SAN IGNACIO DE LOYOLA – ESCUELA ISIL

TÍTULO DE LA INVESTIGACIÓN

“Propuesta de un plan de cultura de seguridad de la información para evitar la filtración de datos de los trabajadores de la empresa Saltalto, 2023”

TRABAJO DE INVESTIGACIÓN PARA OPTAR EL GRADO ACADÉMICO DE:

Bachiller en Administración y Dirección de negocios

Bachiller en Dirección de Tecnologías de Información

PRESENTADO POR:

La Torre Cordero, Jean Jairo - Administración y Dirección de Negocios

Mechan Gonzales, Brayan Manuel - Administración y Dirección de Negocios

Melendez Adames, Mauricio Jose - Administración y Dirección de Negocios

Quinto Huanqque, Josue Federico – Dirección de Tecnologías de Información

ASESOR:

Espinoza Rúa, Celes Alonso

LIMA, PERÚ

2024

ASESOR Y MIEMBROS DEL JURADO

ASESOR:

Espinoza Rúa, Celes Alonso

MIEMBROS DEL JURADO:

Vidal Gutierrez, David

Padilla Atauje, Daniel Humberto

Rebaza Garcia, Luis Rodolfo

DECLARACIÓN JURADA DE ORIGINALIDAD

Yo, Jean Jairo La Torre Cordero identificado con DNI N° 71451621 perteneciente al Programa de Administración y Dirección de Negocios, siendo mi asesor el Sr. Celes Alonso Espinoza Rúa, identificado con DNI N° 42750231, y cuyo código ORCID es 0000-0001-5324-7945

Yo, Brayan Manuel Mechan Gonzales identificado con DNI N° 73449426 perteneciente al Programa de Administración y Dirección de Negocios, siendo mi asesor el Sr. Celes Alonso Espinoza Rúa, identificado con DNI N° 42750231, y cuyo código ORCID es 0000-0001-5324-7945

Yo, Mauricio Jose Melendez Adames identificado con DNI N° 61116752 perteneciente al Programa de Administración y Dirección de Negocios, siendo mi asesor el Sr. Celes Alonso Espinoza Rúa, identificado con DNI N° 42750231, y cuyo código ORCID es 0000-0001-5324-7945

Yo, Josue Federico Quinto Huanqque identificado con DNI N° 46219313 perteneciente al Programa de Dirección de Tecnologías de Información, siendo mi asesor el Sr. Celes Alonso Espinoza Rúa, identificado con DNI N° 42750231, y cuyo código ORCID es 0000-0001-5324-7945

DECLARAMOS BAJO JURAMENTO QUE:

a) Somos los autores del documento académico titulado “Propuesta de un plan de cultura de seguridad de la información para evitar la filtración de datos de los trabajadores de la empresa Saltalto, 2023”

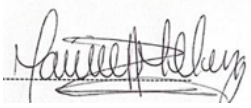
b) El trabajo de investigación es original y no ha sido difundido en ningún medio académico; por lo tanto, sus resultados son veraces y no es copia de ningún otro.

c) El trabajo de investigación cumplió con el análisis del sistema TURNITIN, el cual tiene el 20% de similitud. Se ha respetado el uso de las normas internacionales en cuanto a citas y referencias.

d) Declaramos conocer las consecuencias legales y/o administrativas que puedan derivar si se verifica la falsedad total o parcial de la presente declaración, de acuerdo con lo previsto en el artículo 411 del código penal y el numeral 34.3 del artículo 34 del Texto Único Ordenado de la Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo 004-2019-JUS.

Fecha: 19, marzo, 2024

Firmas de los autores

Nombres	Apellidos	Dni	Firma	Huella
Jean Jairo	**La Torre Cordero**	**71451621**		
Brayan Manuel	**Mechan Gonzales**	**73449426**		
Mauricio Jose	**Melendez Adames**	**61116752**		

Josue Federico	**Quinto Huanqque**	**46219313**		

Firma del asesor

Nombres	Apellidos	Dni	Firma	Huella
Celes Alonso	**Espinoza Rúa**	**42750231**		

DEDICATORIA

Este trabajo está dedicado a nuestros familiares, por su apoyo incondicional, compañía y fortaleza para terminar con éxito nuestro objetivo.

AGRADECIMIENTO

A Dios por brindarnos la vida, la fortaleza y la sabiduría para llevar a cabo este trabajo. De igual forma a ISIL por brindarnos la formación académica y todos los recursos para desarrollar este artículo con éxito. Finalmente, a todos los autores que han aportado con sus posturas e investigaciones haciendo posible el desarrollo de este trabajo.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El objetivo principal de este estudio es sugerir que se instaure una cultura de seguridad de la información para detener las fugas de datos de los empleados en Saltalto, 2023. Con un enfoque cuantitativo, se propuso un diseño no experimental y se recopilaron datos mediante encuestas. Dado el rápido avance de la tecnología y la inadecuada cultura de seguridad de la información que prevalece en muchas empresas, las conclusiones demuestran que la fuga de datos puede prevenirse mediante la implantación de una cultura de seguridad de la información. Por lo tanto, se puede deducir que el fomento de una cultura de seguridad de la información ayudará a prevenir las fugas de datos de los empleados en Saltalto.

Palabras clave: Filtración de información, datos, privacidad, seguridad de la información, robo de credenciales, robo de identidad, fraude cibernético, cibercrimen, mejores prácticas, seguridad informática, cultura organizacional.

ABSTRACT

The primary goal of this study is to suggest that an information security culture be put in place to stop employee data leaks at Saltalto, 2023. With a quantitative approach, the non-experimental design was suggested, and data was gathered via questionnaires. Given the rapid advancement of technology and the inadequate information security culture prevalent in many businesses, the findings demonstrate that data leakage can be prevented by the implementation of an information security culture. Thus, it can be inferred that fostering an information security culture will aid in preventing employee data leaks at Saltalto.

Keywords: Information leakage, data, privacy, information security, credential theft, identity theft, cyber fraud, cybercrime, best practices, information security, organizational culture.

INTRODUCCIÓN

La seguridad de la información se ha vuelto crucial en la actualidad, ya que la filtración de datos puede tener consecuencias devastadoras tanto para los empleados como para la empresa en su conjunto. En este sentido, es fundamental promover una cultura de seguridad en la organización que fomente buenas prácticas y concientice a los trabajadores sobre la importancia de proteger la información sensible de la empresa. El plan propuesto tiene como objetivo principal prevenir la filtración de datos mediante la implementación de medidas de seguridad tecnológicas y la capacitación continua del personal en materia de ciberseguridad.

El presente estudio está estructurado de la siguiente manera:

Capítulo I: En esta parte del trabajo se presenta la información general del proyecto, como el área estratégica de desarrollo, actividad económica y alcance de la solución y la localización.

Capítulo II: Se encuentra la descripción de la investigación aplicada, cómo la formulación del problema, los objetivos, justificación, limitaciones y viabilidad de la investigación. También está el detalle del marco referencial, es decir; los antecedentes, el marco teórico y la definición de los términos básicos. Finalmente, se detalla el diseño metodológico, muestral, la población, muestra, técnicas de recolección de datos y estadísticos junto con los resultados.

Capítulo III: Se detallarán los costos asociados para lograr la implementación de plan.

Capítulo IV: Se compartirá el desarrollo de la propuesta de innovación; es decir, el alcance esperado, la descripción de la propuesta de innovación, diagnóstico situacional, procedimiento de la propuesta de mejora y desarrollo del proyecto de innovación.

I. Información General

1.1. Título del Proyecto

Propuesta de un plan de cultura de Seguridad de la información para evitar la filtración de datos de los trabajadores de la empresa Saltalto, 2023

1.2. Área estratégica de desarrollo prioritario

Este estudio tendrá impacto en el ámbito estratégico de la comunicación, la sociedad y la cultura, ya que beneficiará el desarrollo de una variedad de productos y estudios para evaluar con precisión diferentes realidades y contextos culturales.

1.3. Actividad económica en la que se aplicaría la innovación o investigación aplicada

Este análisis se centra en la actividad económica de servicios del sector terciario, particularmente en el ámbito del desarrollo de campañas de comunicación para organizaciones y cambios sociales. Su finalidad consiste en examinar una entidad y diseñar tácticas de comunicación que optimicen las relaciones interpersonales y los efectos culturales dentro de ella.

