisis cualitativo: La respuesta sugiere que, aunque Recursos Humanos desempeña un papel importante en la implementación de las políticas, las estrategias de comunicación deben mejorarse para garantizar que todos los empleados reciban y comprendan la capacitación.

2. Pregunta: ¿Qué medidas podrías sugerir para fortalecer la seguridad en el manejo de los datos de los empleados?

Respuesta: "Creo que deberíamos tener un protocolo claro sobre cómo manejar la información confidencial, y asegurar que todos los empleados pasen por un entrenamiento de ciberseguridad básico, independientemente de su rol. Además, se debería mejorar la comunicación sobre las políticas de seguridad en la empresa."

Análisis cualitativo: La respuesta destaca la necesidad de protocolos claros y de una capacitación más accesible para todos los empleados, lo que sugiere que la seguridad debe ser una responsabilidad compartida entre todos los departamentos de la empresa.

Entrevista con el Gerente

Cargo: Gerente General

1. Pregunta: ¿Cuál es tu visión general sobre la seguridad de la información en Hidrosoft?

Respuesta: "La seguridad de la información es una prioridad para nosotros, pero hemos identificado que aún existe cierta resistencia o desinformación entre algunos empleados. Las amenazas de ingeniería social son complejas y evolucionan rápidamente, por lo que necesitamos mantener la formación y las prácticas de seguridad siempre actualizadas."

Análisis cualitativo: El gerente reconoce la necesidad de actualizar constantemente las prácticas de seguridad, subrayando la importancia de la capacitación continua y la adaptación frente a nuevas amenazas.

ANEXO C CONTROLES ISO 27001:2022

	CONTROLES ANEXO C ISO 27001:2022			CONTROL VR 2013	ESTADO DEL CONTROL			
	5	CONTROLES ORGANIZACIONALES			NO APLICA	COMPLETO	PARCIAL	NINGUNO
	5	CONTROLES ORGANIZACIONALES				26%		
1	**5.1**	Políticas de seguridad de la información	**Control** La política de seguridad de la información y las políticas específicas asociadas deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal pertinente y partes interesadas pertinentes, y revisadas a intervalos planificados y cuando ocurran cambios significativos en la organización	A.5.1.1.				**X**
2	**5.2**	Roles y responsabilidades en la Seguridad de la Información	**Control** Los roles y responsabilidades de seguridad de la información se deben definir y asignar de acuerdo con las necesidades de la organización	A.6.1.1 A.9.2.1.				**X**
3	**5.3**	Segregación de deberes	**Control** Los deberes y áreas de responsabilidad en conflicto deberían segregarse	A.6.1.2				**X**
4	**5.4**	Responsabilidades de la dirección	Control La Alta Dirección debe exigir a todo el personal la aplicación de la seguridad de la Información de acuerdo con la política de seguridad de la Información establecida, las políticas y los procedimientos específicos de la organización en los aspectos correspondientes.	A.6.1.1	**X**			
5	**5.5**	Contacto con las autoridades	Control La organización debe establecer y mantener contacto con las autoridades pertinentes.	A.6.1.3			**X**	
6	**5.6**	Contacto con grupos de interés especial	Control La organización debe establecer y mantener contacto con grupos de interés especial u otros foros y asociaciones profesionales especializados en Seguridad	A.6.1.4			**X**	
7	**5.7**	Inteligencia de amenazas	ControlLa información relativa a las amenazas a la seguridad de la información se debe recopilar y analizar para producir inteligencia de las amenazas.					**X**
8	**5.8**	Seguridad de la Información en la gestión de proyectos	Control La seguridad de la información se debe integrar en la gestión de proyectos	A.6.1.5				**X**
9	**5.9**	Inventario de información y otros activos asociados	Control Se debe elaborar y mantener un inventario de la información y otros activos asociados, incluidos los propietarios	A.8.1.1			**X**	
10	**5.10**	Uso aceptable de la información y otros activos asociados	Control Se deben identificar, documentar e implementar normas para el uso aceptable y procedimientos para el tratamiento de la información y otros activos asociados.	A.8.1.3				
11	**5.11**	Devolución de activos	Control El personal y otras partes interesadas, según corresponda, deben devolver todos los activos de la organización en su posesión al cambiar o terminar su empleo, contrato o acuerdo	A.8.1.4			**X**	
12	**5.1**	Clasificación de la	Control	A.8.2.1			**X**	

	2	información	La información se debe clasificar de acuerdo con las necesidades de seguridad de la información de la organización sobre la base de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas	A.8.2.3				
13	**5.13**	Etiquetado de la información	Control Se debe elaborar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información de conformidad con el sistema de clasificación de la información adoptado por la organización.	A.8.2.2			**X**	
14	**5.14**	Transferencia de información	Control Las reglas, procedimientos o acuerdos de transferencia de información deben estar vigentes para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.	A.13.2.1			**X**	
15	**5.15**	Control de acceso	Control Las normas para controlar el acceso físico y lógico a la información y otros activos asociados se deben establecer e implementar sobre la base de los requisitos de seguridad empresarial y de la información	A.9.1.1A.9.2.2			**X**	
16	**5.16**	Gestión de identidades	Control Se debe gestionar el ciclo de vida completo de las identidades.	A.9.2.3				**X**
17	**5.17**	Información de autenticación	Control La asignación y gestión de la información de autenticación se debe controlar mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.	A.9.2.4			**X**	
18	**5.18**	Derechos de acceso	Control Los derechos de acceso a la información y otros activos asociados se deben aprovisionar, revisar, modificar y eliminar de acuerdo con la política y reglas específicas de la organización para el control de acceso.	A.9.2.5			**X**	
19	**5.19**	Seguridad de la información en las relaciones con proveedores	Control Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.	A.15.1.1			**X**	
20	**5.20**	Abordar la seguridad de la información dentro de los acuerdos con proveedores	Control Los requisitos pertinentes de seguridad de la información se deben establecer y acordar con cada proveedor en función del tipo de relación con el proveedor	A.15.1.2			**X**	
21	**5.21**	Gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y las telecomunicaciones (TIC)	Control Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados a la cadena de suministro de productos y servicios de TIC.	A.15.1.3				**X**
22	**5.22**	Seguimiento, revisión y gestión del cambio de los servicios de los proveedores	Control La organización debe monitorear, revisar, evaluar y gestionar regularmente el cambio en las prácticas de seguridad de la información de los proveedores y la prestación de servicios.	A.15.2.2				**X**
23	**5.23**	Seguridad de la información para el uso de servicios en la	Control Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se deben establecer, de acuerdo con los requisitos					**X**

		nube	de seguridad de la información de la organización					
24	**5.24**	Planificación y preparación de la gestión de incidentes de seguridad de la información	Control La organización debe planificar y preparar la gestión de incidentes de seguridad de la información mediante la definición, el establecimiento y la comunicación de procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información	A.16.1.1			**X**	
25	**5.25**	Evaluación y decisión sobre eventos de seguridad de la información	Control La organización debe evaluar los eventos de seguridad de la información y debe decidir si clasificarse como incidentes de seguridad de la información	A.16.1.4			**X**	
26	**5.26**	Respuesta a incidentes de seguridad de la información	Control Los incidentes de seguridad de la información se deben responder de conformidad con los procedimientos documentados.	A.16.1.5			**X**	
27	**5.27**	Aprender de los incidentes de seguridad de la información	Control Los conocimientos adquiridos a partir de incidentes de seguridad de la información se deben utilizar para reforzar y mejorar los controles de seguridad de la información.	A.16.1.6				**X**
28	**5.28**	Recopilación de evidencias	Control La organización debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.	A.16.1.7				**X**
29	**5.29**	Seguridad de la información durante una interrupción	Control La organización debe planificar cómo mantener la seguridad de la información en un nivel apropiado durante la interrupción.	A.17.1.1				**X**
30	**5.30**	Preparación de las TIC para la continuidad de negocio	Control La preparación para las TIC se debe planificar, implementar, mantener y probar basado en los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC				**X**	
31	**5.31**	Requisitos legales, legales, reglamentarios y contractuales	Control Los requisitos legales, reglamentarios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos se deben identificar, documentar y mantener actualizados.	A.18.1.1			**X**	
32	**5.32**	Derechos de propiedad intelectual	Control La organización debe implementar procedimientos apropiados para proteger derechos de propiedad intelectual.	A.18.1.2			**X**	
33	**5.33**	Protección de registros	Control Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso y liberación no autorizados	A.18.1.3				**X**
34	**5.34**	Privacidad y protección de la información de identificación personal (PII, por sus siglas en ingles)	Control La organización debe identificar y cumplir con los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales	A.18.1.4			**X**	
35	**5.35**	Revisión independiente de la seguridad de la información	Control El enfoque de la organización para administrar la seguridad de la información y su implementación, incluidas las personas, los	A.18.2.1			**X**	

		procesos y las tecnologías, se debe revisar de forma independiente a intervalos planificados o cuando ocurran cambios significativos					
5.36	Cumplimiento de políticas, reglas y estándares de seguridad de la información	Control El cumplimiento de la política de seguridad de la información, el tema, las políticas específicas, las reglas y los estándares de la organización se debe revisar periódicamente.	A.18.2.2			**X**	
5.37	Procedimientos operativos documentados	Control Los procedimientos operativos de las instalaciones de procesamiento de la información se debe documentar y poner a disposición del personal que los necesite	A.12.1.1			**X**	
				1	1	17	13
6	**CONTROLES DE PERSONAS**					**44%**	
6.1	RESPONSABILIDAD DE LA DIRECCIÓN	Control Las verificaciones de antecedentes de todos los candidatos para convertirse en personal se deben llevar a cabo antes de unirse a la organización y de forma continúa teniendo en cuenta las leyes, regulaciones y ética aplicables y deben ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos	A.7.2.1			**X**	
6.2	Términos y condiciones de empleo	Control Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización para la seguridad de la información	A.7.3.1.			**X**	
6.3	Conciencia de seguridad de la información, educación y formación	Control El personal de la organización y las partes interesadas pertinentes deben recibir información, educación y capacitación adecuadas sobre seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos del tema, según sea pertinente para su función laboral	A.7.2.2			**X**	
6.4	Proceso disciplinario	Control Se debe formalizar y comunicar un proceso disciplinario para tomar medidas contra el personal y otras partes interesadas pertinentes que hayan cometido una violación de la política de seguridad de la información	A.7.2.3			**X**	
6.5	Responsabilidades después de la terminación o cambio de empleo	Control Las responsabilidades y deberes de seguridad de la información que sigan siendo válidos después de la terminación o el cambio de empleo se debe definir, hacer cumplir y comunicar al personal pertinente y a otras partes interesadas	A.7.3.1.			**X**	
6.6	Acuerdos de confidencialidad o no divulgación	Control Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados y firmados periódicamente por el personal y otras partes interesadas pertinentes.	A.7.1,2			**X**	
6.7	Trabajo remoto	Control Las medidas de seguridad se deben implementar cuando el personal trabaje de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización	A.6.2.2				**X**

