UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICAS

CARRERA INGENIERÍA EN SISTEMAS

ESTUDIO DE CASO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

ING. EN SISTEMAS

TEMA:

ANÁLISIS DE SEGURIDAD INFORMÁTICA BAJO LOS ESTÁNDARES ISO 27001 EN LA NOTARÍA ÚNICA DEL CANTÓN ALFREDO BAQUERIZO MORENO.

AUTOR:

ELVIS ABEL HERRERA PALMA

RESUMEN

Este proyecto investigativo se realizó con el objetivo de analizar la seguridad de la informática basada en la norma ISO 27001 en la notaría del cantón Alfredo Baquerizo Moreno. El presente documento investigativo presentado, se desarrolló a través de la recopilación de todo tipo de información, realizando una detallada investigación en las distintas páginas web de libre acceso, artículos científicos, tesis de grado, fuentes y documentaciones bibliográficas disponibles en distintas plataformas digitales.

Los resultados del estudio sobre el análisis de seguridad informática bajo los estándares ISO 27001 en la notaría única del Cantón Alfredo Baquerizo Moreno, incluye el análisis de la implementación de estándares de seguridad lo cual ayudara a establecer políticas de seguridad adecuadas para el entorno de la Notaría Única del Cantón Alfredo Baquerizo Moreno, además de poder identificar oportunamente las amenazas y vulnerabilidades y tener un plan de acción para cualquier eventualidad que se presente en cuanto a la seguridad de la información.

Este proyecto de investigación contribuye a fortalecer la seguridad informática en la Notaría Única del Cantón Alfredo Baquerizo Moreno al analizar la implementación de estándares de seguridad, identificar amenazas y vulnerabilidades, y ofrecer un plan de acción. La seguridad de la información se ha convertido en un aspecto crítico para proteger datos sensibles en la era digital, y este estudio es un paso importante hacia una gestión más efectiva de la seguridad en esta entidad.

La línea de investigación en la cual se basa este estudio es desarrollo de sistemas de la información, comunicación y emprendimientos empresariales y tecnológicos basándose el análisis en la sub línea de investigación de procesos de transmisión de datos y telecomunicaciones.

Palabras Claves: Era digital, seguridad, técnicas, prevención de riesgos, tecnología y análisis.

SUMMARY

This research project was carried out with the aim of analyzing computer security based on the ISO 27001 standard at the notary office in the Alfredo Baquerizo Moreno canton. The present research document was developed through the collection of all types of information, conducting a detailed investigation on various freely accessible websites, scientific articles, graduate theses, sources, and bibliographic documentation available on different digital platforms.

The results of the study on the analysis of computer security under ISO 27001 standards at the unique notary office of the Alfredo Baquerizo Moreno canton include the analysis of the implementation of security standards, which will help establish appropriate security policies for the environment of the Unique Notary Office of the Alfredo Baquerizo Moreno canton, as well as being able to promptly identify threats and vulnerabilities and have an action plan for any eventualities related to information security.

This research project contributes to strengthening computer security at the Unique Notary Office of the Alfredo Baquerizo Moreno canton by analyzing the implementation of security standards, identifying threats and vulnerabilities, and providing an action plan. Information security has become a critical aspect for protecting sensitive data in the digital age, and this study is an important step toward more effective security management in this entity.

The line of research on which this study is based is the development of information systems, communication and business and technological ventures, calculating the analysis in the research subline of data transmission and telecommunications processes.

Keywords: Digital age, security, techniques, risk prevention, technology, and analysis.

INTRODUCCION

En la era digital actual, la seguridad de la información se ha convertido en un aspecto crítico para organizaciones de todas las dimensiones y sectores. La creciente dependencia de la tecnología y la interconexión de sistemas plantean desafíos significativos en términos de protección de datos sensibles y confidenciales. En este contexto, el presente estudio de caso se adentra en el análisis de seguridad informática bajo los estándares ISO 27001 en el entorno de la Notaría Única del Cantón Alfredo Baquerizo Moreno.

La digitalización de los procesos notariales ha simplificado muchas tareas, pero también ha introducido nuevas vulnerabilidades y riesgos. La adopción de estándares internacionales, como la norma ISO 27001, se ha vuelto esencial para garantizar un enfoque sistemático y efectivo en la gestión de la seguridad de la información.

Se mantuvo una reunión en Notaría Única del Cantón Alfredo Baquerizo Moreno con el propósito de introducir el tema de seguridad informática de tal manera que sus funcionarios sean conscientes de su importancia, ya que esta notaría desempeña un papel crucial en la legalización y autenticación de documentos y a medida que el flujo de datos electrónicos se ha vuelto indispensable en sus operaciones, la notaría se enfrenta a la tarea de evaluar y mejorar sus controles de seguridad informática.

La Notaría Única del cantón Alfredo Baquerizo Moreno ha asumido el desafío de mejorar sus prácticas de seguridad informática con el análisis propuesto el cual es necesario para identificar vulnerabilidades y proponer acciones correctivas que fortalezcan la seguridad de los datos, generando confianza en la organización y sus servicios.

El propósito de este caso de estudio es analizar la implementación de los estándares ISO 27001 en la Notaría Única del Cantón Alfredo Baquerizo Moreno y evaluar cómo estos estándares impactan en su postura de seguridad informática. Se busca identificar los puntos claves que enfrentaría la notaría en términos de seguridad de la información y examinar cómo la adopción de la norma ISO 27001 puede contribuir a fortalecer su infraestructura de seguridad.

Es importante destacar que este estudio de caso se centra exclusivamente en La Notaría Única del Cantón Alfredo Baquerizo Moreno y no pretende abarcar todas las complejidades de la seguridad informática del Consejo de la Judicatura el cual es el órgano del gobierno al cual se rige la notaría. Además, las recomendaciones ofrecidas estarán contextualizadas a la realidad y recursos de la notaría en cuestión.

Para el presente estudio de caso se usará metodologías descriptivas cualitativas en la cual obtendremos datos mediante encuestas realizadas al personal de la notaría. Esta metodología nos permitirá poder acercarnos a los métodos que maneja la institución en procesos de seguridad, así tambien se usarán metodologías inductivas para tomar un papel más activo en la investigacion por medio de observación y la práctica experimental.

DESARROLLO

La seguridad de la información es de vital importancia en el mundo globalizado, sobre todo para entidades públicas que manejan procedimientos con información confidencial como es el caso de la Notaría Única del Cantón Alfredo Baquerizo Moreno donde se realizan compraventa de bienes, donaciones, reportes al S.R.I y a la Unidad de Análisis Financiero y Económico, entre otros.

En el ámbito internacional se aplican distintas normas de seguridad de la información como la norma ISO 27001 la cual especifica una serie de requerimientos que la empresa debe cumplir para garantizar la seguridad de la información. Empresas como Microsoft se rigen a la norma ISO 27001.

En el ámbito nacional actualmente, se han visto muchos casos donde las empresas carecen de evaluación y mejora de los controles de seguridad existentes, lo cual pone en riesgo la protección de la información confidencial de sus usuarios.

El caso de estudio se aplica a la Notaria Única del Cantón Alfredo Baquerizo Moreno de esta forma se procede a revisar que normas de seguridad aplica con respecto a la información, teniendo en cuenta que existen normas como las ISO 27001 que permiten garantizar seguridad en la misma.

Entre las funciones y procesos principales de la notaría están la protocolización de documentos, compraventas de bienes, elaboración de reportes financieros al SRI y a la Unidad de Análisis Financiero y Económico entre otros. Estos procesos incluyen información confidencial tanto de los usuarios como de la Notaría.

Justificación

La notaría del canto Alfredo Baquerizo Moreno tiene entre sus actividades y responsabilidades verificar la autenticidad de las firmas y sellos en los documentos presentados por los usuarios, lo cual garantiza la validez legal de los documentos y previene la falsificación; la notaría está obligada a mantener la confidencialidad de la información proporcionada por los usuarios. Esto es crucial para proteger la privacidad y la seguridad de las partes involucradas.

La notaría debe cumplir con las leyes y regulaciones en materia de seguridad de la información, y este análisis de seguridad de la información bajo la norma ISO 27001 es una forma efectiva de evaluar el grado de cumplimiento e identificar áreas de mejora.

Iso

ISO es la sigla de la Organización Internacional de Normalización (en inglés, International Organization for Standardization). La ISO es una organización internacional independiente que desarrolla y publica estándares para una amplia variedad de industrias y sectores en todo el mundo. Estos estándares están diseñados para garantizar la calidad, seguridad y eficiencia de productos, servicios y sistemas, y para facilitar el comercio internacional al estandarizar procesos y requisitos.

La ISO trabaja en estrecha colaboración con organizaciones nacionales de normalización de diferentes países para desarrollar y mantener estos estándares. Los estándares ISO son voluntarios, lo que significa que las organizaciones pueden optar por adoptarlos y cumplir con ellos para mejorar sus procesos y productos, demostrando así su compromiso con la calidad y la excelencia.