1.4. Localización o alcance de la solución

En el caso de que se establezca el tema aprobado, este proyecto de investigación está previsto que se lleve a cabo de octubre a diciembre de 2023. Los siguientes son los pasos para ejecutarlo: la conformidad con la metodología AQP establecida dentro de los parámetros de este estudio, lo que permitirá la creación de un remedio para los empleados de la empresa Saltalto.

II. Descripción de la investigación aplicada o innovación

2.1. Problema de investigación

Es evidente que, en la actualidad, el mundo entero enfrenta una problemática relevante respecto a la filtración de datos personales y empresariales en el contexto digital. Sin la debida autorización o consentimiento previo, la información personal y privada perteneciente a personas u organizaciones puede ser robada y utilizada. Por consiguiente, resulta primordial ejercer responsabilidad al tomar medidas adecuadas para proteger los datos y tener conciencia sobre los riesgos asociados con la filtración de información.

En un mundo basado en datos, la filtración puede impactar a una amplia cantidad de individuos, llegando incluso a afectar a cientos de millones. La digitalización ha generado un aumento exponencial en la cantidad de información transferida durante los procesos, lo cual ha sido aprovechado por ciberdelincuentes (Hill y Swinhoe, 2022).

En Latinoamérica la difusión no autorizada de información ha sido una cuestión recurrente en los últimos años. En la mayoría de los países de la región, se han obtenido y comercializado datos personales de millones de usuarios que utilizan una conocida plataforma digital (Facebook) sin su consentimiento. Esto ha generado gran inquietud por la privacidad y seguridad de la información. Es cierto que en algunos países latinoamericanos aún no se ha desarrollado completamente una cultura relacionada con la ciberseguridad debido a diversos factores, como falta de conciencia sobre la importancia del resguardo adecuado de datos, carencia de recursos para implementar medidas apropiadas y ausencia de regulaciones sólidas para proteger dicha información.

Se sabe muy bien que en Perú ocurre algo similar. La filtración no autorizada tanto corporativa como individual es un problema persistente desde hace varios años atrás. En mayo de 2020, dos especialistas en seguridad informática reportaron el hurto perpetrado por una multitud de 500 individuos que lograron vulnerar el sistema RENIEC destinado al subsidio universal y acceder a los datos personales tanto del beneficiario como los utilizados para suplantar identidades, llegando a sustraer casi un millón de soles. (Linares, 2022).

PROBLEMA: La falta de conciencia en materia de seguridad de la información es un aspecto relevante por considerar en Saltalto. La empresa se enfrenta a una situación crítica debido a la carencia de políticas efectivas que promuevan la protección y el manejo adecuado tanto de datos corporativos como personales. Esta problemática podría derivar en una tragedia si no se toman medidas oportunas para prevenir posibles filtraciones o vulnerabilidades informáticas. Ya que la circunstancia en la que estamos la ciberdelincuencia está en constante acecho y las personas en general no son consciente de los peligros que enfrentan a cada día como extorsión por la información obtenida o fraudes financieros por estafas.

CAUSA: En nivel mundial existen varios tipos de causas entre unas de ellas es la filtración de la información a nivel empresarial ya que presenta un riesgo significativo para la privacidad y seguridad personal por motivos como pérdidas y robos de dispositivos personales o como dispositivos corporativos. Otra causa sería los empleados con malintencionados que de una u otra manera buscará sacar provecho de las redes sociales de la empresa con campañas fantasma de oportunidad de trabajo o mandando enlaces maliciosos a nuestros clientes

potenciales teniendo como finalidad obtener la información privada de los clientes o empresas aliadas a Saltalto.

CONSECUENCIAS: Si el problema de filtración de información de los clientes y trabajadores persiste, la información confidencial de la empresa quedará expuesta y en grave riesgo de ser comercializada por individuos u organizaciones que buscan beneficiarse. Los datos personales de los usuarios afectados no solo ponen en peligro su privacidad digital, sino también su seguridad física al exponer sus direcciones residenciales. además, se pone en peligro la seguridad financiera tanto del cliente como del negocio debido a la divulgación inapropiada e ilegal de información delicada relacionada con finanzas corporativas. Por lo tanto, este problema representa un gran riesgo para cualquier usuario actual o potencialmente interesado en utilizar esta plataforma.

APORTE: Ante esta coyuntura, se plantea instaurar una cultura de seguridad de la información que contemple el fortalecimiento de los sistemas de protección en nuestra entidad con el fin de salvaguardar nuestras cuentas empresariales y garantizar la actualización del software. Asimismo, se sugiere efectuar cada quince días copias de respaldo no solo de la información del personal sino también de los clientes, esto a modo preventivo ante eventuales pérdidas.

2.2. Justificación

Justificación Teórica

Es relevante subrayar que el presente estudio se origina de la urgencia por encontrar una solución pronta y eficaz para evitar filtrada de información crítica en la organización, así como comprender por qué se producen estas y buscar las formas y modalidades en que ocurren estos incidentes. Simultáneamente, con el propósito de informar, la investigación persigue adquirir datos acerca del estado

presente de las filtraciones en la compañía: incluyendo tanto el número de usuarios perjudicados como el tipo de información divulgada, los procedimientos utilizados para su detección y extracción ilícita y las causas que motivan a individuos dedicados a esta actividad que compromete la confidencialidad del público.

Justificación Metodológica

Para alcanzar los propósitos de la investigación, se ha llevado a cabo un método sistemático y riguroso. Se han empleado adecuadamente técnicas cuantitativas de análisis y síntesis acordes al modelo utilizado.

Justificación Práctica

La necesidad de abogar por la adopción de una cultura estructural de seguridad de la información y la aplicación adecuada de medidas preventivas para evitar fraudes o violaciones de datos es la fuerza motriz de la realización de esta investigación. El objetivo es poner fin a diversos medios de sustracción y robo de información privada de la empresa.

Justificación Social

En la actualidad, se desconoce con precisión el grado de exposición de la información tanto de los trabajadores como corporativa perteneciente a nuestra empresa Saltalto, así como también se ignora la frecuencia en que ocurren estos incidentes. Por consiguiente, resulta esencial realizar esta investigación con el fin de establecer la situación y grado actual de protección sobre los datos confidenciales del personal, brindándoles una comprensión más profunda acerca del peligro que representa su exposición.

Por otra parte, en el marco de las óptimas prácticas empresariales, se promueve la investigación para presentar diversas formas y mecanismos de seguridad que puedan aplicarse tanto por nuestra página de Facebook como a fin

de prevenir la filtración de datos. Asimismo, buscamos ampliar el conocimiento del usuario al enseñarle cómo identificar posibles publicaciones falsas o enlaces engañosos que podrían llevarlo a entregar información personal propia o correspondiente a los colaboradores de Saltalto.

2.3. Marco referencial

Antecedentes de la investigación

Antecedentes Nacionales

Méndez estudió los enfoques de seguridad de la información en 2022 para apoyar los esfuerzos de gestión de TI de la Municipalidad de Yungay. El objetivo principal, indisolublemente ligado a la seguridad de la información, fue maximizar la gestión técnica en materia de seguridad informática (hardware, software, operación y servicios). Veinticinco usuarios de las entidades municipales mencionadas conformaron la muestra de la investigación. Para llevar adelante esta investigación se empleó un diseño experimental y aplicativo debido a que los datos fueron recolectados en tiempo real. Asimismo, se utilizó una metodología descriptiva simple para esquematizar dicho diseño. En cuanto a los instrumentos empleados para recopilar información, se utilizaron tanto encuestas como entrevistas. Los resultados indicaron que la solución propuesta resulta ser superior al método actual con un nivel significativo del 2.5%. Por lo tanto, cabe destacar que dicha solución puede considerarse como una alternativa adecuada al problema.

Un estudio sobre la aplicación de la norma ISO 27001 y su efecto en la seguridad de la información en una organización privada fue realizada en 2021 por Rodriguez et al. El objetivo principal del estudio era evaluar los efectos de su utilización. Se incluyeron en la muestra 30 trabajadores de esta empresa. Se utilizó un diseño preexperimental como método de investigación, empleando una

metodología cuantitativa como instrumento para obtener los resultados pertinentes. Los resultados ponen de relieve lo crucial que es aplicar la norma ISO 27001 para garantizar los tres pilares esenciales de disponibilidad, confidencialidad e integridad; como también garantizar una mayor protección a nivel general sobre toda información sensible que maneje esta organización empresarial. En resumen, se propuso que las políticas y procedimientos de la empresa tienen un impacto significativo y deben seguirse estrictamente para lograr el objetivo principal, que es proteger con éxito todos los datos pertinentes para su correcto funcionamiento interno o externo contra cualquier amenaza o vulnerabilidad potencial que pueda existir en esta área en particular dentro del mercado actual.