45	**6.8**	Informes de eventos de seguridad de la información	Control La organización debe proporcionar un mecanismo para que el personal informe oportunamente sobre los eventos de seguridad de la información observados o sospechosos a través de los canales apropiados	A.16.1.3			**X**	
					0	0	7	1
	7	**CONTROLES FÍSICOS**					**36%**	
46	**7.1**	Perímetros de seguridad física	Control Los perímetros de seguridad se deben definir y utilizar para proteger las zonas que contengan información y otros activos asociados.	A.11.1.1			**X**	
47	**7.2**	Entrada física	Control Las zonas seguras deben estar protegidas por controles de entrada y puntos de acceso adecuados	A.11.1.2			**X**	
48	**7.3**	Asegurar oficinas, habitaciones e instalaciones	Control Se debe diseñar e implementar la seguridad física de las oficinas, salas e instalaciones.	A.11.1.3			**X**	
49	**7.4**	Monitoreo de la seguridad física	Control Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados					**X**
50	**7.5**	Protección contra amenazas físicas y ambientales	Control Se debe diseñar e implementar la protección contra las amenazas físicas y medioambientales, como las catástrofes naturales y otras amenazas físicas intencionadas o no intencionadas a las infraestructuras.	A.11.1.4			**X**	
51	**7.6**	Trabajar en áreas seguras	Control Se deben diseñar e implementar medidas de seguridad para trabajar en zonas seguras	A.11.1.5			**X**	
52	**7.7**	Escritorio y pantalla limpios	Control Se deben definir e implementar adecuadamente normas claras para los papeles y los soportes de almacenamiento extraíbles y normas claras sobre pantallas claras para las instalaciones de tratamiento de la información.	A.112.9			**X**	
53	**7.8**	Emplazamiento y protección de equipos	Control El equipo debe estar situado de forma segura y protegida	A.11.2.1			**X**	
54	**7.9**	Seguridad de los activos fuera de las instalaciones	Control Los activos externos deben estar protegidos.	A.11.2.6				**X**
55	**7.10**	Medios de almacenamiento	Control Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y disposición de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización	A.8.3.1			**X**	
56	**7.11**	Servicios públicos de apoyo	Control Las instalaciones de procesamiento de la información deben estar protegidas contra los cortes de energía y otras interrupciones causadas por fallos en los servicios públicos de apoyo.	A.11.2.2			**X**	
57	**7.12**	Seguridad del cableado	Control Los cables que transporten energía, datos o servicios de información de apoyo deben estar protegidos contra la interceptación, las interferencias o los daños.	A.11.2.3			**X**	
58	**7.13**	Mantenimiento de equipos	Control El equipo se debe mantener correctamente	A.11.2.4				**X**

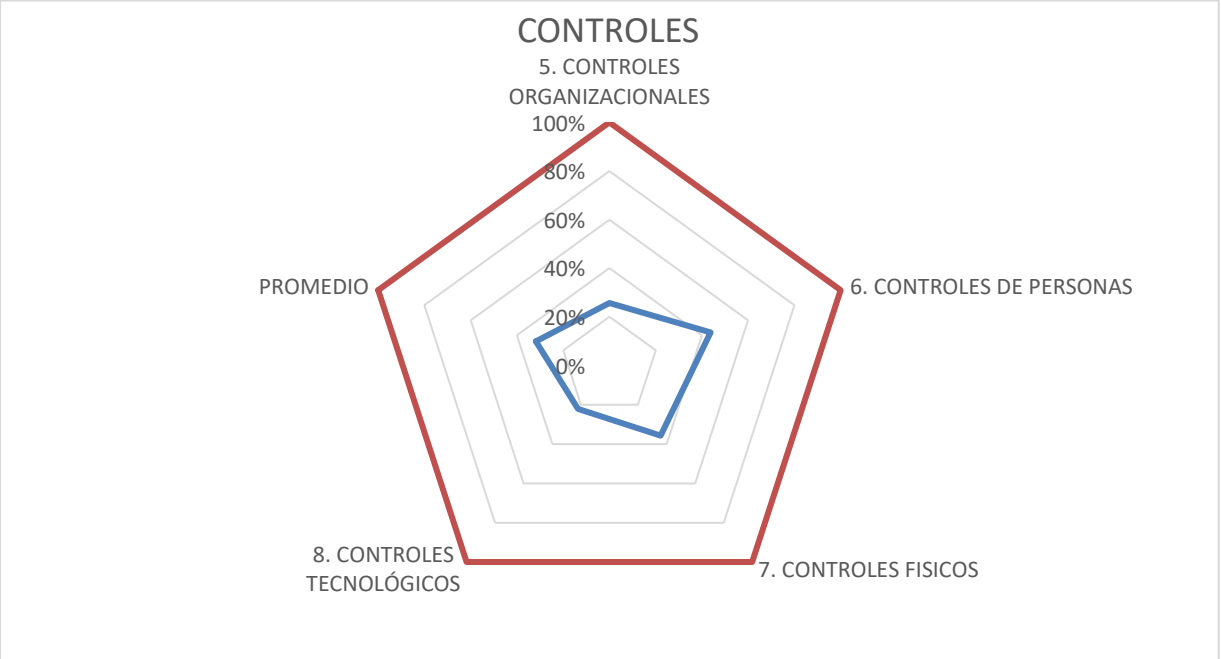
		para asegurar la disponibilidad, integridad y confidencialidad de la información.					
7.14	Disposición o reutilización segura de los equipos	Control Los elementos de los equipos que contengan medios de almacenamiento se deben verificar para asegurarse de que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su disposición o reutilización.	A.11.2.7				**X**
				0	0	10	4
8	**CONTROLES TECNOLOGICOS**					**22%**	
8.1	Dispositivos de punto final de usuario	Control Se debe proteger la información almacenada, procesada o accesible a través de los dispositivos de punto final del usuario	A.8.3.1			**X**	
8.2	Derechos de acceso privilegiado	ControlLa asignación y el uso de los derechos de acceso privilegiado deben estar restringidos y gestionados.	A.9.1.2.A.9.2.2			**X**	
8.3	Restricción de acceso a la información	Control El acceso a la información y a otros activos asociados se debe restringir de acuerdo con la política específica establecida sobre el control de acceso.	A.9.4.1			**X**	
8.4	Acceso al código fuente	Control El acceso para leer o escribir sobre un código fuente, las herramientas de desarrollo, y las librerías de software se deben gestionar apropiadamente	A.14.2.1				**X**
8.5	Autenticación segura	Control Se deben implementar tecnologías y procedimientos de autenticación seguros basados en restricciones de acceso a la información y en la política específica del tema sobre control de acceso.	A.9.4.2			**X**	
8.6	Gestión de la capacidad	Control El uso de los recursos se debe monitorear y ajustar en función de las necesidades de capacidades actuales y previstas.	A.17.1.3			**X**	
8.7	Protección contra malware	Control La protección contra el malware se debe implementar y respaldar mediante la conciencia adecuada del usuario.	A.12.2.1				**X**
8.8	Gestión de vulnerabilidades técnicas	Control Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a dichas vulnerabilidades y se deben adoptar las medidas apropiadas.	A.12.6.1				**X**
8.9	Gestión de la configuración	Control Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes se deben establecer, documentar, implementar, monitorear y revisar.					**X**
8.10	Eliminación de información	Control La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento se debe eliminar cuando ya no sea necesario					**X**
8.11	Enmascaramiento de datos	Control El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la					**X**