En resumen, ISO desarrolla estándares internacionales para promover la calidad, la seguridad y la eficiencia en una amplia variedad de industrias y sectores en todo el mundo.

Iso 27001

ISO 27001 representa una normativa de alcance global que se enfoca en la seguridad de la información. Esta norma fue concebida por la Organización Internacional de Normalización (ISO) con el propósito de establecer un modelo organizado y uniforme para gestionar la seguridad de la información en diversas entidades. El estándar

ISO 27001 plantea un método completo para reconocer, evaluar y administrar los riesgos relacionados con la seguridad de la información, además de establecer exigencias y medidas de control destinadas a salvaguardar el activo más valioso, el cual es la información.

Watkins (2017) menciona que, la norma ISO 27001 se aplica a cualquier tipo de organización, incluyendo pequeñas y medianas empresas, grandes corporaciones, instituciones gubernamentales y sin fines de lucro. También se puede aplicar en cualquier sector, incluyendo tecnología de la información, finanzas, salud y servicios públicos.

La norma ISO 27001 busca asegurar 3 aspectos importantes para la seguridad de la información las cuales son disponibilidad, integridad y confidencialidad de la misma.

Disponibilidad

La disponibilidad implica que la información esté disponible para la persona u organización autorizada en el momento en el que la requiera.

Las empresas y organizaciones necesitan tener disponible la información para poder ejercer sus funciones y brindar sus servicios.

Integridad

La integridad de la información se refiere a que los datos deben ser íntegros en su totalidad, sin ningún tipo de manipulación que los altere por ningún motivo o propósito.

Confidencialidad

La confidencialidad implica que la información debe estar disponible solo para personas autorizadas de la organización y además dichas personas no pueden compartir, difundir o divulgar la información la cual es de carácter privado a terceros.

Sistema de Gestión de Seguridad de la Información (SGSI)

Un Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto de políticas, procedimientos, prácticas y tecnologías diseñadas y aplicadas por una organización para gestionar y proteger de manera efectiva la seguridad de la información. El objetivo principal de un SGSI es garantizar la confidencialidad, la integridad y la disponibilidad de la información sensible y crítica de la organización, así como gestionar los riesgos relacionados con la seguridad de la información de manera sistemática y coherente (Chicaiza, 2018).

Un SGSI se basa en un marco de estándares y directrices que ayudan a la organización a establecer, implementar, supervisar, revisar y mejorar continuamente sus prácticas de seguridad de la información. Uno de los estándares más conocidos relacionados con los SGSI es la norma ISO 27001, que proporciona una estructura y un conjunto de requisitos para la implementación de un SGSI efectivo.

Elementos claves de un SGSI

Política de Seguridad de la Información. Define los principios y objetivos generales de seguridad de la información de la organización.

Identificación de Activos. Enumera y clasifica los activos de información críticos de la organización.

Evaluación de Riesgos. Identifica y evalúa los riesgos de seguridad de la información asociados con esos activos.

Controles de Seguridad. Define medidas y controles específicos para mitigar los riesgos identificados.

Procedimientos Operativos. Establece procedimientos y directrices para el personal en relación con la seguridad de la información.

Concienciación y Formación. Asegura que el personal esté capacitado y consciente de las políticas y prácticas de seguridad.

Gestión de Incidentes de Seguridad. Establece un proceso para identificar, gestionar y responder a incidentes de seguridad de la información.

Revisión y Mejora Continua. Evalúa y mejora regularmente el SGSI para garantizar su eficacia y relevancia.

Auditorías y Revisiones. Realiza auditorías internas y revisiones periódicas para garantizar el cumplimiento de las políticas y controles de seguridad.

Un SGSI es esencial para proteger la información confidencial, cumplir con regulaciones de seguridad de la información y mantener la confianza de los clientes y socios

comerciales. Ayuda a las organizaciones a gestionar los riesgos de seguridad de la información de manera sistemática y garantiza una respuesta adecuada a las amenazas y los incidentes de seguridad.

Ciberseguridad

Según la página web de la empresa Kaspersky, la ciberseguridad implica salvaguardar sistemas informáticos, servidores, dispositivos móviles, equipos electrónicos, redes y datos contra ataques maliciosos. Se refiere también como seguridad de la tecnología de la información o seguridad de la información electrónica (AO Kaspersky Lab, 2023).

Este concepto es relevante en diversos ámbitos, que abarcan desde el entorno empresarial hasta la computación móvil, y puede clasificarse en varias categorías como lo son:

- Seguridad de Red
- Seguridad de aplicaciones
- Seguridad de la información
- Seguridad Operativa
- Recuperación ante desastres y continuidad de negocio
- Capacitación del Usuario final

Todos los puntos anteriores son de vital importancia para la ciberseguridad. En este caso, haremos énfasis en la categoría de seguridad de la información para el desarrollo de este trabajo.

Importancia De La Seguridad De La Información

La información representa el recurso primordial para el funcionamiento de las empresas y la ejecución de las actividades comerciales. Esto conlleva a la necesidad imperante de salvaguardar la información como el recurso más valioso de la entidad. En la actualidad, debido al crecimiento exponencial de la utilización de internet, el avance constante de la tecnología y la falta de conocimiento en la mitigación de riesgos cibernéticos, se han originado numerosas amenazas que explotan debilidades en las estructuras empresariales.

Esto da lugar a la concreción de riesgos que pueden tener un impacto adverso en las organizaciones, provocando la pérdida de una o más de las características esenciales que la información debe conservar las cuales son: disponibilidad, integridad y confidencialidad.

La compañía internacional Kaspersky la cual se dedicada a la seguridad informática con presencia en aproximadamente 195 países del mundo realizó un análisis de los ataques informáticos en el último año y conforme a este análisis de especialistas se determinó que hubo un incremento en los ataques de ciberseguridad en los últimos 2 años frente a periodos pasados. Esta cifra denota un aumento del 617% en comparación con el año previo, equivalente a un promedio de 544 ataques por minuto.

Según Valenzuela y Quijada (2016), El incremento de estos ataques en la región se atribuye principalmente al restablecimiento de las operaciones económicas tras la pandemia. Este fenómeno se ve agravado por la introducción de herramientas impulsadas por Inteligencia Artificial que posibilitan la generación automatizada de contenidos para uso fraudulento. En su totalidad, Kaspersky ha documentado 286 millones de bloqueos de intentos de suplantación

en los últimos 12 meses de los cuales a Ecuador le corresponden 12,2 millones entrando así en el top de países con más ataques en América Latina.

Según Pontiroli (2019), analista de seguridad en Kasperksy, las malas prácticas de las empresas y entidades gubernamentales permiten que el ransomware sea una amenaza real menciona lo siguiente.

"Prácticamente, 2 de cada 3 dispositivos en América Latina tienen vulnerabilidades críticas. Según nuestros datos, el 55% de las computadoras en la región todavía usan Windows 7 y el 5% Windows XP. Sin embargo, lo más aterrador es que la tasa de software pirateado es del 66%*, casi el doble de la tasa promedio mundial de 35%", comenta Pontiroli.

Ataques más comunes

Los ataques informáticos más comunes varían con el tiempo y evolucionan a medida que la tecnología y las prácticas de seguridad se desarrollan. Sin embargo, algunos de los ataques informáticos más comunes que han sido persistentes a lo largo de los años incluyen:

Malware

Esta categoría incluye programas con códigos maliciosos los cuales fueron diseñados para infiltrarse en sistemas y causar daño y robar información.

Todo comienza desde la Infección del dispositivo, por lo general luego de descargar software malicioso involuntariamente, por lo general desde enlaces infectados, o al visitar un sitio web infectado. Según un artículo publicado en la página web de la empresa Avast, nos indica que:

> "El hackeo y el malware van de la mano. El hackeo informático consiste en obtener acceso no autorizado a un dispositivo o red, y por lo general se hace mediante

código malicioso. Además, el código fuente del malware está disponible en la dark web, por lo que hasta los ciberdelincuentes menos habilidosos lo pueden conseguir fácilmente" (Ivan, 2023,parrafo 10).

Existen muchos tipos de malware, pero en cuanto al peligro que representan para la seguridad de la información podemos mencionar especialmente a aquellos que interrumpen la disponibilidad de la información, la integridad y la confidencialidad de la misma.

Spyware

El spyware es un tipo de software malicioso (malware) diseñado para recopilar información personal o confidencial de un dispositivo sin el conocimiento o el consentimiento del usuario. El término "spyware" proviene de la combinación de las palabras "spy" (espía) y "software" (programa informático), lo que refleja su propósito de espiar o vigilar de manera encubierta.

El spyware pone en riesgo la información puesto que la misma puede ser descubierta, poniendo en riesgo la confidencialidad, disponibilidad e integridad de la información.

Las principales funciones del Spyware son:

Recopilación de datos: El spyware se instala en un dispositivo sin que el usuario lo sepa y comienza a recopilar información. Esto puede incluir registros de pulsaciones de teclas, contraseñas, historiales de navegación, detalles de tarjetas de crédito y otra información personal.