Dávila y Dextre (2021) realizaron una investigación sobre el desarrollo de un programa de gestión de vulnerabilidades de seguridad informática con el objetivo de reducir la frecuencia de ataques que enfrenta actualmente la policlínica AMC. Para llevar a cabo esta investigación, fue imperativo conocer el nivel actual de seguridad informática del policlínico, ya que nos basamos en él para determinar con qué precisión están protegidos y qué medidas tomar para mitigar esta situación. Además, fue necesario analizar los datos para determinar el origen exacto de estos ataques y cómo están accediendo a los datos de la empresa. Finalmente, entender que es lo exige actualmente la norma NTP ISO 27001:2014, para poder llevar las nuevas iniciativas en esa línea, de esta manera se puede mejorar las vulnerabilidades y sobre todo cumplir con lo exige la ley.

Se sugiere crear un sistema de gestión para manejar los datos sensibles de la empresa que pueda soportar la inexperiencia que pueda tener un usuario para acceder a ellos. Huincho (2019) realizó un estudio donde se requiere un sistema de gestión para analizar las vulnerabilidades informáticas de la comisaría regional de

Huancavelica. Esta investigación se dio en vista de que se estaba vulnerando la seguridad de la información, los elementos de seguridad que estaban utilizando no eran los mejores y sobre todo la forma en que lo estaban utilizando. Para evitar que se filtre la información o que piratas informáticos accedan a los servidores de la comisaría, han propuesto que, para acceder a la información, cada usuario se registre y se les conceda un posible acceso a otras plataformas. Es responsabilidad de todos los miembros de la organización garantizar que la información en los servidores o en la nube esté siempre segura, por lo que se sugirió que todos los empleados reciban formación sobre este tema y aprendan técnicas de manejo adecuadas. Por otro lado, la organización debe implementar de inmediato mecanismos de seguridad y brindar a los usuarios capacitación especial para mantenerla segura. En resumen, la información se ha convertido en uno de los recursos más importantes para todas las empresas. Es esencial que cualquier procedimiento interno se base en ella para llevarse a cabo. Ser flexible y satisfacer las demandas del mercado es imposible sin los mecanismos suficientes para manejarla.

Antecedentes Regionales

Parra (2022) realizó una investigación acerca de la implementación de la Protección contra Pérdida de Datos (DLP) como parte integral de una estrategia de seguridad para abordar los variados problemas de filtración en Colombia. El objetivo principal consistió en explicar cómo las organizaciones se ven afectadas cuando no se establecen medidas adecuadas que garanticen la seguridad y protección de la información. La muestra incluyó variedad de recursos académicos, tales como libros, bibliotecas virtuales, revistas científicas e informes corporativos. Se utilizó un enfoque cualitativo para llevar a cabo este estudio, utilizando como

instrumento principal la investigación documental tecnológica. Los resultados obtenidos sugieren que DLP puede ser una herramienta efectiva para monitorear y controlar la filtración de datos ante diferentes eventos relacionados con la seguridad. En conclusión, resulta patente que la información constituye uno de los bienes más valiosos en cualquier entidad y su apreciación se vincula estrechamente con las tácticas utilizadas para asegurar su salvaguardia y resguardo.

Basándose en la metodología ISO 2700, Terán (2021) realizó un estudio sobre la seguridad de la gestión de la información en las empresas públicas ecuatorianas. El objetivo principal fue realizar múltiples investigaciones sobre el tema de robo de información, tomando en cuenta el enfoque para mantener y garantizar la seguridad de la información y gestionar más eficazmente los riesgos. La muestra estuvo conformada por diferentes entidades públicas y se empleó un diseño de estudio descriptivo. En el esquema clasificatorio, que sirvió de instrumento, se incorporaron tres preguntas sobre seguridad de la información con mapeo sistemático. Dado que MAGERIT sigue siendo una herramienta eficaz para reducir las amenazas y los riesgos durante sus procesos, incluido el mapeo, los resultados obtenidos fueron pertinentes y controlaron los factores relacionados con la seguridad de la información; además, proporcionó requisitos verificables que el software utilizado en el sector del desarrollo industrial debería tener en cuenta. En resumen, se ha descubierto que un prototipo gestiona los riesgos mediante técnicas destinadas a elevar el listón de la seguridad y el secreto informáticos en los organismos gubernamentales. Aquí se pone de manifiesto lo estrechamente relacionado que está el proceso de optimizar de forma segura toda la información

disponible actualmente dentro de las estructuras estatales con la función crítica que desempeña la seguridad de la información.

Con el fin de analizar y comprender el comportamiento de la seguridad de la información en Colombia, Cano y Almanza (2019) realizaron un estudio sobre la evolución de la seguridad de la información en esa nación. La muestra fue de 186 especialistas en seguridad de la información. Se realizó un estudio descriptivo y se empleó como herramienta un cuestionario con 40 preguntas divididas en 7 áreas. Los hallazgos validan las tendencias mundiales reportadas por las empresas de esta industria y demuestran la importancia básica del tema para las empresas y los problemas que enfrentan en la actualidad. En resumen, se puede concluir que las empresas deben guiarse por modelos y planes de acción que les permitan modificar sus operaciones en curso dentro de los parámetros establecidos por los programas de seguridad de la información en vigor para seguir adelante con el proceso de desarrollo. Esto les permitirá fortificar los estándares necesarios para crear competencias críticas que les permitan anticiparse y no sólo protegerse en un mundo cada vez más impredecible y cambiante.

Gonzalez (2020) realizó una investigación de la situación actual en las organizaciones con respecto a la seguridad informática en Colombia. El propósito general del estudio fue documentar las debilidades más significativas que actualmente utilizan los hackers para vulnerar la seguridad de las organizaciones y cuáles son las consecuencias de ello, para sustentar estos hechos se están incluyendo las estadísticas que está enfrentando actualmente Colombia para todos los sectores, sobre todo el empresarial que viene siendo el más atractivo para los ciberdelincuentes. Luego de haber definido exactamente el objetivo, es necesario entrar al segundo objetivo que es revisar los principales comportamientos que

tienen los hackers al momento de atacar, pero sobre todo analizar los que, si llegan a ser exitosos, no olvidemos que Latinoamérica es una de las regiones más atacadas a nivel mundial, justamente porque son los que menos invierten en seguridad de la información, este hecho genera que las organizaciones estén en todo momento expuestas al mundo. Finalmente, se busca que el usuario pueda entender de una mejor manera como funciona este mundo, mediante reportes simples de todos los ataques que reciben y cuáles son las consecuencias de no ser un usuario responsable, esto llevado de la mano de constantes capacitaciones y sobre todo controles dependiendo de cada puesto de trabajo, es fundamental que todos puedan entender cuáles son los pasos a seguir para que la organización pueda tener una forma segura de navegar y consultar información interna sin vulnerar a la mencionada.

Cifre (2020) realizó un estudio sobre vulnerabilidades de servidores en la nube privada, esto se lleva a cabo de acuerdo con cada organización y ellos deben su información enviando todo a una nube privada para de esa manera utilizar las características de seguridad que tienen las aplicaciones que ofrece el mercado actual. Es necesario establecer políticas de seguridad a nivel internacional que abarque un proceso integral de protección de los activos, directrices operativas claras, roles y responsabilidades definidos para los usuarios, documentación precisa y completa requerida para el cumplimiento normativo, así como una serie de indicadores específicos para evaluar la vulnerabilidad y madurez organizacional.

Antecedentes Internacionales

Sánchez (2017) realizó una investigación sobre los intangibles de la ciberseguridad, en vista de cómo hoy en día se están utilizando cada vez más dispositivos para trabajar. Es fundamental mencionar que el 96% de las empresas

no están preparadas para un ataque cibernético, si bien es cierto están invirtiendo y esta ya es una realidad que las empresas están enfrentando, las organizaciones no invierten lo que deberían en equipos o softwares para contraer estos ataques. Por otro lado, es importante mencionar que las compañías necesitan tener personas capaces de poder instalar estos softwares, ya que puede que obtengan estos servicios, pero si no tienen una buena configuración o actualización cada cierto tiempo no servirá de nada, ya que los hackers buscan cada día una nueva forma de atacar.