			organización sobre control de acceso y otras políticas relacionadas con temas específicos, y los requisitos comerciales, teniendo en cuenta la legislación aplicable					
71	**8.12**	Prevención de fugas de datos	Control Las medidas de prevención de fugas de datos se deben implementar a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.					**X**
72	**8.13**	Copia de seguridad de la información	Control Las copias de seguridad de la información, el software y los sistemas se deben mantener y probar periódicamente de conformidad con la política específica sobre copias de seguridad sobre temas específicos	A.12.3.1			**X**	
73	**8.14**	Redundancia de las instalaciones de procesamiento de información	Control Las instalaciones de procesamiento de la información se deben implantar con redundancia suficiente para cumplir los requisitos de disponibilidad	A.17.2.1				**X**
74	**8.15**	Registro	Control Los registros que guarden actividades, excepciones, fallas y otros eventos pertinentes se deben producir, almacenar, proteger y analizar	A.12.7				**X**
75	**8.16**	Actividades de seguimiento	Control Se debe monitorear el comportamiento anómalo de las redes, los sistemas y las aplicaciones y se deben adoptar las medidas adecuadas para evaluar posibles incidentes de seguridad de la información.					**X**
76	**8.17**	Sincronización de reloj	Control Los relojes de los sistemas de procesamiento de información utilizados por la organización se deben sincronizar con las fuentes de tiempo aprobadas.	A.12.4.4				**X**
77	**8.18**	Uso de programas de utilidad privilegiados	Control El uso de programas de utilidad que puedan ser capaces de anular los controles del sistema y de la aplicación debe restringirse y controlarse estrictamente.	A.12.5.1				**X**
78	**8.19**	Instalación de software en sistemas operativos	Control Se deben implementar procedimientos y medidas para gestionar de forma segura la instalación de programas informáticos en los sistemas operativos	A.12.5.1			**X**	
79	**8.20**	Seguridad de redes	Control Las redes y los dispositivos de red deben estar asegurados, gestionados y controlados para proteger la información de los sistemas y las aplicaciones.	A.13.1.1			**X**	
80	**8.21**	Seguridad de los servicios de red	Control Se deben identificar, implementar y monitorear los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.	A.13.1.2			**X**	
81	**8.22**	Segregación de redes	Control Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en las redes de la organización.	A.13.1.3			**X**	
82	**8.23**	Filtrado web	Control El acceso a sitios web externos se debe				**X**	

		gestionar para reducir la exposición a contenido malicioso.						
83	**8.24**	Uso de la criptografía	Control Se debe definir e implementar normas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.	A.10.1.2			**X**	
84	**8.25**	Ciclo de vida de desarrollo seguro	Control Se deben establecer e implementar normas para el desarrollo seguro de software y sistemas	A.14.2.1			**X**	
85	**8.26**	Requisitos de seguridad de las aplicaciones	ControlLos requisitos de seguridad de la información se deben identificar, especificar y aprobar al desarrollar o adquirir aplicaciones				**X**	
86	**8.27**	Arquitectura de sistemas seguros y principios de ingeniería	Control Los principios para la ingeniería de sistemas seguros se deben establecer, documentar, mantener e implementar a cualquier actividad de desarrollo de sistemas de información	A.14.2.5				**X**
87	**8.28**	Codificación segura	Control Los principios de codificación segura se deben implementar al desarrollo de programas informáticos					**X**
88	**8.29**	Pruebas de seguridad en el desarrollo y aceptación	Control Los procesos de ensayo de seguridad se deben definir e implementar en el ciclo de vida del desarrollo	A.14.2.8				**X**
89	**8.30**	Desarrollo externalizado	Control La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados	A.14.2.7				**X**
90	**8.31**	Separación de entornos de desarrollo, evidencia y producción	Control Los entornos de desarrollo, ensayo y producción deben estar separados y protegidos	A.14.2.9				**X**
91	**8.32**	Gestión del cambio	Control Los cambios en las instalaciones de procesamiento de la información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios	A.12.1.2 A.14.2.2			**X**	
92	**8.33**	Información de las pruebas	Control La información de las pruebas se debe seleccionar, proteger y gestionar adecuadamente	A.14.3.1				**X**
93	**8.34**	Protección de los sistemas de información durante las pruebas de auditoría	Control Las pruebas de auditoría y otras actividades de aseguramiento que impliquen la evaluación de los sistemas operativos se deben planificar y acordar conjuntamente entre el probador y la dirección adecuada	A.14.2.8				**X**
					0	0	15	19

Tabla 17 CONTROLES

CAPÍTULOS	NIVEL DE IMPLEMENTACIÓN	
	NIVEL ACTUAL	NIVEL DESEADO
5. CONTROLES ORGANIZACIONALES	26%	100%
6. CONTROLES DE PERSONAS	44%	100%
7. CONTROLES FISICOS	36%	100%
8. CONTROLES TECNOLÓGICOS	22%	100%
PROMEDIO	32%	100%



ANEXO D: LISTADO Y VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Nro. Activo	Proceso Macro	Subproceso	Tipo de Activo	Nombre de Activo	Descripción del activo	Intención del Uso	Tipo de soporte	Ubicación	Valoración de Impacto (pérdida) C: Confidencialidad I: Integridad D: Disponibilidad			
									C	I	D	VA
A1	Mantenimiento de servidores	Mantenimiento de Servidor NAS	Hardware	NAS	Dispositivo de almacenamiento de alta capacidad conectado a una red	Permite a los usuarios y clientes autorizados, almacenar y recuperar datos en una ubicación localizada	Físico	Data Center	3	3	2	2,67
A2	Gestión Tecnológico	Actualización de Software de Sistemas Operativos	Software	SISTEMA OPERATIVO DE COMPUTADOR DE ESCRITORIO	Es un software que actúa como intermediario entre el hardware de un computador y los programas y aplicaciones que se ejecutan en él	Se encarga de administrar los recursos del sistema, como la memoria y el procesador, y proporciona una interfaz de usuario para que el usuario pueda interactuar con el equipo.	Lógico	Matriz Institución	1	1	3	1,67
A3	Mantenimiento de red	Operación y Mantenimiento	Redes	FORTIGATE	Firewall de Red, para proteger la comunicación de la red.	Dispositivo que se utiliza para proteger una red de amenazas externas a través de la gestión del tráfico de red	Físico y Lógico	Data Center	3	3	3	3,00
A4	Protección de DATA CENTER	Instalación de Equipo	Localidad	BIOMETRICO POR RFID	Es un dispositivo que utiliza tecnología de identificación por radiofrecuencia (RFID) y tecnología biométrica para autenticar la identidad de una persona	La tecnología RFID permite la lectura de etiquetas o tarjetas a través de ondas de radio, mientras que la tecnología biométrica utiliza rasgos físicos únicos, como huellas dactilares o reconocimiento facial, para confirmar la identidad de una persona	Físico	Data Center	3	3	3	3,00

A5	Soporte técnico	Soporte técnico de primer nivel	Organización	DESK SERVICE	El service desk es un soporte multifuncional que incorpora desde servicios técnicos a comerciales.	Sus funciones sirven para brindar soporte a los clientes y organizar los procesos internos de la empresa (demandas de soporte que se generan en el interior de las organizaciones).	Físico y Lógico	Matriz Institución	3	3	3	3,00
A6	Gestión Administrativa Financiera	Servidor Contable	Datos	BASE DE DATOS DEL SISTEMA	Es una herramienta informática que almacena y gestiona información financiera y contable de la Empresa. Esta base de datos contiene información como facturas, recibos, estados financieros, registros de cuentas, movimientos de cuentas bancarias, balances, entre otros.	Permite a la Institución el análisis de información contable para la toma de decisiones financieras, estratégicas y giro de negocios y con ello dar cumplimiento de obligaciones legales y fiscales inherentes de una Empresa Pública.	Digital	Matriz Institución	2	3	3	2,67
A7	Estructura Orgánica	Cargos inadecuados del personal	Personal	TIC´s	Son recursos y herramientas que se utilizan para el proceso, administración y distribución de la información a través de elementos tecnológicos	Facilitar el acceso a la información fácil y rápida en cualquier formato, esto es posible a través de la inmaterialidad; es decir de la digitalización de la información para almacenarla en grandes cantidades o tener acceso aún si está en dispositivos lejanos	Físico y Lógico	Data Center	3	2	2	2,33

ANEXO E: MATRIZ DE ANALIS Y EVALUACIÓN DE RIESGOS

Análisis de Riesgos					Evaluación de Riesgos				
					Impacto	Probabilidad		Cálculo de Evaluación Riesgo	Nivel de Riesgo
Proceso Macro	Subprocesos	Nro. Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad		
Mantenimiento de servidores	Mantenimiento de Servidor NAS	A1	Incumplimiento en el mantenimiento del sistema de información	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	2,67	1	2	5,33	MEDIO
			Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad.	2,67	1	1	2,67	BAJO
			Fenómenos meteorológicos	Susceptibilidad a las variaciones de temperatura	2,67	1	2	5,33	MEDIO
			Hurto de medios o documentos	Copia no controlada	2,67	3	2	16,00	ALTO
			Hurto de medios o documentos	Almacenamiento sin protección	2,67	3	3	24,00	ALTO
			Pérdida del suministro de energía	Susceptibilidad a las variaciones de voltaje	2,67	1	1	2,67	BAJO
Gestión Tecnológico	Actualización de Software de Sistemas Operativos	A2	Fallos en la actualización	Ausencia o insuficiencia de pruebas de software	1,67	1	1	1,67	BAJO
			Vulnerabilidades de seguridad	Software nuevo o inmaduro	1,67	2	2	6,67	MEDIO

			Interrupción del flujo de trabajo	Interfaz de usuario compleja	1,67	2	2	6,67	MEDIO
Mantenimiento de red	Operación y Mantenimiento	A3	Negación de acciones	Ausencia de pruebas de envío o recepción de mensajes	3,00	1	2	6,00	MEDIO
			Escucha encubierta	Líneas de comunicación sin protección	3,00	2	3	18,00	ALTO
			Escucha encubierta	Tráfico sensible sin protección	3,00	3	2	18,00	ALTO
			Falsificación de derechos	Ausencia de identificación y autentificación de emisor y receptor	3,00	3	3	27,00	ALTO
			Falla del equipo de telecomunicaciones	Conexión deficiente de los cables.	3,00	1	1	3,00	BAJO
Protección de DATA CENTER	Instalación de Equipo	A4	Destrucción de equipo o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3,00	3	2	18,00	ALTO
			Pérdida del suministro de energía	Red energética inestable	3,00	1	2	6,00	MEDIO
			Hurto de equipo	Ausencia de protección física de la edificación, puertas y ventanas	3,00	2	3	18,00	ALTO
Soporte técnico	Soporte técnico de primer nivel	A5	Perdida de equipo	Ausencia de planes de continuidad	3,00	2	2	12,00	ALTO
			Ingeniería social	Fugas de información	3,00	3	3	27,00	ALTO
Gestión Administrativa Financiera	Servidor Contable	A6	Hurto de medios o documentos	Copia no controlada	2,67	2	2	10,67	ALTO