Envío de datos: Una vez que ha recopilado datos, el spyware los envía de manera encubierta a un servidor remoto controlado por el atacante.

Falta de consentimiento: La característica distintiva del spyware es que opera sin el consentimiento o el conocimiento del usuario. Por lo general, se instala junto con otros programas o se oculta en sitios web maliciosos, correos electrónicos o descargas.

Propósitos maliciosos: El spyware se utiliza para diversos fines maliciosos, que pueden incluir robo de identidad, fraude financiero, seguimiento de actividades en línea, publicidad invasiva y más.

Ransomware

Ransomware es un tipo de malware o software malicioso cuya función es el cifrado de la información del equipo infectado con el propósito de pedir a la víctima un rescate de la información generalmente a cambio de grandes sumas de dinero.

Su nombre proviene de las palabras "ransom" (rescate) y "software" (programa informático), ya que implica el secuestro de datos y la demanda de un rescate económico a cambio de su liberación.

En esencia, el ransomware es un tipo de malware diseñado para cifrar los archivos o sistemas de una víctima de manera que no puedan ser accedidos o utilizados sin una clave de descifrado. Una vez que el ransomware ha infiltrado un dispositivo o red, muestra un mensaje de rescate en la pantalla de la víctima, generalmente solicitando un pago a cambio de realizar el descifrado necesario para recuperar los archivos.

Existen varias formas en que el ransomware puede ingresar a un sistema. El más común es a través de correos electrónicos, donde los delincuentes envían mensajes engañosos que persuaden a los destinatarios a abrir un archivo adjunto o hacer clic en un enlace malicioso. Una vez que se ejecuta el ransomware, comienza a cifrar los archivos de la víctima

y, a menudo, se muestra una cuenta regresiva que aumenta la presión sobre la víctima para que pague el rescate.

El ransomware ha evolucionado con el tiempo y ha adquirido diversas variantes y tácticas. Algunos tipos populares incluyen Locky, WannaCry, Petya, Cryptolocker, Ryuk, entre otros. Además, los atacantes suelen amenazar con eliminar permanentemente los archivos cifrados si no se paga el rescate en un plazo determinado, lo que aumenta la urgencia y el temor de las víctimas.

El impacto del ransomware puede ser devastador. Las empresas pueden perder acceso a datos cruciales, lo que puede paralizar sus operaciones y causar pérdidas financieras significativas. Además, pagar el rescate no garantiza que los delincuentes cumplan su parte del trato y proporcionen la clave de descifrado. Además, el pago de rescates a menudo financia actividades criminales adicionales.

Phishing

El ataque de phishing tiene como principal objetivo el envío masivo de correos electrónicos a una empresa o entidad. Estos correos electrónicos son diseñados para parecer que provienen de fuentes confiables, como entidades bancarias legítimas, aunque en realidad son fraudulentos. El propósito detrás de estos correos electrónicos es engañar al usuario o víctima para que revele información confidencial, que luego se utiliza con fines fraudulentos, como beneficio personal o la venta de datos robados en la deep web.

Para lograr esto, los correos de phishing a menudo contienen enlaces que, cuando se hacen clic, redirigen a las víctimas a sitios web falsificados que imitan a sitios de confianza. En estos sitios falsificados, los usuarios pueden ser inducidos a proporcionar información

sensible, como contraseñas, números de tarjeta de crédito o información bancaria. Sin embargo, en lugar de ir a las entidades legítimas, esta información termina en manos del estafador, quien la utiliza para sus propios fines fraudulentos.

> "El phishing es un término que se usa para describir una de las tácticas más comunes empleadas por criminales cibernéticos con el propósito de estafar y obtener información confidencial de manera fraudulenta. Esta información sensible puede abarcar desde contraseñas hasta detalles completos de tarjetas de crédito o datos bancarios de la persona afectada" (Monsalve, 2018,p.3).

Ataques de Ingeniería Social

Un ataque de ingeniería social es una estrategia sofisticada y manipuladora utilizada por individuos o grupos malintencionados para obtener información confidencial, acceso no autorizado a sistemas, o persuadir a las víctimas para que realicen acciones perjudiciales. En lugar de explotar vulnerabilidades técnicas, como en los ataques informáticos convencionales, la ingeniería social se basa en la explotación de aspectos psicológicos, emocionales y sociales de las personas. Los perpetradores de estos ataques aprovechan la confianza, la empatía, el miedo, la curiosidad y otros impulsos humanos para lograr sus objetivos.

Los ataques de ingeniería social pueden adoptar diversas formas, desde el contacto en persona o telefónico hasta el uso de medios digitales, como correos electrónicos, mensajes de texto o redes sociales. Algunas de las técnicas comunes de ingeniería social incluyen el phishing, donde los atacantes envían mensajes engañosos que parecen ser de fuentes legítimas para inducir a las víctimas a revelar información confidencial, y el pretexting, que implica crear una historia falsa o un pretexto para obtener datos sensibles.

Además, los atacantes a menudo realizan una investigación exhaustiva sobre sus víctimas antes de llevar a cabo un ataque. Esto puede implicar la recopilación de información personal de fuentes públicas, como redes sociales, o la observación de comportamientos y patrones de comunicación.

El objetivo final de un ataque de ingeniería social puede variar ampliamente. Puede ser el robo de información financiera, contraseñas, secretos comerciales, acceso a redes corporativas o gubernamentales, el secuestro de cuentas en línea o la propagación de malware.

Para prevenir los ataques de ingeniería social, es fundamental aumentar la conciencia y la educación sobre este tipo de amenaza. Las organizaciones deben implementar políticas de seguridad robustas, capacitar a su personal para reconocer las señales de posibles ataques y promover una cultura de seguridad cibernética. A nivel individual, es importante mantener un nivel saludable de escepticismo ante las solicitudes de información confidencial y verificar la autenticidad de las fuentes antes de responder a ellas.

Ataques DDoS (Denegación de Servicio Distribuido)

En estos ataques, los atacantes inundan un sitio web o servicio en línea con una gran cantidad de tráfico falso, lo que provoca la caída del servidor y la indisponibilidad del servicio.

Ataques de inyección de SQL

Los atacantes insertan código SQL malicioso en las entradas de un sitio web para manipular una base de datos y acceder o modificar datos confidenciales.

Ataques de hombre en el medio (Man-in-the-Middle, MitM)

En estos ataques, un atacante intercepta y altera la comunicación entre dos partes, a menudo sin que ninguna de las partes lo sepa.

La notaría única de Alfredo Baquerizo Moreno y la seguridad de la información

La Notaría Única del Cantón Alfredo Baquerizo Moreno tiene su sede en el cantón Jujan, la cual brinda sus servicios profesionales desde hace más de 7 años. En ella se brindan servicios de Protocolización de documentos, elaboración y legalización de contratos, y todo lo que abarca el ámbito de legalización de documentos por medio de notario público.

La notaría cuenta con recurso humano los cuales se desempeñan como empleados multifuncionales.

La notaría actualmente cuenta con problemas con los datos e información almacenada en sus equipos. No posee una base de datos como tal, solo registros en archivos como Hojas de cálculo y documentos de Word.

Su infraestructura de red es simple, no posee controles de acceso, ni ningún tipo de regla que opere sobre el tráfico de red.

Debido a que los empleados de la notaría deben brindar una atención cercana al cliente, lo cual implica que los ordenadores estén cerca de terceros que ingresan a la notaría, los cuales podrían ser alcanzados con facilidad provocando robo o perdida de información.

La implementación de estándares de seguridad basados en la norma ISO 27001 nos ayudara a establecer políticas de seguridad adecuadas para el entorno de la Notaría Única del Cantón Alfredo Baquerizo Moreno, además de poder identificar oportunamente las amenazas

y vulnerabilidades y tener un plan de acción para cualquier eventualidad que se presente en cuanto a la seguridad de la información.

Resultados

En el Anexo, encuesta a los empleados de la notaría; pregunta: "¿Existen políticas y procedimientos para la seguridad de la información en la Notaría?"

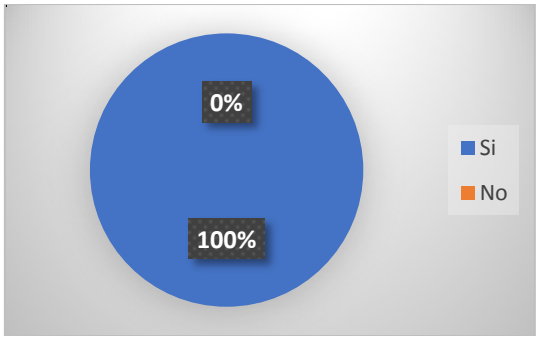
Tabla 1

Resultados de la encuesta, primera pregunta.

	Frecuencia	**Porcentaje**
SI	5	100%
NO	0	0%
TOTAL	5	100%

Figura 1

Resultados de la encuesta, primera pregunta.