Ávila (2022), realizo una investigación en México sobre la posibilidad de crear una comisión o un área en el gobierno para la ciberseguridad, ya que actualmente el mundo está cada vez más virtualizado, es por ello, que se requiere que este tipo de implementaciones están reguladas para que en todo momento las empresas públicas y privadas sigan un régimen de seguridad de la información. En la era que estamos viviendo, nos damos cuenta de que es necesario asegurar bien la información que proporcionan los clientes o las empresas, ya que, es eso lo que hace que las estrategias están cada vez más dirigidas y es justamente lo que genera que seamos más vulnerables, debido a ello, la investigación lo que busca es regular y asegurar más la privacidad de las personas y empresas en el ámbito de seguridad de la información.

2.4. Bases teóricas

Variable: Filtración de datos

Definición

De acuerdo con Linares et al. (2019), la filtración de información se refiere a la apropiación o sustracción de datos en línea mediante el uso de herramientas

como cortafuegos y, principalmente, virus informáticos para extraer información ilícitamente. Además, Pérez Porto define la filtración como una actividad que conlleva el reparto de documentación e información personal, confidencial, valiosa y/o privilegiada.

Tecnologías de la información

De acuerdo con Linares et al. (2019), en el mercado se pueden encontrar una variedad de herramientas electrónicas que forman parte del concepto de las TIC, tales como televisores, teléfonos móviles, dispositivos audiovisuales, computadoras personales, laptops, tabletas y smartphones. No obstante, actualmente son las computadoras portátiles y los teléfonos móviles quienes ostentan una mayor usabilidad debido a que nos permiten acceder a numerosas plataformas digitales y aplicaciones informáticas que son esenciales para el manejo diario e ininterrumpido de Internet.

Responsabilidad

De acuerdo con Samaniego y Ponce (2021), la gran mayoría de los ataques a la información confidencial en línea son llevadas a cabo por sujetos que, ya sea intencionalmente o no, pueden poner en riesgo nuestra privacidad y ocasionar perjuicios significativos.

Cultura de interacción

Linares et al. (2019) exponen cómo la interacción con las Tecnologías de la Información y Comunicación se ha convertido en una actividad cotidiana que se construye a través de la relación con los dispositivos electrónicos, y se observa principalmente en el grupo poblacional conocido como millennials y centennials.

Para ellos, el propósito de esta interrelación no solo radica en consumir contenido, sino también en compartirlo mediante la reproducción de archivos audiovisuales, redistribución y difusión de estos.

Implicación de las redes sociales

La divulgación de datos se erige como una preocupación relevante en los ámbitos políticos, sociales y económicos. En las plataformas digitales, la magnitud de esta amenaza y sus variadas fuentes resultan inquietantes; según Linares et al. (2019), el auge de estas redes ha posibilitado nuevas formas de cometer delitos como el fraude online, el robo virtual y otros delitos.

Variable: Seguridad de la información

Definición

La ISO/IEC 27001 define la seguridad de la información como el conjunto de acciones preventivas y correctivas adoptadas por una organización o sistema técnico para garantizar la seguridad y protección de los datos, según Altarmirano (2020).

Pilares o principios

Según Samaniego y Ponce (2021) en referencia a los tres pilares de la seguridad de la información debe basarse en tres recursos: la confidencialidad como la gestión de privilegios para permitir el uso autorizado, el cifrado de la información para impedir el acceso no autorizado y la autenticación del individuo para confirmar que es quien dice ser. El segundo es la integridad, que se mantiene mediante la supervisión de la red, las copias de seguridad frecuentes, el despliegue de sistemas de control y la aplicación de políticas de auditoría para asegurarse de

que los datos no se extravían ni acaban en manos equivocadas. El factor más importante es la disponibilidad, que se consigue tomando precauciones preventivas contra posibles obstáculos y haciendo que estén disponibles cuando se necesiten.

Ciberseguridad

La ciberseguridad, según Valoyes (2019), es la salvaguarda de los recursos de información frente a posibles amenazas que puedan comprometer la confidencialidad, integridad y disponibilidad de los datos procesados, almacenados o transferidos a través de sistemas en red.

Seguridad en dispositivos móviles

Samaniego y Ponce (2021) brindaron recomendaciones sobre la implementación de medidas de seguridad en dispositivos móviles, entre las cuales se destacan: activar el bloqueo automático después de un período determinado, establecer contraseñas previas al acceso a aplicaciones, evitar la función de autocompletado para usuarios y contraseñas, ser precavido al instalar aplicaciones por terceros y abstenerse de almacenar información confidencial en el dispositivo.

Política de seguridad de las contraseñas

Según afirman Samaniego y Ponce (2021), resulta imperativo generar contraseñas robustas mediante la utilización de caracteres diversos, emplear claves diferentes entre sí, modificarlas periódicamente y recurrir a la alternativa de guardar las contraseñas en tu dispositivo.

Riesgos y amenazas

Para Samaniego y Ponce (2021) existen diversas categorías de riesgos que afectan tanto a dispositivos como a individuos, entre los cuales se encuentran el phishing, una maniobra fraudulenta en línea dirigida al usuario, y el malware, es decir, programas maliciosos capaces de dañar los sistemas informáticos. A fin de evitar o reducir tales amenazas resulta fundamental implementar medidas de seguridad efectivas como la ocultación de señales inalámbricas y la protección del acceso a estas.

Desinformación en redes

Argemi (2019) señala que, en ocasiones la exclusividad en las redes sociales puede ser tan abrumadora que algunas personas, con el fin de descubrir lo que sucede detrás de esas publicaciones falsas, proporcionan información personal solicitada para acceder a dicha publicación; sin embargo, ignoran que están entregando toda su información privada.

ISO 27001

La Organización Internacional de Normalización creó la norma ISO 27001 para facilitar la administración de las normas de seguridad de la información. Planificar, ejecutar, verificar y actuar es el enfoque de proceso continuo sobre el que se fundamenta. La implantación de un sistema eficaz de seguridad de la información se rige por los requisitos establecidos por tal certificación.

2.5. Objetivo general y específicos

Objetivos Generales

1) Proponer un plan de cultura de seguridad de la información para evitar la filtración de datos de los trabajadores de la empresa Saltalto, 2023.

Objetivos Específicos

- Elaborar el diagnóstico situacional de la filtración de datos para proponer un plan de cultura de seguridad de la información para los trabajadores de la empresa Saltalto, 2023.
- Elaborar un plan de una cultura de seguridad de la información para evitar la filtración de datos para los trabajadores de la empresa Saltalto, 2023.
- Describir los beneficios de la cultura de seguridad de la información al evitar la filtración de datos para los trabajadores de la empresa Saltalto, 2023.

Viabilidad

Esta investigación se enmarca dentro de la temática de los cambios sociales y el desarrollo de campañas de comunicación en las empresas, ya que su objetivo es analizar una organización y desarrollar métodos de comunicación para fortalecer sus interacciones interpersonales y su efecto cultural. Así, el apoyo personal del equipo de sistemas de la empresa y la de un especialista en seguridad de la información, llevará a cabo las técnicas necesarias para recopilar los datos necesarios para realizar este proyecto, lo cual hace viable esta investigación.

Limitaciones

El estudio actual se centrará en la planificación de la aplicación con los trámites necesarios. No se incluirá ningún trabajo especializado de otros campos o especialidades como diseño gráfico, ingeniería o derecho. Se identificarán, explicarán y mostrarán todas las ubicaciones, independientemente de sus dimensiones, características, precio, alojamiento o identidad visual. También tenemos en cuenta la rotación de personal, que puede impedir la adopción de una cultura de seguridad porque Saltalto, al ser una empresa de comercio electrónico, sufre cambios internos de personal. En 2023, hubo ocho nuevas contrataciones y diez salidas.

2.6. Plan de actividades del proyecto

Estudio de situación actual

- Se llevará a cabo un análisis del estado actual de la empresa para determinar cómo se gestiona actualmente la seguridad de la información dentro de la organización. Con este fin, se utilizarán herramientas y programas informáticos para identificar las áreas problemáticas y los posibles puntos conflictivos. Basándonos en las respuestas de las veinte personas que participaron en el proceso de entrevistas, sabemos que actualmente no existe una política clara sobre el tratamiento de datos sensibles y que no hay defensas contra los ciberataques.
- Para implementar esta primera fase, se realizará con el soporte de la empresa Fortinet quienes son los líderes en seguridad de la información y ofrecen herramientas con costos asequibles mediante el uso de la nube.