			Hurto de medios o documentos	Almacenamiento sin protección	2,67	3	3	24,00	ALTO
			Ausencia de documentación	Error en el uso	2,67	1	1	2,67	BAJO
Estructura Orgánica	Cargos Inadecuados de Personal	A7	Incumplimiento en la disponibilidad del personal	Ausencia de personal	2,33	2	2	9,33	ALTO
			Uso no autorizado de los equipos	Ausencia de mecanismos de monitoreo	2,33	3	2	14,00	ALTO
			Destrucción de equipos y medios	Procedimientos inadecuados de contratación	2,33	2	3	14,00	ALTO

TRATAMIENTO DE RIESGOS

Análisis de Riesgos		Evaluación de Riesgos	Tratamiento de Riesgos							Riesgo residual
Nro. Activo	Amenaza	Nivel de Riesgo	Método de tratamiento de Riesgos	Tipo de control	Controles a Implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado	
A1	Incumplimiento en el mantenimiento del sistema de información	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	GENERAR UN CRONOGRAMA DE MANTENIMIENTO CON UN RESPONSABLE PARA INFORMAR	1	1	2,67	BAJO	ACEPTABLE
	Polvo, corrosión, congelamiento	BAJO	ACEPTAR	NO APLICA CONTROL						
	Fenómenos meteorológicos	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	IMPLEMENTACION DE SISTEMA DE REFRIGERACION QUE MANTENGA UNA TEMPERATURA ADECUADA	1	1	2,67	BAJO	ACEPTABLE
	Hurto de medios o documentos	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL CORRECTIVO	REFUERZO DE LA SEGURIDAD FISICA DEL DATA CENTER	2	1	5,33	MEDIO	INACEPTABLE
	Hurto de medios o documentos	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	CIFRADO DE LA INFORMACION	1	1	2,67	BAJO	ACEPTABLE
	Pérdida del suministro de energía	BAJO	ACEPTAR	NO APLICA CONTROL						
A2	Fallos en la actualización	BAJO	ACEPTAR	NO APLICA CONTROL						
	Vulnerabilidades de seguridad	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	ADQUISICION DE LICENCIAS	1	1	1,67	BAJO	ACEPTABLE

	Interrupción del flujo de trabajo	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	PERSONALIZACION DE ACUERDO AL USUARIO	1	1	1,67	BAJO	ACEPTABLE
A3	Negación de acciones	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	TESTEO DE COMUNICACIÓN	1	2	6,00	MEDIO	INACEPTABLE
	Escucha encubierta	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	AUTORIZACION POR MAC	1	1	3,00	BAJO	ACEPTABLE
	Escucha encubierta	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL CORRECTIVO	ENCRIPTACION DE PUNTO A PUNTO	1	1	3,00	BAJO	ACEPTABLE
	Falsificación de derechos	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	CREAR UN CANAL CIFRADO	1	1	3,00	BAJO	ACEPTABLE
	Falla del equipo de telecomunicaciones	BAJO	ACEPTAR	NO APLICA CONTROL						
A4	Destrucción de equipo o medios	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL CORRECTIVO	PROTECCION DEL EQUIPO MEDIANTE CASE	1	1	3,00	BAJO	ACEPTABLE
	Pérdida del suministro de energía	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	IMPLEMENTACION DE UPS	1	1	3,00	BAJO	ACEPTABLE
	Hurto de equipo	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	INSTALACION DE CCTV	1	1	3,00	BAJO	ACEPTABLE
A5	Perdida de equipo	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	CONTROL PREVENTIVO	1	1	3,00	BAJO	ACEPTABLE
	Ingeniería social	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	BLOQUEO DE PAGINAS NO AUTORIZADAS / CAPACITACION	1	1	3,00	BAJO	ACEPTABLE
A6	Hurto de medios o documentos	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	CIFRADO DE LA INFORMACION	1	1	2,67	BAJO	ACEPTABLE

	Hurto de medios o documentos	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	CREACION DE ESPEJO	2	1	5,33	MEDIO	INACEPTABLE
	Ausencia de documentación	BAJO	ACEPTAR	NO APLICA CONTROL						
A7	Incumplimiento en la disponibilidad del personal	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	DELEGACION DERESPONSABILIDADES Y CONTRATAR PERSONAL IDONEO	1	1	2,33	BAJO	ACEPTABLE
	Uso no autorizado de los equipos	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL CORRECTIVO	CREAR SALES E IMPLEMENTAR PERSONAL DE MONITOREO DE CCTV	1	1	2,33	BAJO	ACEPTABLE
	Destrucción de equipos y medios	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	CONTRATAR PERSONAL ADECUADO ACORDE A LAS NECESIDADES ESPECIFICAS DEL PUESTO DE TRABAJO	1	1	2,33	BAJO	ACEPTABLE

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

ANEXO F: PLAN DE MITIGACIÓN DE RIESGOS

Objetivo: Detallar las medidas de seguridad propuestas para mitigar los riesgos de ingeniería social identificados durante la investigación, proporcionando una descripción exhaustiva de cada una de las estrategias de seguridad recomendadas para la protección de los datos sensibles y la infraestructura tecnológica de Hidrosoft.

1. Implementación de Autenticación Multifactorial (MFA)

La autenticación multifactorial (MFA) es una medida de seguridad esencial para proteger el acceso a sistemas y datos sensibles de Hidrosoft. Combina múltiples factores de autenticación para garantizar que solo los usuarios autorizados puedan acceder a los recursos.

---

1. Objetivos de la MFA

- **Reducir el riesgo de acceso no autorizado:** Evitar que un atacante acceda a sistemas incluso si obtiene credenciales básicas como usuario y contraseña.
- **Proteger datos sensibles:** Salvaguardar la información de clientes y empleados.
- **Cumplir con normativas:** Asegurar el cumplimiento de regulaciones y estándares de seguridad.

---

2. Factores de Autenticación

El MFA requiere al menos dos de los siguientes factores:

1. **Algo que el usuario sabe:**
    - Contraseñas.
    - PIN.
2. **Algo que el usuario tiene:**
    - Token físico (dispositivos USB, tarjetas inteligentes).
    - Código enviado al correo electrónico o teléfono (OTP: One-Time Password).

- Aplicaciones de autenticación como Google Authenticator o Microsoft Authenticator.

3. **Algo que el usuario es:**
    - Biométricos (huella digital, reconocimiento facial, escaneo de iris).

---

3. Proceso de Implementación

Fase 1: Evaluación Inicial

- Identificar los sistemas y datos críticos que requerirán MFA.
- Realizar un análisis de riesgos para priorizar las áreas que más lo necesiten.
- Evaluar las soluciones tecnológicas disponibles que sean compatibles con la infraestructura actual.

Fase 2: Selección de Herramientas

- Elegir un proveedor de MFA confiable y escalable como:
    - Duo Security.
    - Microsoft Azure MFA.
    - Google Authenticator.
    - Authy.
- Asegurarse de que la herramienta elegida sea compatible con las aplicaciones y sistemas usados por Hidrosoft.

Fase 3: Diseño de la Implementación

- Establecer políticas claras sobre quiénes deben usar MFA y en qué contextos.
    - Ejemplo: Acceso remoto, sistemas con datos sensibles, cambios en configuraciones críticas.
- Definir los métodos de autenticación según los roles y necesidades de los usuarios.
- Integrar la solución MFA con los sistemas existentes (correo, VPN, aplicaciones empresariales).

Fase 4: Pruebas Piloto

- Realizar pruebas con un grupo reducido de usuarios para:
    - Detectar problemas técnicos.

    - Recoger feedback sobre la experiencia del usuario.
    - Ajustar configuraciones según sea necesario.

Fase 5: Implementación General

- Activar MFA en todas las cuentas de usuarios que tengan acceso a datos sensibles.
- Proveer instrucciones detalladas para la configuración inicial:
    - Guías paso a paso para registrar dispositivos o aplicaciones.
    - Sesiones de capacitación para resolver dudas.
- Establecer un sistema de soporte técnico para atender posibles inconvenientes.

---

4. Consideraciones Clave

- **Facilidad de uso:** Elegir métodos de MFA que sean sencillos para los empleados, minimizando interrupciones en sus tareas diarias.
- **Respaldo en caso de pérdida:** Tener opciones de recuperación, como códigos de respaldo o contacto con soporte, en caso de que los usuarios pierdan sus dispositivos.
- **Monitoreo y auditoría:** Implementar registros de auditoría para rastrear el uso del MFA y detectar intentos fallidos de acceso.

---

5. Beneficios de Implementar MFA

- **Protección robusta:** Mitiga el riesgo de acceso no autorizado incluso en caso de robo de contraseñas.
- **Cumplimiento normativo:** Refuerza la seguridad para alinearse con estándares como ISO 27001 y regulaciones de protección de datos.
- **Confianza del cliente:** Mejora la percepción de Hidrosoft como una organización comprometida con la seguridad.

---

6. Seguimiento y Mejora Continua

- Evaluar periódicamente la efectividad del MFA.
- Actualizar la configuración según las necesidades emergentes o nuevos vectores de ataque.