El 100% de los empleados manifestó que ya existen políticas para el aseguramiento de la información, y la gran mayoría, 80%; manifestó que están familiarizados con estas políticas según cuestionamiento, pregunta "¿Está familiarizado con las políticas y procedimientos de seguridad de la información de la notaría?".

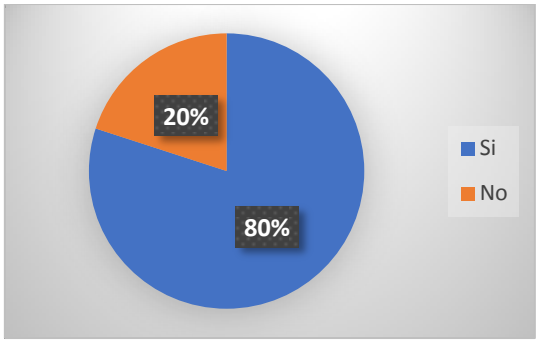
Tabla 2

Resultados de la encuesta, segunda pregunta.

	Frecuencia	**Porcentaje**
SI	4	80%
NO	1	20%
TOTAL	5	100%

Figura 2

Resultados de la encuesta, segunda pregunta.



La norma establece que la alta dirección debe establecer una política de seguridad de la información que sea idóneo para la organización, incluya los objetivos de seguridad de la información, que se establezca un compromiso de cumplir con estos requerimientos y promueva una mejora continua. Estas políticas deberán estar documentadas, deben ser comunicadas dentro de la organización y estar a disposición de los interesados según corresponda (ISO/CEI, 2022,p.3).

Además, la norma nos invita a tomar conciencia de estas políticas de seguridad de la información, de los beneficios para el desempeño de la seguridad de la información y de lo que implica no cumplir ellas (ISO/CEI, 2022).

Según la pregunta "¿Sabe qué hacer si pierde un dispositivo que contiene información confidencial de la organización, como una laptop o un teléfono móvil?"

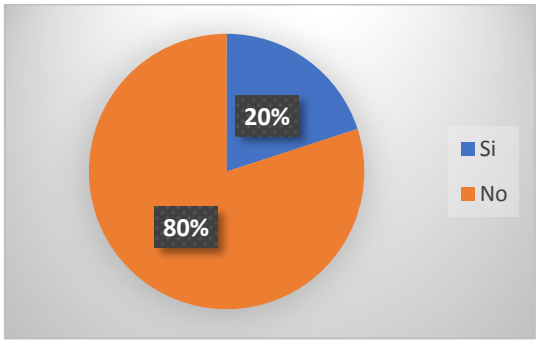
Tabla 3

Resultados de la encuesta, tercera pregunta.

	Frecuencia	**Porcentaje**
SI	1	20%
NO	4	80%
TOTAL	5	100%

Figura 3

Resultados de la encuesta, tercera pregunta.



El resultado indica que el 80% de los empleados de la notaría no sabría qué hacer, y qué medidas tomar ante una eventualidad como la pérdida de un dispositivo que contenga información confidencial para la notaría. Esto supone que nunca se ha evaluado un riesgo de tal magnitud, tampoco elaborado un plan de acción en un caso de que se dé este suceso.

La notaría deberá tomar acciones para abordar estos riesgos de seguridad de la información. Para lo cual es necesario planificar como se llevarán a cabo, cómo se evaluarán estos riesgos y cuál es el debido tratamiento de los mismos.

Según el cuestionamiento "¿La empresa realiza evaluaciones de riesgos de seguridad de la información de forma periódica?" los empleados de la notaría manifiestan en un 100% la negativa a esta pregunta.

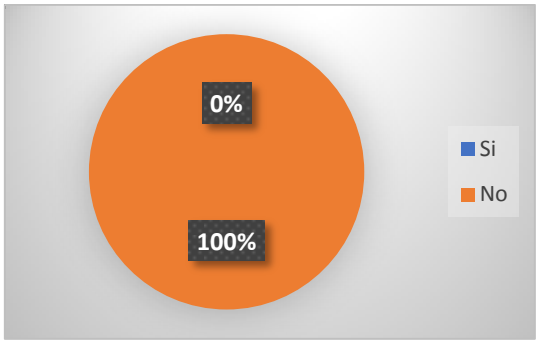
Tabla 4

Resultados de la encuesta, cuarta pregunta.

	Frecuencia	**Porcentaje**
SI	0	0%
NO	5	100%
TOTAL	5	100%

Figura 4

Resultados de la encuesta, cuarta pregunta.



La Norma indica que se debe aplicar el proceso de evaluación de riesgos de seguridad de la información para identificar los riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de la información dentro del alcance del sistema de gestión de seguridad de la información. También se debe medir la posibilidad de que estos incidentes ocurran y cuáles serían sus consecuencias (ISO/CEI, 2022,p.4).

También nos indica que dichas evaluaciones deben llevarse a cabo periódicamente, en intervalos planificados o cada vez que sea necesario y se lo propongan, siempre teniendo en cuenta los criterios de su planificación además de documentar y guardar los resultados de dichas evaluaciones (ISO/CEI, 2022,p.8).

La norma ISO 27001 en su Anexo A (Normativo), tabla A.1, sobre los controles de seguridad de la información; literal 7.1 sobre los perímetros físicos de seguridad, establece que: “Los perímetros de seguridad se definirán y utilizarán para proteger las áreas que contienen información y otros activos asociados” (ISO/CEI, 2022,p.14).

Así también en el literal 5.25 sobre la evaluación y decisión sobre eventos de seguridad de la información, establece que: “La organización debe evaluar los eventos de seguridad de la información y decidir si se clasificarán como incidentes de seguridad de la información” (ISO/CEI, 2022,p.13).

Además, el literal 5.26 y 5.27 nos habla de que se debe responder ante los incidentes de seguridad de la información de acuerdo a los procedimientos documentados por la norma y también mejorar continuamente mediante el conocimiento obtenido en estos incidentes de seguridad para así poder fortalecer y mejorar los controles de seguridad de la información (ISO/CEI, 2022,p.13).

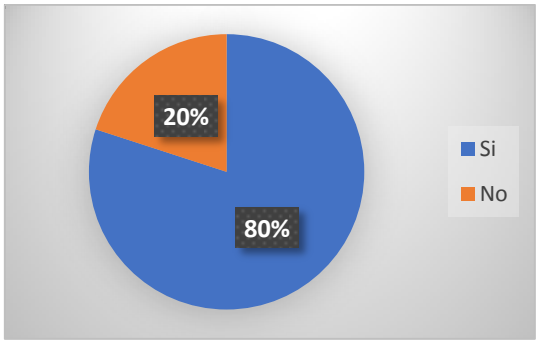
Tabla 5

Resultados de la encuesta, quinta pregunta.

	Frecuencia	**Porcentaje**
SI	4	80%
NO	1	20%
TOTAL	5	100%

Figura 5

Resultados de la encuesta, quinta pregunta.



En el cuestionamiento "¿Considera usted que se está asegurando la disponibilidad, integridad y confidencialidad de la información en la notaría?" el 80% de los empleados considera que se está cumpliendo con los pilares fundamentales de la seguridad de la información.

Sin embargo, al no existir una evaluación de los riesgos y al no tener una planificación para ejercer acción en caso de que ocurran estas eventualidades nos indica que la respuesta a este cuestionamiento no corresponde a la realidad de la Organización. Si bien se cuida la información física que está en su poder, el personal de la notaría desconoce cómo cuidar de la información de sus equipos informáticos.

En cuanto a controles de acceso, según la pregunta "¿Se ha realizado controles de acceso para los datos de los usuarios?" el 60% considera que, si se han establecido controles de acceso, frente al otro 40% el cual manifiesta que desconoce si se han aplicado o no.

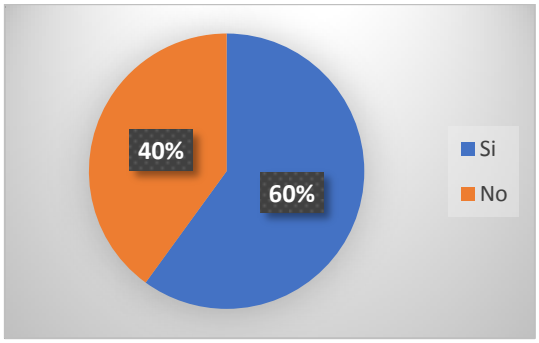
Tabla 6

Resultados de la encuesta, sexta pregunta.

	Frecuencia	**Porcentaje**
SI	3	60%
NO	2	40%
TOTAL	5	100%

Figura 6

Resultados de la encuesta, sexta pregunta.



La norma indica que "La asignación y uso de los derechos de acceso privilegiado se restringirá y gestionará" (ISO/CEI, 2022,p.15).

Las políticas de seguridad de la información de la organización deben incluir clausulas donde se especifique los sujetos que tienen autorización para acceder a la información que reposa en la organización sea física o eléctronica.