- Por otro lado, se harán pruebas de estrés en el sistema para ver cómo reacciona el cliente interno, esto por supuesto, en un ambiente controlado y sin poner en riesgo la información que se tiene en la compañía.
- Finalmente, es importante entender que es una empresa con un público relativamente joven, ya que el 90% está entre los 25 y 30 años, por lo que son más vulnerables al tener acceso a redes sociales y manejar fácilmente el Internet, sin embargo, esto también es beneficioso para la compañía, ya que es un público que puede aprender de una manera más rápida y optar comportamientos rápidos.

Objetivos

- Mejorar la conciencia de seguridad de los empleados de la empresa.
- Reducir los riesgos de seguridad de la información.
- Proteger los datos de la empresa y sus clientes.

Estrategias

- Campaña de sensibilización: Para educar a los miembros del personal sobre las amenazas a la seguridad de la información y cómo salvaguardar la organización y a sí mismos, se llevará a cabo una campaña de concienciación.
- Formación: Los trabajadores que manejen datos sensibles o privados deben recibir formación especializada en seguridad de la información.
- Normas y procedimientos: Todo el personal aplicará y respetará normas y procedimientos claros y básicos de seguridad de la información.

- Cambio de cultura: La educación y formación constantes del personal, junto con la creación de un entorno de trabajo centrado en la seguridad de la información, fomentarán una cultura de seguridad de la información.

Tomando en consideración la diversidad de los trabajadores dentro de la organización, estamos abarcando como paso final la gestión de la resistencia al cambio bajo este contexto. Para ello estamos tomando las siguientes estrategias para abordarla:

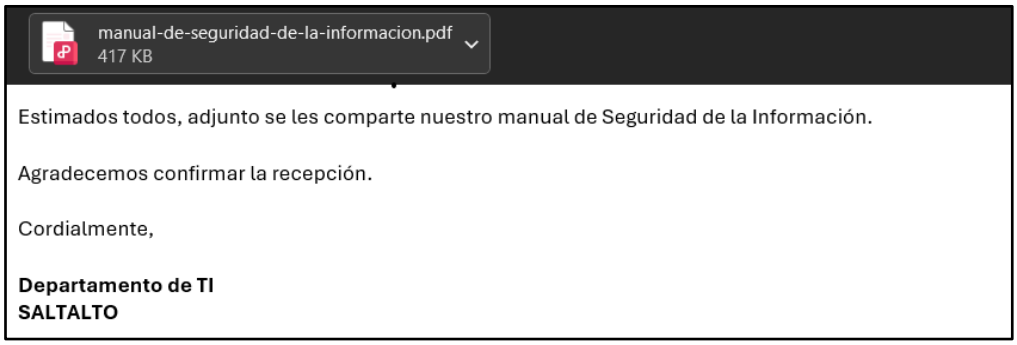
- Crear canales de comunicación inequívocos entre los distintos departamentos de la empresa, incluidos los de marketing, RRHH, etc. Fomentar la participación del personal en el proceso de transición formando grupos de trabajo y celebrando seminarios educativos.
- Gestión reactiva al tomar en cuenta las situaciones personales y familiares de los empleados y analizando el impacto que tendrá ello en su vida profesional y personal. Identificando las principales preocupaciones y temores de los trabajadores con relación al cambio, y abordándolos de manera efectiva mediante el diálogo y la negociación.
- Monitoreando constantemente el progreso del cambio, identificando posibles obstáculos y ajustando las estrategias según sea necesario. Plantear soluciones ofreciendo alternativas y de ser necesario explicando a los resistores los beneficios del cambio.

Acciones específicas

- Redactar un manual de seguridad de la información que se enviará a todos los empleados.
- Realización de cursos y talleres de formación sobre seguridad de la información.

Figura 1:

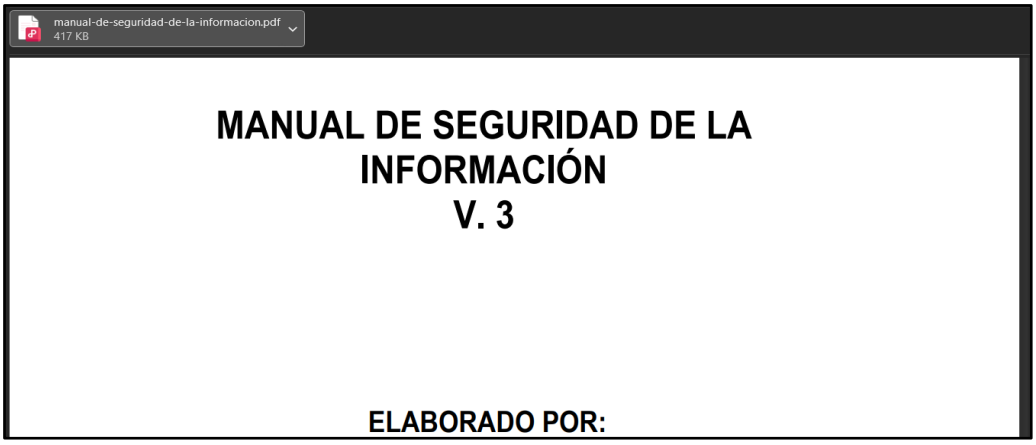
Envío de manual de seguridad de la información por email



Nota: Elaboración propia.

Figura 2:

Manual de seguridad de la información en formato PDF



Nota: Elaboración propia.

Se brindarán talleres de capacitación a toda la empresa con el apoyo del proveedor de seguridad TI Fortinet para enseñar cuales son los nuevos objetivos de la organización y sobre todo que entiendan cuál será la nueva cultura propuesta de ahora en adelante. Por otro lado, se presentará el plan de capacitaciones que haremos para se tenga claro en qué consiste esta nueva estrategia y cómo van a aportar al desarrollo de esta.

Figura 3:

Programa de capacitación del proveedor de seguridad Fortinet

Nota: Adaptado de Fortinet.com

La estructura del curso contendrá los siguientes módulos:

Figura 4:

Módulos del curso de concientización en seguridad de la información

Concientización sobre la seguridad de la información
Actores maliciosos
Ingeniería social
Ataques de suplantación de identidad
Seguridad de correo electrónico
Malware y ransomware
Protección de contraseña
Autenticación de múltiples factores
Seguridad de datos
Privacidad de datos
Control de acceso
Seguridad móvil
Amenaza interna
Política de escritorio limpio
Teletrabajo
Seguridad de conferencias web
Compromiso del correo electrónico empresarial
Propiedad intelectual
Consejos para un viaje seguro
Redes sociales
Gerentes: Marcos de seguridad de la información
Gerentes: Concientización sobre la seguridad de la información
Gerentes: Implementación y administración del servicio de capacitación y concientización en ciberseguridad de Fortinet

Nota: Adaptado de Fortinet.com

Todos los empleados deben haber recibido capacitación y ser evaluados tomando conocimiento del sistema de seguridad, es necesario que todos entiendan la responsabilidad que tienen en sus manos, en vista de que el mayor riesgo que tiene la empresa es el factor humano, ya que Perú por estadística es uno de los países más vulnerables y sobre todo más atacados de Latinoamérica.

Para esta etapa se harán videos institucionales para que los colaboradores puedan tener acceso a estos en todo momento luego de las capacitaciones, de esa

manera pueden revisarlos en caso tengan una duda o consulta. Se creará un espacio de consultas con la marca para gestionar cualquier situación nueva que se pueda presentar. Los resultados de las encuestas muestran que los empleados carecen de conocimientos sobre seguridad de la información, por lo que se sugiere formación para garantizar que todos sepan hablar con esta terminología. Finalmente, se apoyará mediante el envío de boletines de seguridad vía correo electrónico mostrando algunos consejos de seguridad de la información.

Figura 5:

Boletín de seguridad masificado a través de email

Nota: Recuperado de Pronabec.gob.pe

En esta etapa proponemos el uso del producto Crodwstrike Falcón en específico la característica de inteligencia artificial generativa, Charlotte AI.