- Mantener a los empleados informados sobre buenas prácticas relacionadas con MFA.

2. Capacitación Periódica sobre Ingeniería Social

La capacitación continua es clave para equipar a los empleados con las herramientas necesarias para identificar y mitigar las amenazas de ingeniería social. Aquí se presenta un plan estructurado para Hidrosoft:

1. Objetivo de la Capacitación

- Desarrollar la capacidad de los empleados para reconocer tácticas de ingeniería social como phishing, vishing, smishing y pretexting.
- Reducir la vulnerabilidad de la empresa al fortalecer la primera línea de defensa: los empleados.
- Promover una cultura de ciberseguridad proactiva.

---

2. Contenidos de la Capacitación

La capacitación debe cubrir los siguientes aspectos:

Conceptos Básicos

- ¿Qué es la ingeniería social?
- Ejemplos de ataques comunes:
    - Phishing: Correos electrónicos engañosos.
    - Smishing: Mensajes de texto fraudulentos.
    - Vishing: Llamadas telefónicas manipuladoras.
    - Pretexting: Creación de escenarios falsos para obtener información.

Reconocimiento de Amenazas

- Cómo identificar mensajes sospechosos:
    - Ortografía y gramática inusual.
    - Enlaces o adjuntos inesperados.
    - Solicitudes urgentes o fuera de lo común.
- Cómo verificar la autenticidad de las solicitudes.

Respuestas Ante un Intento de Ataque

- Procedimientos para reportar mensajes sospechosos.
- Acciones inmediatas en caso de divulgar información por error.

Impacto de los Ataques

- Casos reales y simulados de cómo los ataques de ingeniería social afectan la seguridad empresarial.

---

3. Métodos de Capacitación

- **Sesiones Presenciales o Virtuales:**
    - Instructores especializados en ciberseguridad.
    - Interacción en tiempo real para resolver dudas y realizar simulaciones.
- **Materiales Interactivos:**
    - Videos explicativos y guías visuales.
    - Ejercicios prácticos que simulen escenarios de ingeniería social.
- **E-learning:**
    - Cursos en línea accesibles para los empleados según su disponibilidad.
    - Test de evaluación al finalizar cada módulo.

---

4. Simulaciones y Pruebas Prácticas

- **Ataques Simulados:** Realizar simulaciones periódicas para evaluar la respuesta de los empleados y reforzar los aprendizajes.
- **Feedback Personalizado:** Proveer retroalimentación inmediata a quienes caigan en las simulaciones, identificando áreas de mejora.

---

5. Frecuencia y Actualización

- **Periodicidad:** Implementar capacitaciones trimestrales.
- **Actualización:** Adaptar los contenidos para incluir nuevas tácticas emergentes de ingeniería social.

- **Evaluación:** Realizar evaluaciones al finalizar cada capacitación para medir el impacto y ajustar los programas.

---

6. Beneficios Esperados

- Mayor conciencia y preparación ante amenazas de ingeniería social.
- Reducción de incidentes causados por errores humanos.
- Fortalecimiento de la cultura organizacional en torno a la ciberseguridad.

3. Simulaciones de Phishing

Las simulaciones de phishing son una herramienta clave para evaluar la preparación de los empleados y detectar vulnerabilidades en las defensas de la empresa. Se recomienda realizar simulaciones de phishing de forma periódica e impredecible, lo que permitirá a Hidrosoft evaluar la respuesta de los empleados ante un ataque real de este tipo.

Estas simulaciones deben incluir los siguientes pasos y características esenciales:

1. Planificación de las Simulaciones de Phishing

Antes de comenzar, es importante definir los objetivos de las simulaciones:

- Identificar puntos débiles en el conocimiento y comportamiento de los empleados.
- Mejorar la capacidad de los empleados para reconocer ataques de phishing y actuar de manera adecuada.
- Evaluar la efectividad de las políticas y la capacitación actuales.

2. Diseño de los Ataques de Phishing

- **Personalización de correos electrónicos**: Diseñar mensajes que sean relevantes para el entorno laboral de los empleados. Por ejemplo, simulaciones que parezcan provenir de un cliente, proveedor o un departamento interno de la empresa.
- **Uso de tácticas realistas**: Incluir enlaces a sitios falsos, adjuntos maliciosos y solicitudes de datos personales o de acceso a sistemas.
- **Multicanal**: Ampliar las simulaciones más allá del correo electrónico para incluir:
    - **Smishing**: Enviar mensajes de texto simulando ser servicios confiables.
    - **Vishing**: Realizar llamadas simuladas para obtener información confidencial.

- **Redes sociales**: Crear perfiles falsos para intentar interactuar con empleados.

3. Ejecución de las Simulaciones

- **Periodicidad e imprevisibilidad**: Realizar simulaciones trimestrales en días y horarios no anunciados para evaluar respuestas espontáneas.
- **Segmentación**: Dirigir simulaciones específicas a diferentes departamentos o roles dentro de la empresa.

4. Evaluación de Resultados

- **Recolección de métricas**:
  - Número de empleados que hacen clic en enlaces falsos.
  - Número de empleados que divulgan información confidencial.
  - Tiempo de reacción antes de reportar el intento de phishing.
- **Análisis de patrones**: Identificar si ciertos tipos de mensajes o canales tienen tasas de éxito más altas para los atacantes.

5. Retroalimentación y Aprendizaje

- **Educación inmediata**: Los empleados que caigan en las simulaciones deben recibir una alerta que:
  - Explique por qué el correo o mensaje era un intento de phishing.
  - Indique qué señales deberían haber detectado.
  - Proporcione recursos para mejorar su capacidad de respuesta.
- **Reportes generales**: Compartir de manera anónima las estadísticas y lecciones aprendidas con toda la empresa para fomentar una cultura de seguridad.

6. Revisión y Ajuste

- Realizar un análisis posterior a cada simulación para:
  - Identificar tendencias o patrones en las respuestas.
  - Ajustar las capacitaciones y políticas con base en los hallazgos.
  - Implementar mejoras continuas en los programas de seguridad.

4. Desarrollo de un Código Ético y Comunicación Transparente

La creación de un código ético y una estrategia de comunicación transparente

son elementos fundamentales para fortalecer la confianza de los empleados, clientes y socios comerciales, y para promover prácticas de ciberseguridad responsables en Hidrosoft.

---

1. Código Ético en Ciberseguridad

El código ético debe ser un documento accesible que sirva como guía para las decisiones y acciones relacionadas con la seguridad de la información. Este código debe incluir:

Principios Básicos

1. **Compromiso con la privacidad:**
    - Priorizar la protección de los datos personales de clientes, empleados y socios.
    - Garantizar el manejo ético de la información sensible, limitando su uso al propósito autorizado.
2. **Responsabilidad corporativa:**
    - Reconocer la obligación de actuar proactivamente ante riesgos cibernéticos.
    - Asumir responsabilidad por los incidentes de seguridad y trabajar para remediarlos de manera efectiva.
3. **Transparencia:**
    - Comunicar oportunamente las medidas implementadas y cualquier incidente de seguridad.
    - Establecer protocolos claros para informar a los clientes y empleados sobre los riesgos detectados.
4. **Cumplimiento normativo:**
    - Alinearse con regulaciones locales e internacionales como la Ley Orgánica de Protección de Datos Personales (Ecuador, 2021) y el Reglamento General de Protección de Datos (GDPR).

Divulgación

- Asegurar que el código sea accesible para todos los empleados a través de la intranet y en formato físico para las oficinas.

- Presentarlo a los nuevos empleados durante su inducción y realizar capacitaciones anuales sobre su contenido.

---

2. Campañas Internas de Concienciación

Para garantizar que los empleados comprendan y adopten los principios del código ético, es necesario implementar campañas internas regulares:

Actividades Propuestas

- **Material educativo:**
    - Crear guías prácticas, infografías y boletines que expliquen los principios del código ético y cómo aplicarlos en el día a día.
- **Talleres y seminarios:**
    - Organizar sesiones interactivas para discutir casos reales y cómo los principios éticos ayudaron a resolver desafíos de ciberseguridad.
- **Simulaciones y ejercicios:**
    - Realizar simulaciones de incidentes de seguridad para evaluar cómo los empleados aplican los principios éticos en situaciones reales.

Evaluación de Impacto

- Realizar encuestas para medir la comprensión de los empleados sobre el código ético y su percepción de las campañas de concienciación.
- Ajustar las campañas con base en los resultados para maximizar su efectividad.

---

3. Relación con Clientes: Comunicación Transparente

La transparencia con los clientes es clave para fortalecer la confianza y demostrar un compromiso con la seguridad y la ética.

Iniciativas Clave

1. **Informes Periódicos:**
    - Publicar actualizaciones regulares sobre las medidas de seguridad implementadas, incluyendo avances y logros.
    - Compartir informes de auditorías externas que certifiquen el cumplimiento de estándares de ciberseguridad.

2. **Gestión de Incidentes:**
    - Establecer un protocolo claro para notificar a los clientes sobre incidentes que puedan afectar sus datos.
    - Explicar las acciones correctivas tomadas y cómo se evitarán problemas similares en el futuro.
3. **Canales de Comunicación Directos:**
    - Habilitar una línea de atención exclusiva para inquietudes de seguridad.
    - Proveer respuestas rápidas y claras a las preguntas de los clientes relacionados con sus datos.
4. **Campañas de Confianza:**
    - Crear contenido educativo en redes sociales y boletines electrónicos para informar a los clientes sobre cómo proteger su información.
    - Resaltar las iniciativas de ciberseguridad de Hidrosoft para aumentar la percepción de confiabilidad.