Según cuestionamiento "¿La notaría realiza copias de seguridad de la información periódicamente?", según datos obtenidos vemos que el 60% del personal manifiesta que no se hace copia de seguridad de la información periodicamente, lo cual supone la mayoría frente al 40% que manifiesta que si se realiza un respaldo de la información.

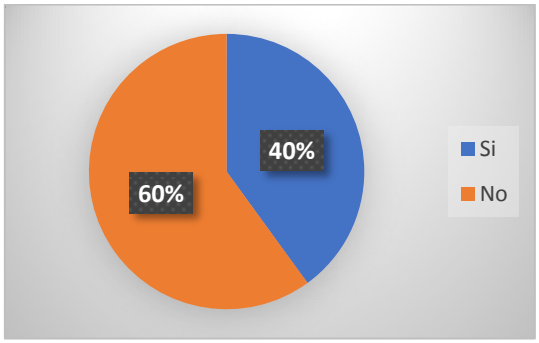
Tabla 7

Resultados de la encuesta, séptima pregunta.

	Frecuencia	**Porcentaje**
SI	2	40%
NO	3	60%
TOTAL	5	100%

Figura 7

Resultados de la encuesta, séptima pregunta.



La norma nos indica en su anexo normativo que "Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán periódicamente de acuerdo con la política de copia de seguridad específica del tema acordada" (ISO/CEI, 2022,p.16).

Las copias de seguridad son de vital importancia ya que en caso de perdida de información existe la posibilidad de recuperar los datos mediante la misma. Las copias de seguridad de la información ayudan a que la información esté disponible aún cuando ocurran incidentes de seguridad o perdidas materiales.

Aunque la notaría procura con diligencia la protección de la información contra amenazas de origen físico o incluso por accidentes como sería el caso de un incendio, un desastre natural o cualquier eventualidad que ponga en riesgo la integridad de su archivo físico, tal como indica la norma en su normativa que indica que: “Se debe diseñar e implementar la protección contra amenazas físicas y ambientales, tales como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura”. (ISO/CEI, 2022,p.15). El mayor problema es la falta de conocimiento del personal, según las respuestas obtenidas en el cuestionamiento “¿Conoce usted qué es un Sistema de Gestión de Seguridad de la Información?”

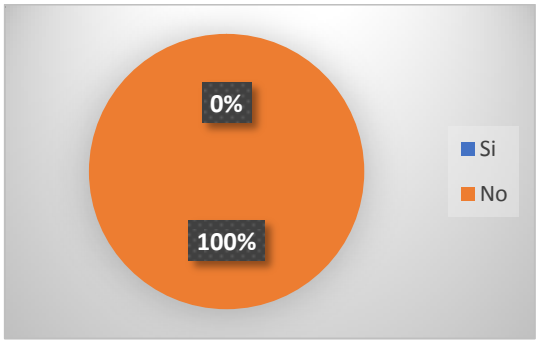
Tabla 8

Resultados de la encuesta, octava pregunta.

	Frecuencia	**Porcentaje**
SI	0	0%
NO	5	100%
TOTAL	5	100%

Figura 8

Resultados de la encuesta, octava pregunta.



podemos ver que el 100% del personal no conoce acerca de lo que es un sistema de gestión de seguridad de la información, y sus conocimientos en cuanto a ataques informáticos y detección de riesgos para la información son muy básicos ya que el 80% del personal no es capaz de identificar un ataque informático o un intento de robo de información según cuestionamiento: "¿Es usted capaz de identificar un ataque informático, o un intento de robo de información?".

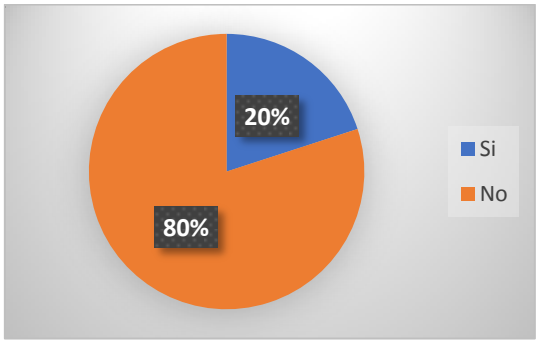
Tabla 9

Resultados de la encuesta, novena pregunta.

	Frecuencia	**Porcentaje**
SI	1	20%
NO	4	80%
TOTAL	5	100%

Figura 9

Resultados de la encuesta, novena pregunta.



El personal de la notaría necesita capacitación en el área de seguridad informática, según la norma ISO 27001 que desconocen del tema, ya el 100% manifiesta que no ha recibido capacitación en el último año según cuestionamiento "¿Ha recibido capacitación en seguridad de la información en los últimos 12 meses?".

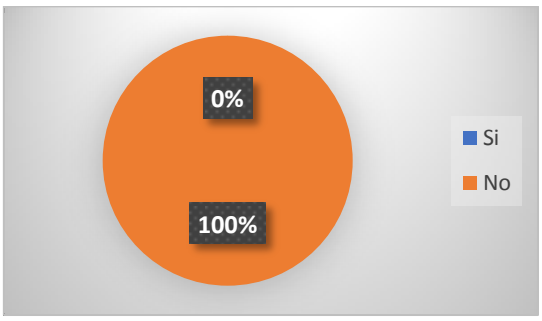
Tabla 10

Resultados de la encuesta, décima pregunta.

	Frecuencia	**Porcentaje**
SI	0	0%
NO	5	100%
TOTAL	5	100%

Figura 10

Resultados de la encuesta, décima pregunta.



> En su Anexo de normativa nos indica que: “El personal de la organización y las partes interesadas relevantes deben recibir la conciencia, educación y capacitación adecuadas en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral” (ISO/CEI, 2022,p.14).

Caso práctico de vulneración de seguridad

Luego de conocer los resultados de las encuestas realizadas al personal de la notaría, hemos determinado que el mayor problema es el desconocimiento del tema de seguridad informática.

Ejemplificaremos un caso de vulneración de la seguridad de la información el cual podría tener lugar en la notaría si no se toma las medidas necesarias acogiéndose a la norma ISO 27001. Antes que nada, revisaremos brevemente los contextos de esta amenaza.

Microsoft support diagnostic tool

Microsoft Support Diagnostic Tool, sus siglas MSDT “es una aplicación que se utiliza para recopilar automáticamente información de diagnóstico y enviarla a Microsoft cuando algo falla en Windows.” (AO KASPERSKY LAB, 2022). Puesto que esta utilidad es proporcionada por Microsoft y está diseñada para ayudar a diagnosticar y solucionar problemas en el sistema operativo lo cual es bueno, pero no del todo ya que genera un problema el cual radica en que esta aplicación recopila información sobre el sistema con la finalidad de proponer soluciones a problemas comunes sean simples o complejos que los usuarios puedan enfrentar al utilizar Windows.

Vulnerabilidad Follina

La Vulnerabilidad llamada “Follina”, está basada en un fallo de seguridad en la herramienta de soporte MSDT de Microsoft, antes mencionada.

Por alguna razón la aplicación de soporte que proporciona Microsoft, la cual cabe recalcar viene por defecto en el sistema operativo Windows; se le pueden inducir parámetros con los cuales se pueden ejecutar instrucciones en ventana de comandos.

Follina, usa la función de plantilla remota de Microsoft Office, para recuperar un archivo HTML alojado en un servidor web remoto, el cual a su vez baja una carga maliciosa mediante el puerto 8000, esta carga remota hace uso de la herramienta MSDT para poder ejecutar cualquier comando mediante ventana de comandos.

Anteriormente se conocían métodos similares como, por ejemplo, el uso de macros insertados en documentos de Microsoft office, con la finalidad de que el código que se ejecuta realice descargas de archivos que infecten el sistema de archivos y así tomar posesión de la información. Follina, usa un método diferente pero el resultado es similar.

La ejecución de este código malicioso se puede llevar a cabo mediante la apertura de un archivo de Word preparado, e incluso sin necesidad de abrirlo si tiene activado la vista previa de documentos en el explorador de archivos.