Charlotte AI es un analista de seguridad de IA generativa que usa los datos de seguridad de mayor fiabilidad global y se mejora constantemente por medio un estrecho circuito de retro alimentación de los motores de detección de amenazas cibernéticas. Charlotte AI, ayudará a los usuarios de todo nivel a mejorar su capacidad de parar las infracciones y, al mismo tiempo, reducir la complejidad de las operaciones de seguridad. Los usuarios pueden realizar preguntas y recibir respuestas intuitivas desde la plataforma de Crodwstrike Falcón. A continuación, se presentan los distintos casos de uso observados en el entorno organizativo:

Caso de uso 1: Brindar potencial a cada usuario

Charlotte AI brinda la capacidad a todos los usuarios a comprender mejor las amenazas y riesgos que enfrenta la organización.

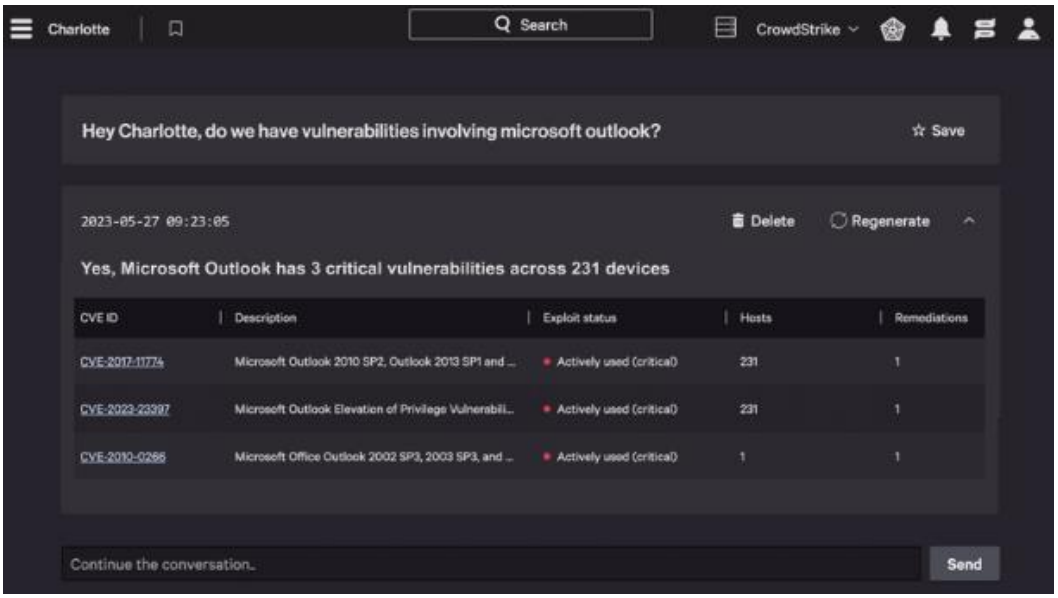
Por ejemplo, el administrador de seguridad de la información está preparándose para una reunión de la junta directiva. Por tanto, requiere recopilar información oportuna, relevante y procesable sobre la postura de seguridad organizacional que permita a la junta directiva tomar decisiones informadas y basadas en riesgos.

Se puede obtener información en tiempo real sobre el perfil de riesgo, el panorama de amenazas, el grado de vulnerabilidades significativas, la postura de seguridad actual, las necesidades de cumplimiento, las métricas de rendimiento de la seguridad de la información y otros aspectos de la empresa gracias a Charlotte AI.

En el siguiente gráfico, el administrador pregunta qué vulnerabilidad de sistema relacionadas a Microsoft Outlook se tienen actualmente en la organización:

Figura 6:

Uso de Charlotte AI en el caso de uso 1



Nota: Recuperado de Crowdstrike.com

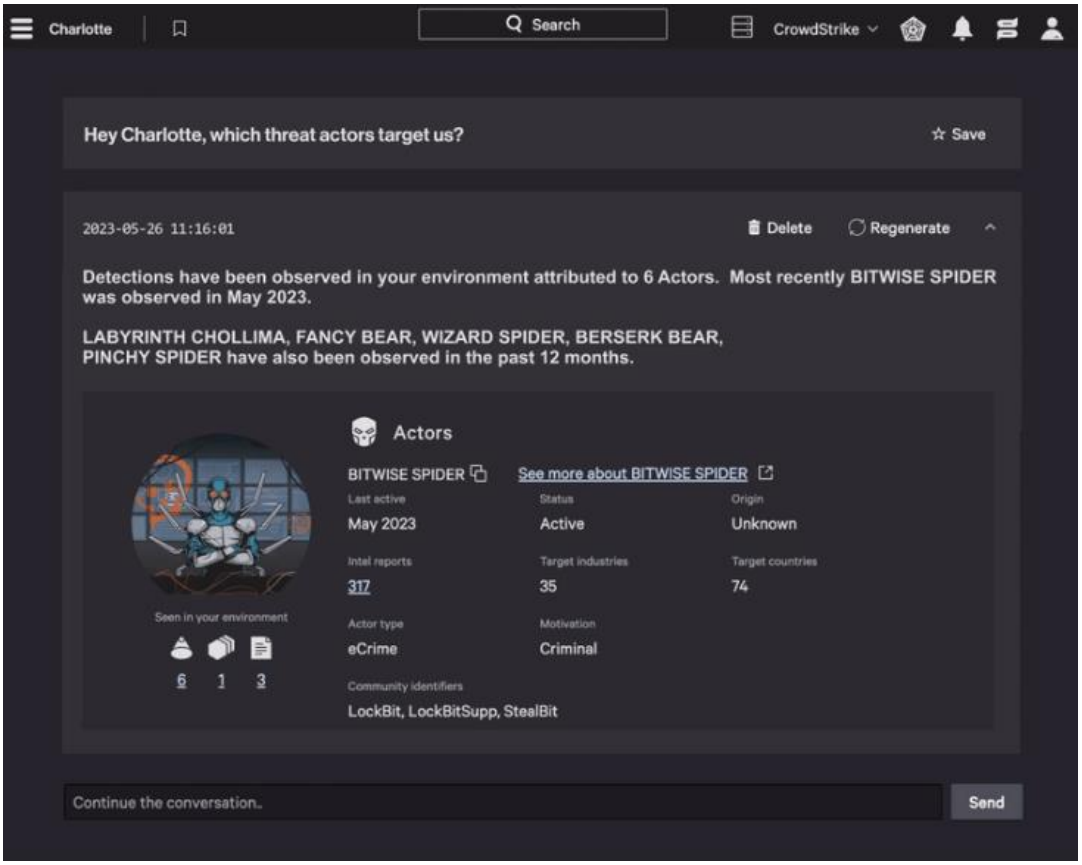
Caso de uso 2: Mejora en la búsqueda de amenazas

Para los profesionales de seguridad y TI poco experimentados, Charlotte AI brinda la posibilidad de tomar mejores decisiones en menos tiempo, dando una respuesta más rápida a incidentes críticos. Si se contrata un nuevo analista de seguridad, como un miembro de nivel 1 de un SOC, que recién está aprendiendo la plataforma Falcón, le ayudará a operar como un analista más avanzado con consultas simples. Esto es una inducción básica.

En el siguiente gráfico, un miembro recién contratado del área de seguridad pregunta sobre cuáles actores de amenazas atacan la organización:

Figura 7:

Uso de Charlotte AI en el caso de uso 2



Nota: Recuperado de Crowdstrike.com

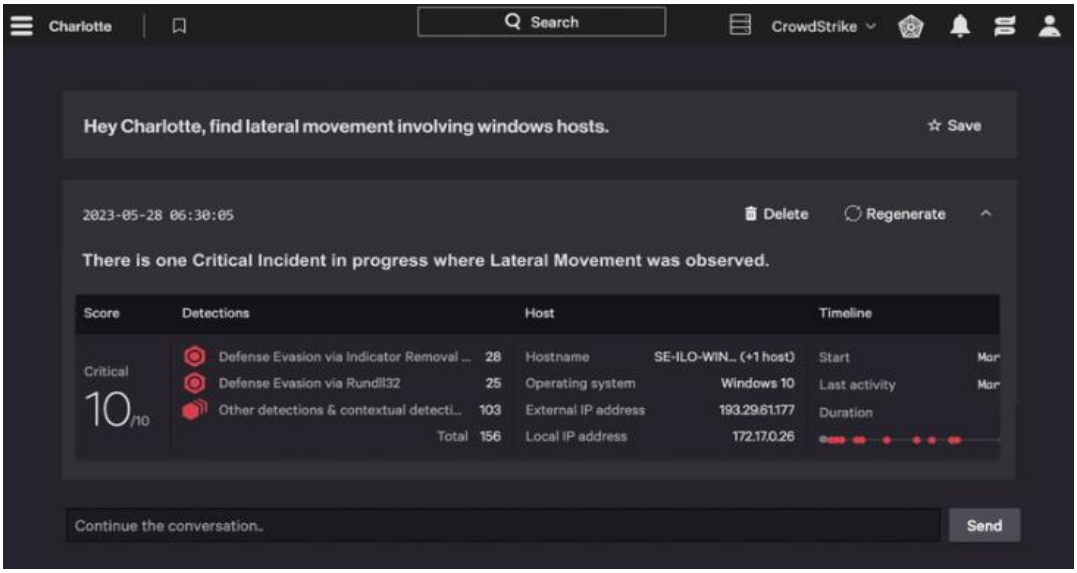
Caso de uso 3: Automatizar las tareas repetitivas