---

4. Beneficios del Código Ético y la Comunicación Transparente

- **Fortalecimiento de la confianza:** Mejora la percepción de Hidrosoft como una empresa ética y responsable.
- **Cultura organizacional:** Fomenta un entorno donde la seguridad y la ética son prioridades compartidas.
- **Reducción de riesgos:** Minimiza el impacto de posibles incidentes al demostrar un compromiso proactivo con la seguridad y la transparencia.

5. Monitoreo Continuo y Auditorías de Seguridad

El monitoreo continuo es una de las prácticas más efectivas para detectar y mitigar los riesgos de seguridad antes de que se conviertan en incidentes graves. Para Hidrosoft, se recomienda establecer un programa robusto de monitoreo que detecte accesos no autorizados, ataques cibernéticos y anomalías en los sistemas. Este programa debe estar basado en los siguientes componentes clave:

1. Monitoreo Continuo

El monitoreo continuo implica la vigilancia activa de los sistemas y redes para identificar actividades sospechosas o anomalías. Esto incluye:

Herramientas de Monitoreo

- **Sistemas de Detección y Prevención de Intrusos (IDS/IPS):** Implementar herramientas que detecten y respondan a actividades sospechosas automáticamente.
- **Análisis de comportamiento del usuario y la entidad (UEBA):** Utilizar soluciones basadas en inteligencia artificial para identificar patrones inusuales en el comportamiento de usuarios o dispositivos.
- **Paneles de control en tiempo real:** Configurar dashboards que muestren alertas, métricas de rendimiento y eventos de seguridad en tiempo real.

Acciones de Monitoreo

- **Alertas proactivas:** Configurar notificaciones automáticas para incidentes como intentos de acceso no autorizado, cambios en configuraciones críticas o transferencia de datos sensibles.
- **Pruebas de estrés y simulación:** Realizar pruebas regulares para evaluar la capacidad de los sistemas de soportar ataques o picos inusuales de tráfico.
- **Supervisión 24/7:** Asegurar que haya personal o sistemas automatizados supervisando la infraestructura todo el tiempo.

---

2. Auditorías de Seguridad

Las auditorías proporcionan una revisión sistemática y detallada de los sistemas de seguridad para identificar vulnerabilidades y garantizar el cumplimiento normativo.

Tipos de Auditorías

- **Auditorías internas:**
  - Realizadas por el equipo de TI o ciberseguridad de Hidrosoft.
  - Enfocadas en revisar el cumplimiento de las políticas internas de seguridad.
- **Auditorías externas:**
  - Llevadas a cabo por expertos o terceros independientes.

    - Útiles para identificar problemas que podrían ser pasados por alto internamente.
- **Auditorías de cumplimiento:**
    - Evaluar el alineamiento con normativas como la Ley Orgánica de Protección de Datos Personales o estándares internacionales como ISO 27001.

Elementos Clave en una Auditoría

- **Evaluación de vulnerabilidades:** Identificar sistemas, redes o aplicaciones que presenten puntos débiles.
- **Pruebas de penetración:** Simular ataques controlados para medir la efectividad de las defensas existentes.
- **Revisión de permisos y accesos:** Verificar que los niveles de acceso de los empleados estén alineados con sus roles.
- **Análisis de políticas y procedimientos:** Evaluar si las políticas de seguridad son adecuadas, están actualizadas y son cumplidas.

---

3. Reportes y Acciones Correctivas

- **Documentación de hallazgos:** Registrar todas las vulnerabilidades detectadas y las áreas de mejora en un informe detallado.
- **Plan de acción:** Establecer un cronograma para resolver las vulnerabilidades críticas y reforzar los puntos débiles identificados.
- **Revisión periódica:** Realizar auditorías de seguimiento para garantizar que las acciones correctivas han sido implementadas correctamente.

---

4. Beneficios del Monitoreo Continuo y Auditorías

- **Identificación temprana:** Detectar amenazas antes de que puedan causar daños significativos.
- **Mejora continua:** Ajustar y fortalecer las defensas en función de los hallazgos.
- **Cumplimiento normativo:** Garantizar el cumplimiento de las regulaciones locales e internacionales.
- **Confianza organizacional:** Incrementar la confianza de clientes y empleados al demostrar un compromiso constante con la seguridad.

Conclusión

El Plan de Mitigación de Riesgos tiene un enfoque estratégico y práctico para abordar las vulnerabilidades de Hidrosoft frente a ataques de ingeniería social. Este plan incluye una combinación de medidas técnicas, educativas y organizacionales diseñadas para reforzar la seguridad y crear una cultura de ciberseguridad sólida dentro de la empresa.

Beneficios Clave de la Implementación:

1. **Fortalecimiento de la Seguridad:** La implementación de controles como la **autenticación multifactorial (MFA)** y el monitoreo continuo reducirá significativamente las posibilidades de acceso no autorizado.
2. **Protección de Datos Sensibles:** Salvaguardar la información confidencial de clientes y empleados es fundamental para cumplir con las normativas legales y mantener la confianza.
3. **Resiliencia Organizacional:** Las capacitaciones periódicas y las simulaciones de phishing aumentarán la capacidad de respuesta ante intentos de ataque, reduciendo errores humanos.
4. **Cumplimiento Normativo y Ético:** La creación de un **Código Ético** garantiza que las políticas de seguridad estén alineadas con las mejores prácticas y principios éticos.

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

ANEXO G : MARCO NORMATIVO Y REFERENCIAS LEGALES

Objetivo: Este anexo tiene como propósito detallar las leyes y regulaciones clave que rigen la protección de datos en Ecuador y su impacto directo en la gestión de la seguridad en Hidrosoft. A través de un análisis de las normativas aplicables, se presentarán los marcos legales bajo los cuales la empresa debe operar para garantizar la seguridad de los datos personales y el cumplimiento de las mejores prácticas en protección de la información.

1. Ley Orgánica de Protección de Datos Personales (LOPDP, Ecuador 2021)

Descripción:

La Ley Orgánica de Protección de Datos Personales (LOPDP) establece un marco legal para la gestión y protección de datos personales en Ecuador. Su propósito principal es garantizar el respeto a los derechos fundamentales de privacidad, confidencialidad y acceso a la información de los ciudadanos, adaptándose a las mejores prácticas internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea.

Objetivo:

- Proteger los datos personales de ciudadanos, asegurando que su tratamiento se realice de manera ética, legal y segura.
- Otorgar control a los titulares sobre el uso y tratamiento de sus datos.

Requisitos Clave:

1. **Consentimiento informado:**
    - Los datos personales solo pueden ser tratados previa autorización explícita del titular, quien debe ser informado del propósito, duración y condiciones de uso de sus datos (LOPDP, Art. 7).

- Es obligatorio obtener un consentimiento claro y verificable, especialmente en casos de datos sensibles.

2. **Derechos del titular de datos:**
   - Garantiza el derecho de los titulares a:
     - **Acceso:** Solicitar información sobre qué datos personales se almacenan y cómo se están utilizando (LOPDP, Art. 13).
     - **Rectificación:** Corregir datos incorrectos, inexactos o desactualizados (LOPDP, Art. 14).
     - **Oposición:** Rechazar el uso de sus datos para ciertos fines (LOPDP, Art. 15).
     - **Eliminación:** Solicitar la supresión de datos cuando ya no sean necesarios o se hayan usado de manera indebida (LOPDP, Art. 16).
   - Estos derechos deben ser atendidos por los responsables del tratamiento en plazos específicos.

3. **Seguridad de los datos:**
   - Obliga a las empresas a implementar medidas técnicas y organizacionales adecuadas para prevenir:
     - Accesos no autorizados.
     - Pérdidas, alteraciones o destrucción de datos personales (LOPDP, Art. 35).
   - Requiere la adopción de estándares como el cifrado, autenticación multifactorial y análisis de vulnerabilidades.

4. **Notificación de brechas:**
   - En caso de incidentes de seguridad que comprometan los datos personales, es obligatorio:
     - Informar a las autoridades reguladoras dentro de 72 horas.

- Notificar a los titulares afectados con información clara sobre el incidente y medidas adoptadas para mitigarlo (LOPDP, Art. 38).

5. **Transferencia internacional de datos:**
    - Los datos personales solo pueden ser transferidos fuera de Ecuador si el país receptor garantiza un nivel de protección equivalente o superior al de la LOPDP (LOPDP, Art. 45).

Impacto en Hidrosoft:

1. **Implementación de controles robustos:**
    - Hidrosoft debe:
        - Adoptar soluciones tecnológicas avanzadas como cifrado de extremo a extremo y autenticación multifactorial.
        - Realizar auditorías regulares de seguridad para detectar y corregir vulnerabilidades.

2. **Capacitación del personal:**
    - Es necesario sensibilizar y capacitar a todos los empleados sobre:
        - La importancia de proteger los datos personales.
        - Cómo manejar solicitudes de acceso, rectificación, oposición y eliminación de datos.
    - Implementar simulaciones de incidentes para medir la preparación del personal.

3. **Establecimiento de procesos claros:**
    - Hidrosoft debe diseñar procedimientos internos específicos para atender las solicitudes de los titulares de datos, cumpliendo con los plazos establecidos por la ley.
    - Desarrollar protocolos para gestionar incidentes de seguridad, asegurando una respuesta rápida y efectiva.

4. **Relación con clientes y terceros:**
    - Garantizar que los contratos con proveedores y socios comerciales incluyan cláusulas que exijan el cumplimiento de la LOPDP.
    - Comunicar de manera transparente a los clientes las medidas implementadas para proteger sus datos.