Prueba de penetración

Para la siguiente prueba vamos a necesitar lo siguiente:

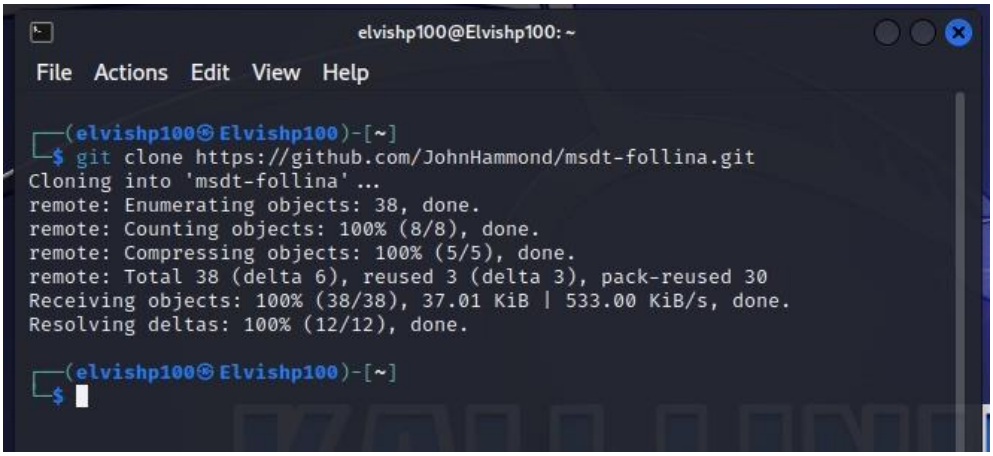
Kali Linux para preparar y realizar el ataque, repositorio de GitHub el cual contiene los archivos necesarios para clonar y ejecutar en Kali y por último un computador con Windows

10, para simular la postura de la víctima. A esto también se requiere el conocimiento básico de Python y de comandos de Kali Linux.

Como primer paso para esta prueba vamos a nuestro sistema Kali, mediante ventana de comandos vamos a clonar el repositorio GitHub donde están los archivos necesarios para esta prueba.

Figura 11

Clonar repositorio



Verificamos que estos archivos se encuentren en el directorio.

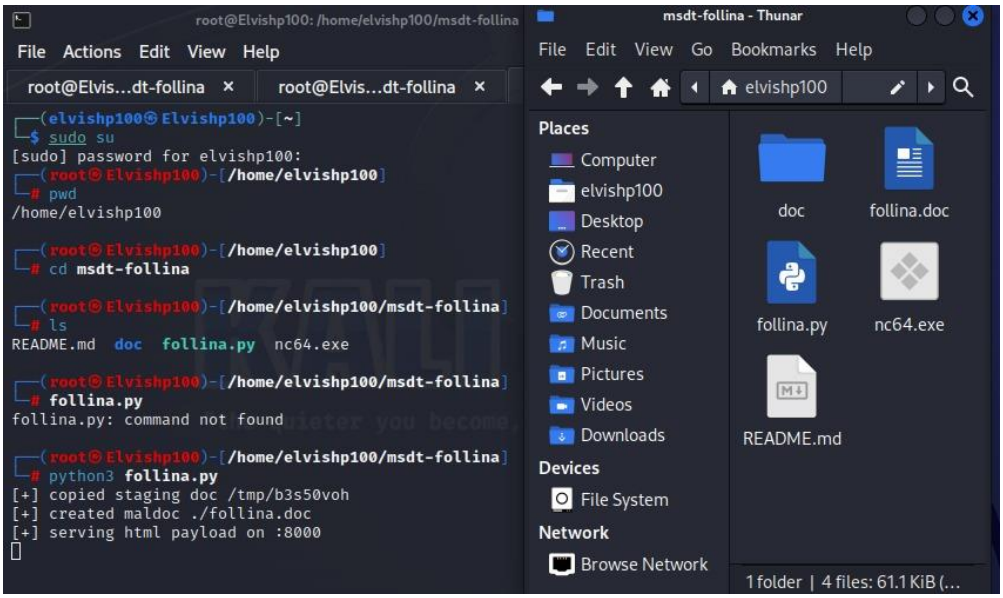
Figura 12

Archivos necesarios

Generamos el archivo malicioso de extensión .doc. Ejecutando el comando que ejecuta el archivo de phyton.

Figura 13

Generación de Follina.doc



Como podemos observar se ha creado el archivo malicioso, además se ha creado el servicio web en el puerto 8000, puerto desde el cual se va a bajar la carga maliciosa.

Tenemos dos opciones, cargar el archivo al servicio web de Kali, o hacer uso de ingeniería social para lograr que la victima ejecute el archivo en su computadora.

En este caso vamos a simular el escenario en que la victima descarga el documento desde alguna web.

Vamos a habilitar el puerto 80, del servicio web de Kali Linux; El cual es diferente del puerto 8000 generado anteriormente.

En este caso hemos creado y alojado una página web que simule la descarga del archivo.

Figura 14

Archivo prueba.html

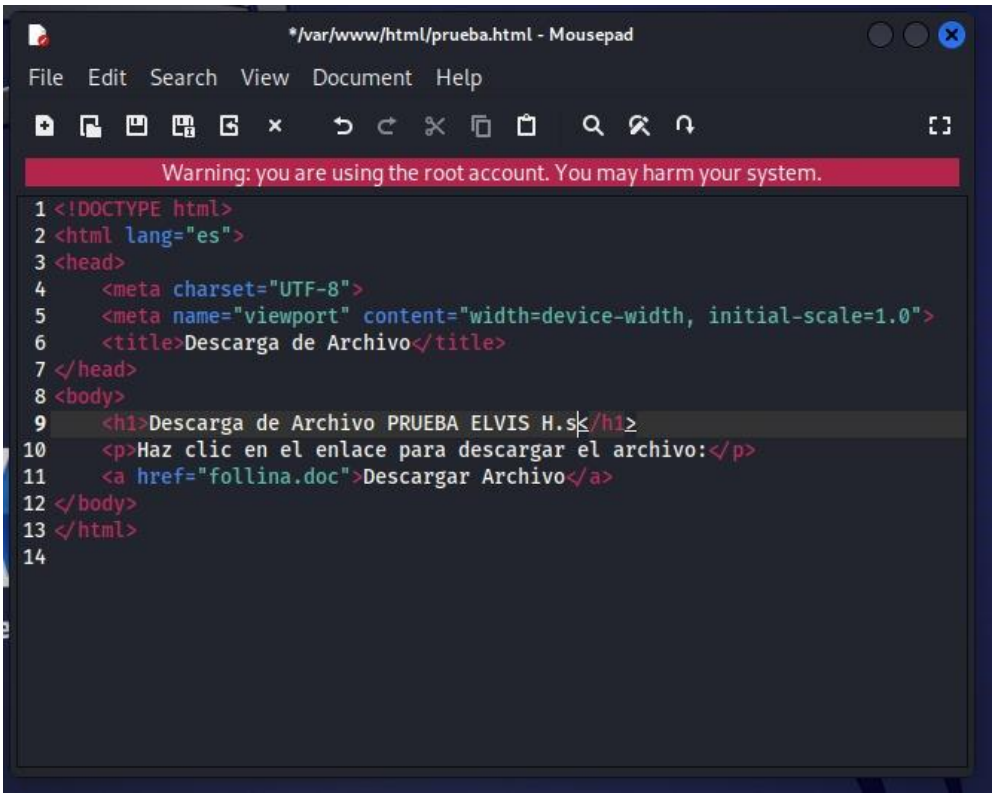
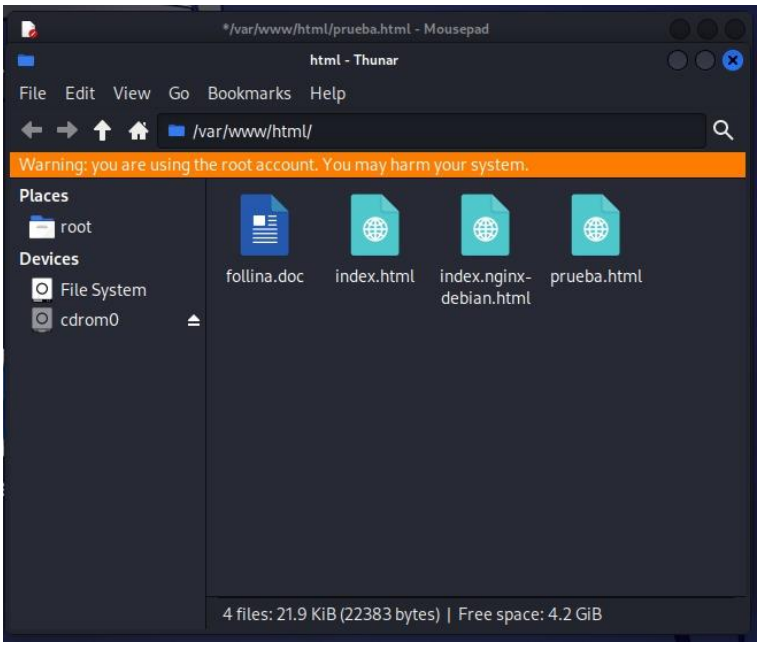


Figura 15

Alojamiento de página de prueba



En el Pc de la Victima, accedemos a la dirección Ip de nuestro Kali Linux, y haremos lo que normalmente haría la víctima, descargar el archivo.

Figura 16

Conexión desde Pc de Victima.

Al momento en que la victima ejecuta el archivo, va a empezar la actividad en el puerto 8000, el cual bajara la carga maliciosa en el ordenador de la víctima.