Charlotte AI minimiza el esfuerzo al automatizar tareas repetitivas y tediosas como lo son la recolección y extracción de datos y la búsqueda y detección de amenazas básicas, al mismo tiempo que simplifica la realización de acciones de seguridad más complejas. Charlotte AI puede automatizar las acciones de detección y respuesta a escala, en toda la organización o un grupo específico de equipos finales.

En el siguiente gráfico, un administrador de seguridad consulta sobre actividades sospechosas que involucran equipos Windows:

Figura 8:

Uso de Charlotte AI en el caso de uso 3



Nota: Recuperado de Crowdstrike.com

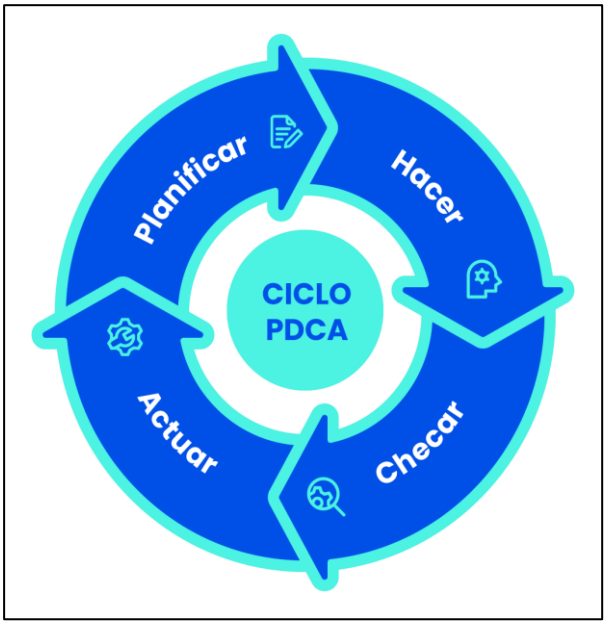
Resultados esperados

1) Una disminución de los riesgos para la seguridad de la información.
2) Una mayor comprensión de la seguridad de la información del personal.
3) Mayor protección de los datos para la empresa y sus clientes.
4) El establecimiento de una cultura de seguridad de la información en la empresa.

Utilizando la técnica del ciclo Deming (PDCA), este plan de trabajo se revisará y modificará periódicamente para comprobar su eficacia. Este planteamiento permitirá a la empresa responder a las necesidades de los clientes internos y externos, aumentar la eficacia, acelerar la productividad y adaptarse a los cambios futuros.

Figura 9:

Ciclo de Deming para garantizar la adaptación a los cambios



Nota: Recuperado de Tractian.com

2.7. Metodología del proyecto

Diseño metodológico

Tipo: La actual investigación adopta un enfoque aplicado, debido a que después de una revisión teórica exhaustiva, se ha diseñado una propuesta concreta y viable para resolver el problema identificado.

Enfoque: En el presente estudio se emplea un enfoque cuantitativo, dado que se llevarán a cabo encuestas para la recolección de datos precisos y concretos que permitan obtener resultados numéricos. Esto resultará fundamental para reunir la información necesaria, que contribuirá significativamente al establecimiento de las conclusiones del análisis.

Diseño: El estudio es de naturaleza no experimental, dado que ningún factor puede ser manipulado, controlado o alterado durante el proceso. Asimismo, se trata de un diseño transversal ya que la recolección de datos tendrá lugar en un único momento. Por otro lado, su diseño es descriptivo debido a la literatura disponible y los antecedentes que respaldan el acceso a la muestra del estudio.

Nivel: La asociación significativa entre las variables de seguridad de la información y filtración de datos se examina utilizando el enfoque correlacional.

Diseño muestral

La muestra se diseñará a través de la participación de los trabajadores de la empresa Saltalto, 2023.

Población

La población que se escogerá para la investigación es de 20 personas.

Muestra

La muestra escogida en base a la población es de 20 trabajadores de la empresa Saltalto, que comprenden las siguientes áreas: Gerencia, Administración, Comercial, Marketing y Logística.

Técnica de recolección de datos

El Taller de Investigación Aplicada e Innovación, creado en el ciclo 2024-0, fue el escenario del proceso de recogida de información. Para conocer la relación entre la seguridad de la información y la fuga de datos, en este estudio se administraron diez preguntas a través de un cuestionario, en el que se empleó la técnica de la encuesta.

Técnicas estadísticas de procesamiento de la información

En un primer momento, se recopilaron datos mediante un cuestionario prediseñado para determinar el nivel de comprensión de la seguridad de la información y cómo afecta a la filtración de datos. Tras la recogida de datos, se completó el análisis estadístico pertinente y se tabularon los datos para su posterior estudio.

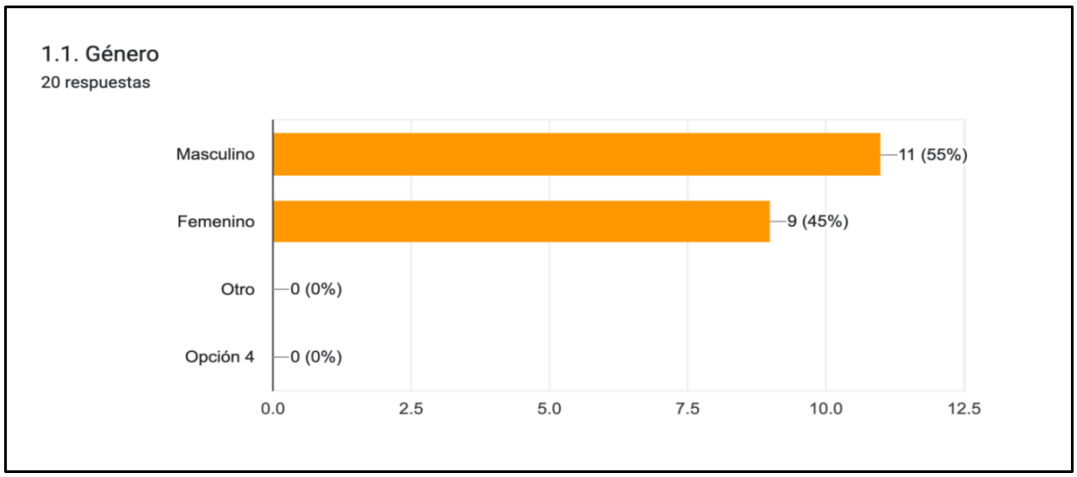
Resultados

Análisis descriptivo

Resultados de encuesta

Figura 10:

Resultados pregunta 1

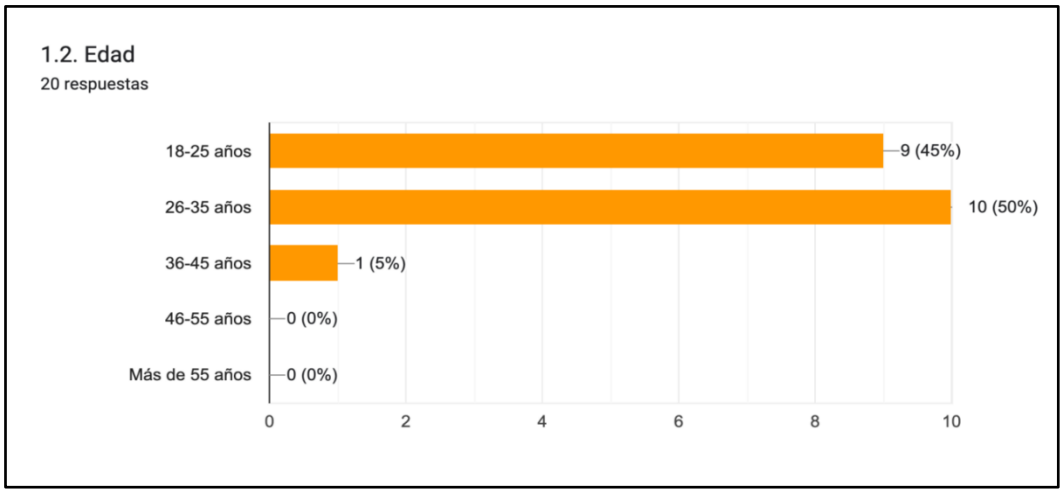


Nota: Elaboración propia.