2. Reglamento sobre la Protección de Datos Personales (2022)

Descripción:

El Reglamento sobre la Protección de Datos Personales complementa la Ley Orgánica de Protección de Datos Personales (LOPDP) al detallar los requisitos técnicos y operativos necesarios para garantizar la protección de datos sensibles. Este reglamento proporciona lineamientos específicos que ayudan a las organizaciones a implementar medidas efectivas para proteger la información y cumplir con las normativas vigentes.

Elementos Clave:

1. **Protección de datos sensibles:**
    - Exige medidas adicionales para salvaguardar información crítica, como:
        - Datos relacionados con la salud.
        - Información financiera.
        - Datos biométricos y otros de alta sensibilidad.
    - Promueve el uso de tecnologías avanzadas como cifrado, autenticación multifactorial y controles de acceso estrictos para minimizar riesgos.

2. **Evaluaciones de impacto:**
    - Obliga a las empresas a realizar análisis periódicos sobre los riesgos asociados al tratamiento de datos personales (Reglamento, Art. 10).
    - Estas evaluaciones deben:
        - Identificar vulnerabilidades en los sistemas y procesos.

- Proponer medidas correctivas específicas.
- Ser documentadas como evidencia de cumplimiento normativo.

3. **Responsable de Protección de Datos (DPO):**
    - Establece la obligación de designar un delegado de Protección de Datos (DPO) con las siguientes responsabilidades:
        - Supervisar el cumplimiento de las normativas internas y externas relacionadas con la protección de datos.
        - Actuar como punto de contacto entre la organización y las autoridades regulatorias.
        - Garantizar que las políticas internas sean consistentes con las disposiciones del reglamento.

Impacto en Hidrosoft:

1. **Evaluaciones periódicas de impacto:**
    - Realizar análisis de riesgos al menos una vez al año para identificar vulnerabilidades y validar la eficacia de las medidas de seguridad.
    - Documentar los resultados de estas evaluaciones y diseñar planes de acción para mitigar riesgos detectados.

2. **Asignación de un DPO:**
    - Designar un delegado de Protección de Datos con las competencias necesarias para:
        - Supervisar prácticas internas relacionadas con la gestión de datos personales.
        - Asistir en consultas legales y regulatorias, fortaleciendo la relación con las autoridades competentes.
        - Garantizar que las políticas y procesos de Hidrosoft estén alineados con el reglamento.

3. **Revisión de políticas:**
    - Actualizar continuamente las políticas de privacidad y seguridad en función de cambios normativos, avances tecnológicos y mejores prácticas internacionales.
    - Establecer procedimientos claros para la gestión del tratamiento, acceso y eliminación de datos sensibles.

3. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2018)

Descripción:

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos regula el uso de tecnologías digitales para realizar transacciones electrónicas de manera segura. Su objetivo es asegurar la autenticidad, integridad y confidencialidad de la información transmitida por medios digitales, proporcionando un marco legal para el comercio electrónico en Ecuador.

Requisitos Clave:

1. **Uso de mecanismos seguros:**
    - Establece la obligatoriedad de emplear herramientas tecnológicas que garanticen la seguridad de las transacciones electrónicas.
    - Requiere la implementación de:
        - **Cifrado de datos** para proteger la información transmitida en las transacciones.
        - **Autenticación** para verificar la identidad de las partes involucradas.

2. **Validez legal de firmas electrónicas:**
    - Reconoce las firmas electrónicas como equivalentes legales de las firmas manuscritas, siempre que cumplan con los requisitos técnicos establecidos en la ley (Art. 13).
    - Las firmas electrónicas deben ser verificables y garantizar la autenticidad del firmante y la integridad del documento.

3. **Protección de mensajes de datos:**
    - Garantiza la validez y la admisibilidad como prueba en procedimientos legales de los mensajes de datos siempre que se demuestre su autenticidad e integridad (Art. 12).

Impacto en Hidrosoft:

1. **Transacciones electrónicas seguras:**
    - Hidrosoft debe implementar herramientas tecnológicas que aseguren:
        - La confidencialidad y autenticidad de las transacciones realizadas con clientes, proveedores y socios.
        - La protección de los datos transmitidos mediante técnicas de cifrado y autenticación.

2. **Gestión de firmas electrónicas:**
    - Incorporar sistemas de gestión de firmas electrónicas que cumplan con los estándares legales establecidos por la normativa.
    - Asegurar la capacitación del personal en el uso correcto de estas herramientas y su integración en procesos internos.

3. **Protección de datos en mensajes electrónicos:**
    - Establecer políticas internas que garanticen la integridad de los mensajes de datos enviados o recibidos.
    - Implementar soluciones tecnológicas para archivar, autenticar y verificar la integridad de los mensajes electrónicos.

4.ISO/IEC 27001: Estándar Internacional para la Gestión de la Seguridad de la Información

Descripción:

La norma ISO/IEC 27001 es un estándar internacional reconocido para la gestión de la seguridad de la información. Proporciona un marco sistemático para proteger la confidencialidad, integridad y disponibilidad de la información, ayudando a las organizaciones a identificar, gestionar y reducir riesgos de seguridad.

Objetivo:

- Establecer un Sistema de Gestión de Seguridad de la Información (SGSI) que permita a las organizaciones proteger la información de manera eficiente y conforme a las mejores prácticas internacionales.
- Garantizar la continuidad del negocio mediante la identificación y mitigación de riesgos asociados a la seguridad de la información.

Elementos Clave:

1. **Política de Seguridad de la Información:**
    - Definir políticas claras y accesibles que guíen la gestión de la seguridad en la organización (ISO/IEC 27001, Cláusula 5).

2. **Gestión de Riesgos:**
    - Realizar análisis regulares para identificar riesgos potenciales en los procesos, sistemas y datos.
    - Implementar medidas preventivas y correctivas basadas en estos análisis (Cláusula 6).
3. **Controles de Seguridad:**
    - Aplicar controles técnicos y organizacionales definidos en el Anexo C del estándar, como:
        - **Control de accesos.**
        - **Gestión de incidentes de seguridad.**

- **Cifrado y protección de datos.**
- **Capacitación y concienciación en seguridad.**

4. **Auditorías Internas y Certificación:**
    - Realizar auditorías periódicas para evaluar la eficacia del SGSI.
    - Obtener la certificación ISO/IEC 27001 mediante auditores externos como evidencia de conformidad con el estándar.

Impacto en Hidrosoft:

1. **Establecimiento de un SGSI:**
    - Hidrosoft debe implementar un Sistema de Gestión de Seguridad de la Información que abarque:
        - Políticas y procedimientos claros para la gestión de datos sensibles.
        - Evaluación continua de riesgos y ajustes en los controles de seguridad.

2. **Conformidad con estándares globales:**
    - Seguir los lineamientos de ISO/IEC 27001 mejora la capacidad de Hidrosoft para proteger su información y cumplir con normativas locales, como la LOPDP y el Reglamento de Protección de Datos.

3. **Mejor reputación y confianza:**
    - La certificación ISO/IEC 27001 incrementa la confianza de clientes y socios, mostrando el compromiso de Hidrosoft con la seguridad de la información.

4. **Preparación ante incidentes:**
    - Fortalecer los protocolos de respuesta a incidentes y garantizar la continuidad operativa ante posibles ciberataques o fallas de seguridad.

5. Importancia del Cumplimiento Normativo en Hidrosoft

Cumplir con las leyes y normativas relacionadas con la protección de datos y la ciberseguridad no solo es una obligación legal, sino también un componente clave para garantizar el éxito y la sostenibilidad de Hidrosoft. Los principales beneficios incluyen:

1. Reputación Organizacional

- El cumplimiento normativo fortalece la confianza de clientes y socios al demostrar un compromiso con la protección de datos personales.
- Una empresa alineada con estándares legales e internacionales proyecta una imagen de responsabilidad y profesionalismo.
- Refuerza la percepción de Hidrosoft como una organización ética y confiable en el manejo de información sensible.

2. Evitar Sanciones

- El incumplimiento puede acarrear multas significativas que afecten las finanzas de la empresa.
- Las sanciones legales pueden incluir restricciones operativas, pérdida de contratos o auditorías obligatorias que afecten la continuidad del negocio.
- Además de las consecuencias económicas, una infracción puede ocasionar daño irreparable a la reputación de la empresa.

3. Gestión Ética de Datos

- Cumplir con las normativas promueve prácticas responsables y éticas en la gestión de la información.
- Refuerza una cultura organizacional basada en la protección de los derechos de los titulares de datos.
- Asegura que Hidrosoft opere de manera alineada con principios fundamentales como la privacidad, transparencia e integridad.

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

ANEXO H: PLANTILLAS DE POLÍTICAS DE SEGURIDAD

1. POLÍTICA DE CONTRASEÑAS

1.1. Propósito

Establecer lineamientos para la creación, uso, administración y protección de contraseñas con el fin de salvaguardar el acceso a los sistemas y la información sensible de la organización.

1.2. Alcance

Esta política aplica a todos los empleados, colaboradores externos, contratistas y cualquier persona que acceda a los sistemas, redes y aplicaciones de la empresa.

1.3. Lineamientos Generales

Longitud y Complejidad

Las contraseñas deben tener una longitud mínima de 8 caracteres.

Deben incluir al menos un carácter en mayúscula, un carácter en minúscula, un número y un símbolo especial (p. ej., `! @ # $ %`).

Se prohíbe el uso de contraseñas comunes o triviales como “123456”, “password”, “qwerty”, etc.

Cambio Periódico de Contraseña

Las contraseñas deben cambiarse cada 90 días.

No se pueden reutilizar las últimas 3 contraseñas (historial de contraseñas).