Figura 17

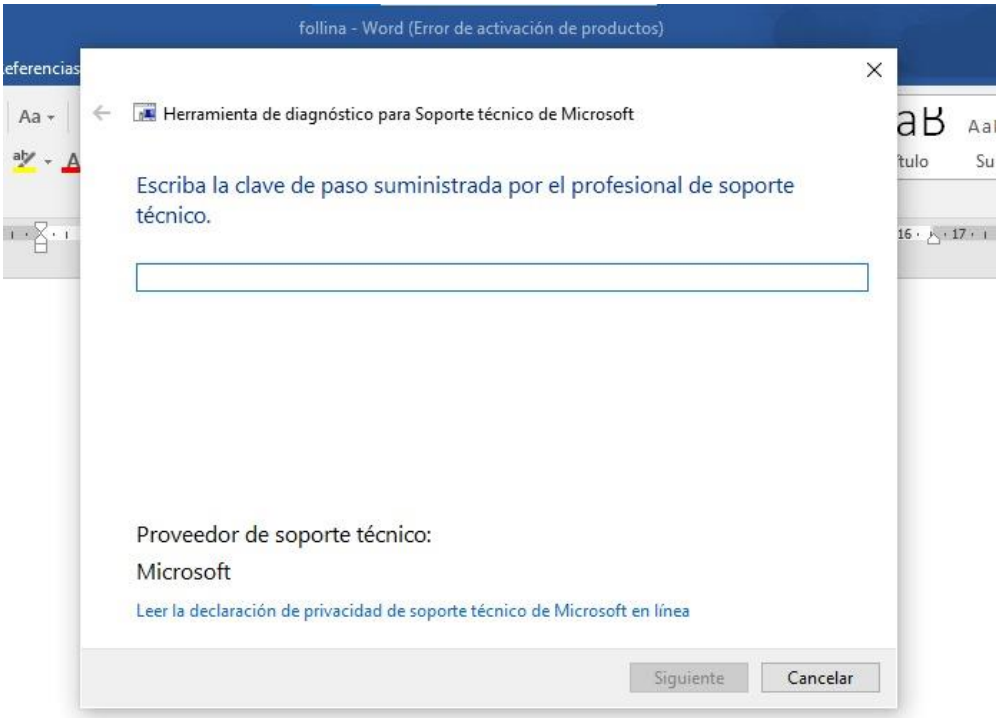
Descarga de archivo infectado.

Como podemos observar se abre la herramienta de Microsoft, la cual mediante los parámetros de código del archivo Python, hace que se ejecute una acción mediante ventana de comandos. En este caso en específico el ordenador de la víctima cuenta con el último parche de seguridad 2023 lo cual nos abre el asistente, sin embargo no ejecuta ningún parámetro

puesto que nos pide un código de servicio el cual es proporcionado directamente desde Microsoft. Esta es una medida de seguridad que tomó Microsoft para combatir esta vulnerabilidad.

Figura 18

Ejecución del archivo.



Aunque existe un parche de seguridad, la probabilidad de que el ordenador de la víctima no posea dicha actualización es alta, sin mencionar sistemas operativos anteriores a windows 10, como por ejemplo windows 8 y 8.1 los cuales ya contaban con esta herramienta de diagnóstico de windows y las cuales carecen de soporte al estar descontinuados.

Usando este mismo método podemos establecer comandos que copien, editen o eliminen la información del computador lo cual supone una vulnerabilidad grave y un riesgo para la información lo cual es precisamente lo que se pretende evitar con esta prueba.

Recomendaciones

La vulnerabilidad Follina, la cual está basada en la herramienta de diagnostico de Windows representa un peligro importante para la seguridad de la información. La probabilidad de que un escenario similar ocurra en la Notaría Única del Cantón Alfredo Baquerizo Moreno es alta y las consecuencias en caso de efectuarse este ataque son graves. Por eso es importante tomar acción para que esto no ocurra.

Aunque siempre se recomienda tener actualizado Windows a sus ultimas versiones ya que suelen aplicar parches de seguridad cerrándole las puertas a estos ataques, no es suficiente para solventar el problema, ya que estos métodos de ataque también están evolucionando para evadir nuevas seguridades.

Follina, depende del protocolo URL del asistente de diagnostico de Windows, el cual es el medio para que se baje la carga maliciosa y se ejecuten las instrucciones por ventana de comandos.

Solucionaremos este fallo deshabilitando el protocolo URL del asistente, lo haremos mediante la ventana de comandos de Windows, con privilegios de Administrador; con las siguientes instrucciones “reg delete HKEY_CLASSES_ROOT\ms-msdt /f”. la cual sirve para borrar el registro mediante el comando.

Este es solo un pequeño ejemplo de una vulnerabilidad que puede sufrir la Notaria. Por eso es importante que se tome acción y consciencia acerca de la seguridad de la información conforme lo establece la norma ISO 27001.

CONCLUSIONES

La Notaría Única del Cantón Alfredo Baquerizo Moreno, a lo largo de sus años de servicio en el ámbito de la legalización de documentos y servicios notariales, ha brindado un importante respaldo a la comunidad. Sin embargo, en su actual estado, enfrenta desafíos significativos relacionados con la gestión de la información y la seguridad de la misma. En este análisis, hemos identificado varios aspectos críticos que necesitan atención y mejora.

En primer lugar, se ha destacado la ausencia de una infraestructura tecnológica la cual de prioridad a la seguridad de la información. La notaría depende en gran medida de registros en archivos de hojas de cálculo y documentos de Word para gestionar la información. Esto representa un riesgo importante en términos de disponibilidad, integridad y confidencialidad de los datos. La falta de una base de datos centralizada y medidas de seguridad efectivas plantea un problema significativo para la protección de la información sensible de los clientes y la eficiencia operativa. Además, la notaría cuenta con controles de acceso los cuales son adecuados para la información física que reposa en el archivo de la notaría sin embargo no son idóneos para la información guardada en medios digitales.

Aunque la notaría cuenta con sus propios métodos para cuidar la información no se han establecido políticas y procedimientos formales de seguridad de la información. Esto se traduce en una exposición a riesgos de seguridad.

Los empleados, debido a la naturaleza de su trabajo, están en contacto directo con terceros que ingresan a la notaría. Esta situación aumenta la posibilidad de incidentes de seguridad, como la pérdida o el robo de información confidencial. Así como el ejemplo anterior, hay muchas vulnerabilidades y riesgos que deben ser identificados y deben medir su alcance y la posibilidad de que ocurra.

La falta de conocimiento en términos de seguridad de la información es el principal problema, por lo cual el personal no está preparado para identificar ataques informáticos o para responder adecuadamente a incidentes de seguridad. Esto destaca la necesidad urgente de proporcionar capacitación y concienciación en seguridad de la información a todo el equipo.

La norma ISO 27001 se ha presentado como una solución viable para abordar estos desafíos. Esta norma ofrece un marco sólido para establecer políticas y procedimientos de seguridad de la información, así como para realizar evaluaciones periódicas de riesgos y adoptar medidas preventivas y correctivas. La alta dirección debe liderar este proceso, estableciendo una política de seguridad de la información y promoviendo una cultura de seguridad dentro de la organización.

En resumen, la Notaría Única del Cantón Alfredo Baquerizo Moreno enfrenta desafíos significativos en términos de seguridad de la información y gestión de datos. La implementación de estándares de seguridad basados en la norma ISO 27001 es esencial para garantizar la protección de la información, la integridad de los datos y la confianza de los clientes. Además, es imperativo proporcionar capacitación y concienciación al personal para fortalecer la seguridad de la información en todos los niveles de la organización. Estos pasos son esenciales para garantizar la continuidad y el éxito de la notaría en el futuro.

BIBLIOGRAFÍA

AO Kaspersky Lab. (2023). *¿Qué es la ciberseguridad? 14 de Septiembre de 2023, de Kaspersky Latam: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security*

Chicaiza, J. (2018). *Implementación de la Norma ISO 27001:2013 en una Institución Financiera en Ecuador. Ambato: Publicacion Universidad de los Andes.*

Global Suite Solutions. (20 de Julio de 2023). *¿Qué es la norma ISO 27001 y para qué sirve? 14 de Septiembre de 2023, de Global Suite Solutions: https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/*

ISO/CEI. (25 de Octubre de 2022). *Seguridad de la Información, Ciberseguridad y Protección de la Privacidad - Sistemas de Gestión de la Seguridad de la Información - Requisitos. 14 de Septiembre de 2023, de Organización Internacional de Normalización: https://es.scribd.com/document/616176936/ISO-27001-2022-espanol*

Ivan, B. (19 de enero de 2023). *¿Qué es el malware y cómo protegerse de los ataques? 14 de Septiembre de 2023, de Avast Software s.r.o.: https://www.avast.com/es-es/c-malware#:~:text=Los%20hackers%20suelen%20utilizar%20spyware,para%20cometer%20robo%20de%20identidad*

Monsalve, J. (21 de Noviembre de 2018). *CIBERSEGURIDAD: PRINCIPALES AMENAZAS EN COLOMBIA (INGENIERÍA SOCIAL, PHISHING Y DoS). Universidad Piloto de Colombia, pág. 3. 14 de Septiembre de 2023*

Pontiroli, S. (2019). *Cyber Defense through Threat Intelligence. La Plata, Buenos Aires, Argentina: Treaintel Universidad Tecnologica Nacional.*

Valenzuela, R., & Quijada, R. (2016). *Guía de Referencia ISO 27001:2013 para Entidades de Gobierno en Chile. Santiago de Chile: Editorial Capopeyan.*

Watkins, S. (2017). *Implementando ISO 27001: Una Guía Práctica para Utilizar el Marco del SGSI (Sistema de Gestión de Seguridad de la Información). Burlington, Massachusetts, Estados Unidos: The Fire.*

ANEXO 1

ENCUESTA REALIZADA AL PERSONAL DE LA NOTARÍA ÚNICA DEL CANTÓN ALFREDO BAQUERIZO MORENO.

¿Existen políticas y procedimientos para la seguridad de la información en la Notaría?

- Sí
- No

¿Está familiarizado con las políticas y procedimientos de seguridad de la información de la notaría?

- Sí
- No

¿Sabe qué hacer si pierde un dispositivo que contiene información confidencial de la organización, como una laptop o un teléfono móvil?

- Sí
- No

¿La empresa realiza evaluaciones de riesgos de seguridad de la información de forma periódica?

- Sí
- No

¿Se ha realizado controles de acceso para los datos de los usuarios?

- Sí
- No

¿La notaría realiza copias de seguridad de la información periódicamente?

- Sí
- No

¿Considera usted que se está asegurando la disponibilidad, integridad y confidencialidad de la información en la notaría?

- Sí
- No

¿Conoce usted qué es un Sistema de Gestión de Seguridad de la Información?

- Sí
- No

¿Es usted capaz de identificar un ataque informático, o un intento de robo de información?

- Sí
- No

¿Ha recibido capacitación en seguridad de la información en los últimos 12 meses?

- Sí
- No

ANEXO 2

SOLICITUD DE AUTORIZACIÓN

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
DECANATO

Babahoyo, 23 de agosto del 2023
D-FAFI-UTB-00599-2023

Abogada.
Lelia Etelvina Burgos Rugel
REPRESENTANTE LEGAL DE LA NOTARÍA ÚNICA DEL CANTÓN ALFREDO BAQUERIZO MORENO.
Presente. –

De mis consideraciones:

Reciba un cordial saludo por parte de la Facultad de Administración, Finanzas e Informática de la Universidad Técnica de Babahoyo, donde formamos profesionales altamente capacitados en los campos de Tecnologías de la Información y de Administración, competentes, con principios y valores cuya practica contribuye al desarrollo integral de la sociedad, es por ello que buscamos prestigiosas Empresas e Instituciones Públicas y Privadas en las cuales nuestros futuros profesionales tengan la oportunidad de afianzar sus conocimientos.

El señor **ELVIS ABEL HERRERA PALMA** con cédula de identidad No. **0928060912** estudiante de la Carrera de Ingeniería en Sistemas, matriculado en el proceso de titulación en el periodo junio – octubre 2023, trabajo de titulación modalidad Estudio de Caso, previo a la obtención del grado académico profesional *universitario* de tercer nivel como Ingeniero en Sistemas**,** solicita por intermedio del Decanato de esta Facultad el debido permiso para poder culminar su proyecto, el cual titula: **"ANÁLISIS DE SEGURIDAD INFORMÁTICA BAJO LOS ESTÁNDARES ISO 27001 EN LA NOTARÍA ÚNICA DEL CANTÓN ALFREDO BAQUERIZO MORENO".**

Atentamente,

Lcdo. Eduardo Galeas Guijarro, MAE.
DECANO
c.c: Archivo

UNIVERSIDAD TÉCNICA DE BABAHOYO · FAC. ADMINISTRACIÓN FINANZAS E INFORMÁTICA · DECANATO

Presentado en la ciudad de Alfredo Baquerizo Moreno – Jujan, a los doce días del mes de septiembre del dos mil veintitrés a las nueve horas.-

NOTARIA UNICA DEL CANTON ALFREDO BAQUERIZO MORENO
REPUBLICA DEL ECUADOR
Ab. Lelia Burgos Rigel
JUJAN

ANEXO 3

AUTORIZACIÓN

Alfredo Baquerizo Moreno, 12 de septiembre de 2023.

Señor.
Ing. Eduardo Galeas Guijarro, Msc.
DECANO DE LA FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO
Presente. -

De mi consideración:

Reciba un cordial saludo, me dirijo a usted para dar contestación a la solicitud recibida por la Universidad Técnica de Babahoyo y la Facultad de Administración, Finanzas e Informática que usted acertadamente dirige, para informar lo siguiente.

El Señor. **Elvis Abel Herrera Palma** con cédula de ciudadanía número **092806091-2**, estudiante de **Ingeniería en Sistemas**, matriculado en el proceso de titulación junio – octubre 2023, realizó una investigación sobre la seguridad informática de la notaría a mi cargo.

Por lo antes expuesto, **AUTORIZO AL SEÑOR ELVIS ABEL HERRERA PALMA** para que realice su trabajo de titulación denominado **"**Análisis De Seguridad Informática Bajo Los Estándares ISO 27001 En La Notaría Única Del Cantón Alfredo Baquerizo Moreno**",** requisito indispensable previo a la obtención del título de Ingeniería En Sistemas.

Agradeciendo de antemano a la presente solicitud, particular que comunico para los fines correspondientes.

Atentamente.

NOTARIA UNICA DEL CANTON ALFREDO BAQUERIZO MORENO
REPUBLICA DEL ECUADOR
Ab. Lelia Burgos Rugel
JUJAN

AB. LELIA ETELVINA BURGOS RUGEL

CC. 0910644517

ANEXO 4

CERTIFICADO DE ANALISÍS ANTIPLAGIO

CERTIFICADO DE ANÁLISIS
magister

estudio de caso Elvis Herrera v8.0.parasubir

6% Similitudes

7% Texto entre comillas
3% similitudes entre comillas
2% Idioma no reconocido

Nombre del documento: estudio de caso Elvis Herrera v8.0.parasubir.docx
ID del documento: bf498be3d33f3c4903280d758fca05e9e5a9b3e4
Tamaño del documento original: 582,88 kB
Autor: Elvis Herrera

Depositante: Elvis Herrera
Fecha de depósito: 16/9/2023
Tipo de carga: url_submission
fecha de fin de análisis: 16/9/2023

Número de palabras: 7041
Número de caracteres: 45.688

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**www.pmg-ssi.com** | Controles de la ISO/IEC 27001:2022 (I). Controles organizacion… https://www.pmg-ssi.com/2023/01/controles-de-la-iso-iec-270012022-i-controles-organizacionales/... 8 fuentes similares	1%		Palabras idénticas: 1% (100 palabras)
2	**repositorio.unsch.edu.pe** http://repositorio.unsch.edu.pe/bitstream/UNSCH/1751/1/TESIS SIS48_Cce.pdf 8 fuentes similares	1%		Palabras idénticas: 1% (84 palabras)
3	**latam.kaspersky.com** | Kaspersky: América Latina registra 5 mil ataques de ranso… https://latam.kaspersky.com/about/press-releases/2020_kaspersky-america-latina-registra-5-mil-at... 2 fuentes similares	1%		Palabras idénticas: 1% (84 palabras)
4	**repositorioacademico.upc.edu.pe** | Diseño de un Sistema de Gestión de Segurida… https://repositorioacademico.upc.edu.pe/bitstream/10757/652121/3/Monteza_ML.pdf 7 fuentes similares	< 1%		Palabras idénticas: < 1% (67 palabras)
5	**Documento de otro usuario** #122e58 El documento proviene de otro grupo 3 fuentes similares	< 1%		Palabras idénticas: < 1% (61 palabras)

Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**Documento de otro usuario** #2c8c4b El documento proviene de otro grupo	< 1%		Palabras idénticas: < 1% (29 palabras)
2	**openaccess.uoc.edu** | Plan de implementación de la ISO/IEC 27001:2013, en la fun… https://openaccess.uoc.edu/bitstream/10609/81145/6/feduardosanchezTFM0618memoria.pdf	< 1%		Palabras idénticas: < 1% (28 palabras)
3	**www.kaspersky.es** | Follina (CVE-2022-30190): una vulnerabilidad en MSDT | Blog … https://www.kaspersky.es/blog/follina-cve-2022-30190-msdt/27225/	< 1%		Palabras idénticas: < 1% (19 palabras)
4	**www.scielo.org.co** | Desafíos nacionales frente a la ciberseguridad en el escenari… http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199	< 1%		Palabras idénticas: < 1% (19 palabras)
5	**blog.innevo.com** | SGSI: Qué es y Cómo Implementarlo https://blog.innevo.com/que-es-sgsi	< 1%		Palabras idénticas: < 1% (13 palabras)