Almacenamiento y Compartición

Las contraseñas no deben escribirse en lugares visibles (post-its, hojas de papel, etc.).

Se recomienda el uso de un gestor de contraseñas seguro para su almacenamiento en caso de ser necesario.

Las credenciales de acceso son personales e intransferibles; está prohibido compartirlas con otros empleados o externos.

Bloqueo de Cuenta

Se activará el bloqueo de cuenta tras un número determinado de intentos fallidos de inicio de sesión (por ejemplo, 5 intentos).

Para desbloquear una cuenta, se requerirá la verificación de identidad según los procedimientos establecidos por TI.

2. POLÍTICA DE USO DE CORREO ELECTRÓNICO

2.1. Propósito

Asegurar el uso adecuado y seguro del correo electrónico corporativo para proteger la información de la empresa y mantener la confidencialidad, integridad y disponibilidad de los datos.

2.2. Alcance

Esta política es de aplicación para todos los usuarios que dispongan de una cuenta de correo electrónico corporativa, incluyendo empleados, consultores y personal externo autorizado.

2.3. Lineamientos Generales

Uso Adecuado

El correo electrónico corporativo debe utilizarse principalmente para actividades relacionadas con la empresa.
Se desaconseja el uso de la cuenta de correo corporativo para fines personales que no estén relacionados con el desempeño laboral.

Confidencialidad y Clasificación de la Información

No se debe enviar información sensible o clasificada sin cifrar (en caso de existir medios de cifrado disponibles).
Verificar que el destinatario sea correcto antes de enviar información confidencial.

Protección contra Phishing y Malware

No abrir enlaces o descargar archivos adjuntos de correos sospechosos o remitentes desconocidos.
Reportar de forma inmediata a TI cualquier mensaje que parezca malicioso (phishing, spam, etc.).

Restricciones Adicionales

De acuerdo con la política de HIDROSOFT:
No se permite el envío de cadenas de mensajes de tipo comercial, político, religioso, o que contengan contenido discriminatorio o pornográfico.
Los usuarios deben respetar las normas de tamaño de adjuntos y formato corporativo definido por el CSI.

3. POLÍTICA DE USO DE DISPOSITIVOS MÓVILES

3.1. Propósito

Regular el uso y la seguridad de los dispositivos móviles (teléfonos, tablets, laptops) que acceden a la red y a los datos corporativos, para proteger la información institucional.

3.2. Alcance

Esta política aplica a todo dispositivo móvil (propiedad de la empresa o personal, bajo un esquema de BYOD — Bring Your Own Device) que acceda a sistemas y datos de la organización.

3.3. Lineamientos Generales

Control de Acceso

Todos los dispositivos deben contar con métodos de bloqueo seguros (contraseña, PIN, biometría).
Debe habilitarse el cifrado de datos siempre que el dispositivo y el sistema operativo lo permitan.

Uso Apropiado de Aplicaciones

Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; solo se deben instalar aplicaciones desde repositorios oficiales.
Se desaconseja conectar dispositivos empresariales a redes públicas como cafeterías o aeropuertos.

Protección de Datos

Es obligatorio el uso de VPN (Virtual Private Network) o canales seguros para acceder a sistemas corporativos desde redes externas o públicas.
Los usuarios deben evitar almacenar información personal o no relacionada con el negocio en dispositivos empresariales.

Actualizaciones y Mantenimientos

Todos los dispositivos deben contar con el software y sistema operativo actualizados regularmente.
Los usuarios deben aceptar y aplicar las actualizaciones notificadas por el sistema.

4. POLÍTICAS DE SEGURIDAD COMPLEMENTARIAS

4.1. Política de uso adecuado de internet

- El acceso a internet se restringe exclusivamente para actividades laborales aprobadas por la organización.
- No está permitido visitar sitios web no relacionados con el trabajo, incluyendo plataformas de redes sociales, servicios de streaming o cualquier contenido prohibido.
- Los usuarios deben evitar descargar software o archivos no autorizados.

4.2. Política de intercambio de información

- Cualquier transferencia de información sensible debe realizarse mediante canales seguros y con las debidas autorizaciones.
- El intercambio de información confidencial con terceros debe estar respaldado por acuerdos de confidencialidad.

4.3. Política de protección frente a software malicioso

- Es obligatorio el uso de software antivirus y antimalware en todas las estaciones de trabajo y dispositivos móviles.
- Los usuarios deben reportar cualquier actividad sospechosa o intento de ataque a la Mesa de Ayuda de TI.

4.4. Política de seguridad para equipos empresariales

- Los dispositivos empresariales solo deben ser utilizados para actividades laborales y deben mantenerse bajo supervisión adecuada.
- Cualquier pérdida o robo de un dispositivo debe ser notificado inmediatamente al área de TI.

4.5. Política de copias de respaldo

- Todas las áreas deben garantizar que los datos críticos se respalden periódicamente en sistemas seguros.
- Los respaldos deben almacenarse en ubicaciones separadas y protegidas contra acceso no autorizado.

4.6. Política de cumplimiento con requisitos legales y contractuales

- Todos los usuarios y sistemas deben cumplir con la legislación vigente relacionada con la protección de datos, derechos de autor y licenciamiento de software.
- Es ilegal duplicar o distribuir software sin la autorización correspondiente del titular de los derechos.

4.7. Política de reporte y tratamiento de incidentes

- Cualquier incidente de seguridad, incluyendo accesos no autorizados o sospecha de malware, debe ser reportado inmediatamente al equipo de TI.
- Los incidentes serán investigados y se implementarán medidas correctivas para evitar su repetición.

OBSERVACIONES FINALES DEL ANEXO 1

- Las políticas compiladas integran medidas preventivas y correctivas alineadas con las mejores prácticas internacionales, como ISO 27001 y 27002.
- La implementación efectiva de estas políticas requiere un compromiso organizacional y capacitación constante de los empleados.
- Se recomienda realizar auditorías periódicas para evaluar el cumplimiento y la eficacia de las políticas.

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

ANEXO I: Cuestionario para Evaluar Recomendaciones Éticas y Estrategias de Ciberseguridad en Hidrosoft

Percepción de Políticas de Seguridad

¿Qué tan efectivas considera que son las políticas actuales de seguridad de la información para proteger los datos sensibles de la empresa?

- - Muy efectivas
- - Efectivas
- - Algo efectivas
- - Poco efectivas
- - Nada efectivas

¿Conoce las políticas relacionadas con el uso de dispositivos móviles y conexiones remotas?

- - Sí, y las aplico regularmente
- - Sí, pero no las aplico regularmente
- - No las conozco

¿Considera que las políticas de clasificación y manejo de la información son claras y fáciles de implementar?

- - Muy claras
- - Claras
- - Algo claras
- - Poco claras
- - Nada claras

Plan de Mitigación de Riesgos

¿Está de acuerdo con la implementación de la autenticación multifactorial (MFA) como medida de seguridad?

- - Totalmente de acuerdo
- - De acuerdo

- - Neutral
- - En desacuerdo
- - Totalmente en desacuerdo

¿Cómo calificaría la claridad y efectividad del plan de mitigación de riesgos propuesto en su área de trabajo?

- - Muy efectivo
- - Efectivo
- - Algo efectivo
- - Poco efectivo
- - Nada efectivo

Capacitación y Conciencia

¿Ha recibido capacitación sobre amenazas de ingeniería social en los últimos 12 meses?

- - Sí
- - No

¿Considera que las simulaciones de phishing realizadas han mejorado su capacidad para identificar y evitar ataques?

- - Mucho
- - Algo
- - Poco
- - Nada

¿Qué tan relevante considera que es la capacitación práctica sobre ciberseguridad para su desempeño diario?

- - Muy relevante
- - Relevante
- - Algo relevante
- - Poco relevante
- - Nada relevante

Responsabilidad y Ética

¿Se siente motivado para reportar incidentes de seguridad, incluso si han sido causados por un error humano?

- - Muy motivado
- - Motivado
- - Algo motivado
- - Poco motivado
- - Nada motivado

¿Qué tan claro considera que es el código ético relacionado con la ciberseguridad dentro de la empresa?

- - Muy claro
- - Claro
- - Algo claro
- - Poco claro
- - Nada claro

Sistemas de Respuesta a Incidentes

¿Cree que existen procedimientos claros y eficaces para manejar incidentes de seguridad en la empresa?

- - Muy claros y eficaces
- - Claros y eficaces
- - Algo claros y eficaces
- - Poco claros y eficaces
- - Nada claros y eficaces

¿Qué tan rápido considera que se responde a los incidentes reportados?

- - Muy rápido
- - Rápido
- - Algo rápido
- - Poco rápido
- - Nada rápido

Infraestructura y Controles

¿Qué tan satisfecho está con las herramientas tecnológicas proporcionadas para proteger la información (VPN, herramientas de cifrado)?

- - Muy satisfecho
- - Satisfecho
- - Algo satisfecho
- - Poco satisfecho
- - Nada satisfecho

¿Considera que los controles de acceso a la información son consistentes y justos?

- - Muy consistentes y justos
- - Consistentes y justos
- - Algo consistentes y justos
- - Poco consistentes y justos
- - Nada consistentes y justos

Cultura de Seguridad

¿Siente que la cultura organizacional fomenta una actitud proactiva hacia la seguridad de la información?

- - Totalmente de acuerdo
- - De acuerdo
- - Neutral
- - En desacuerdo
- - Totalmente en desacuerdo

¿Considera que la comunicación interna sobre riesgos y medidas de seguridad es adecuada y oportuna?

- - Muy adecuada y oportuna
- - Adecuada y oportuna
- - Algo adecuada y oportuna
- - Poco adecuada y oportuna
- - Nada adecuada y oportuna