Respondieron al estudio nueve mujeres y once hombres. Veinte personas en total respondieron a los cuestionarios que utilizamos para nuestro estudio.

Figura 11:

Resultados pregunta 2

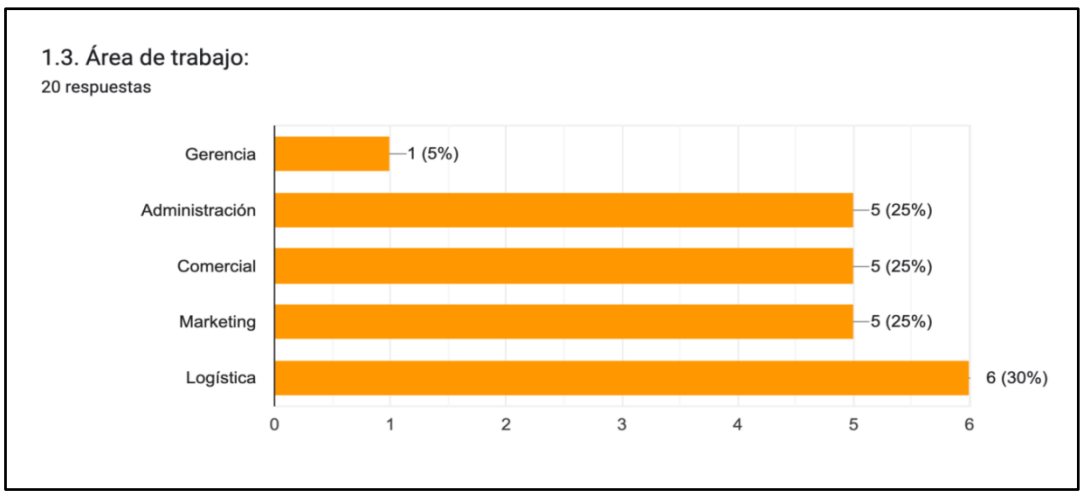


Nota: Elaboración propia.

En conclusión, Saltalto es una organización joven con metodologías de trabajo únicas. El rango de edad oscila entre los 18 y 25 años, con 9 personas que representan el 45%; de 26 a 35 años, con 10 personas que representan el 50%; y en el caso de 36 a 45 años, con el director general, que se encuentra en el rango de jóvenes que buscan cambios constantes en su organización. Saltalto tiene la cultura de contratar gente joven porque cree en sus capacidades y les da oportunidades a pesar de no tener muchos años de experiencia.

Figura 12:

Resultados pregunta 3



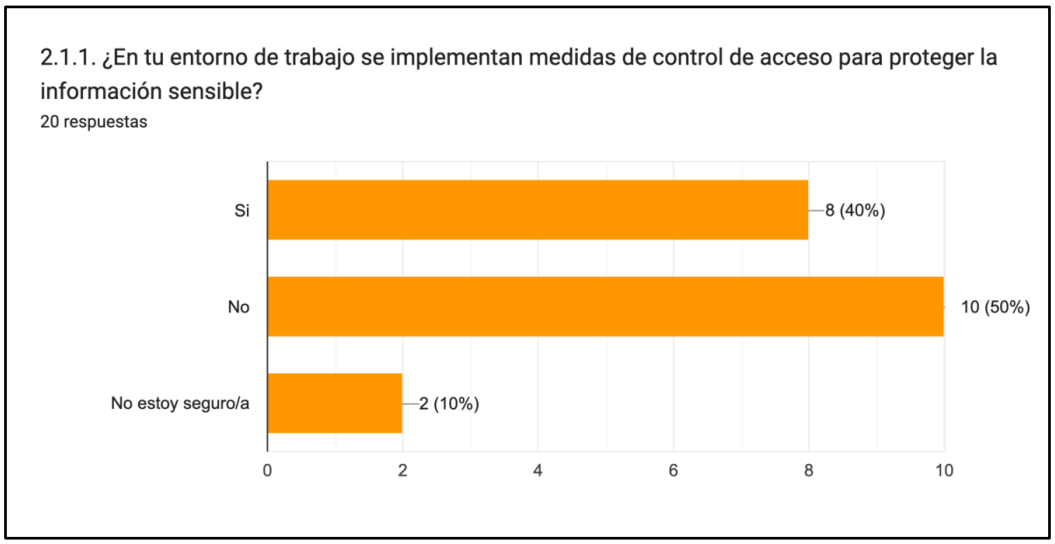
Nota: Elaboración propia.

Como se mencionó se hizo una encuesta a todos los miembros de la organización, la cual está representada en diferentes áreas, por ende, se posee un control de acceso distinto. La Gerencia representa un 5%, el 25% es Administración que está compuesta por personal como la administradora, coordinadoras, asistente administrativo, tesorería, el 25 % es área de comercial que está representada por el personal de ventas, head de comercial, planeador de productos. El 25% es área

de Marketing que está representada por head de marketing, asistentes de marketing, asistente de contenido, diseñadoras. Mientras que el 30% es área de Logística, que está representada por head de logística, asistente de compras, asistentes de embarques, asistentes de despacho. Cada área mencionada tiene procesos y sistemas distintos que a su vez se complementan.

Figura 13:

Resultados pregunta 4

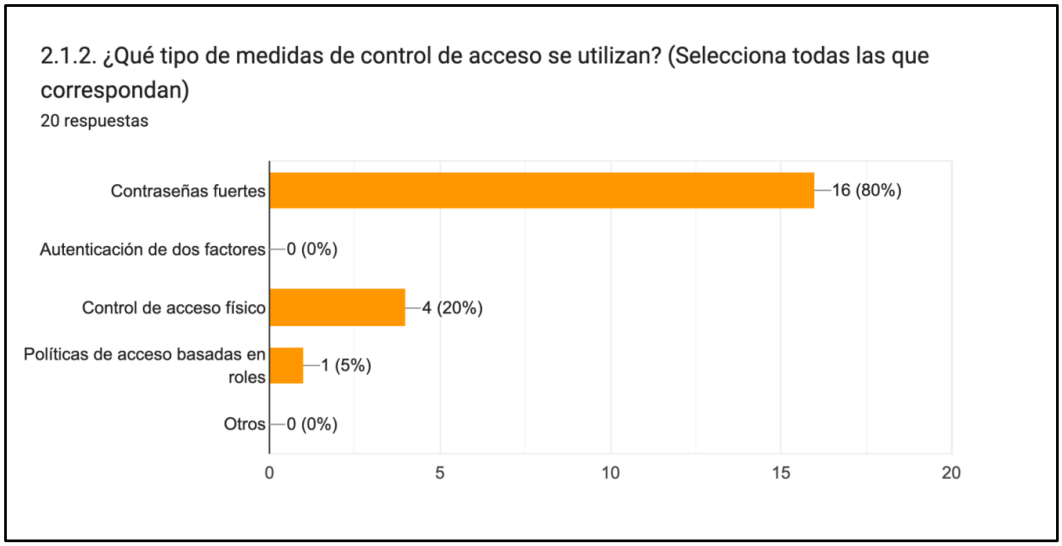


Nota: Elaboración propia.

Por medio de esta pregunta nos damos cuenta que un 50% de los miembros de la organización no cuentan con medidas de protección a la información por motivos como la falta de interés propia o falta de capacitación en la organización, si bien el 40% responden que, si se implementan estas medidas, es debido a que hay alta rotación de personal donde las personas más antiguas de la empresa buscan capacitarse y seguir vigente en la organización, por ende, hay un 10% de miembros que aún no saben si se implementan estas medidas.

Figura 14:

Resultados pregunta 5



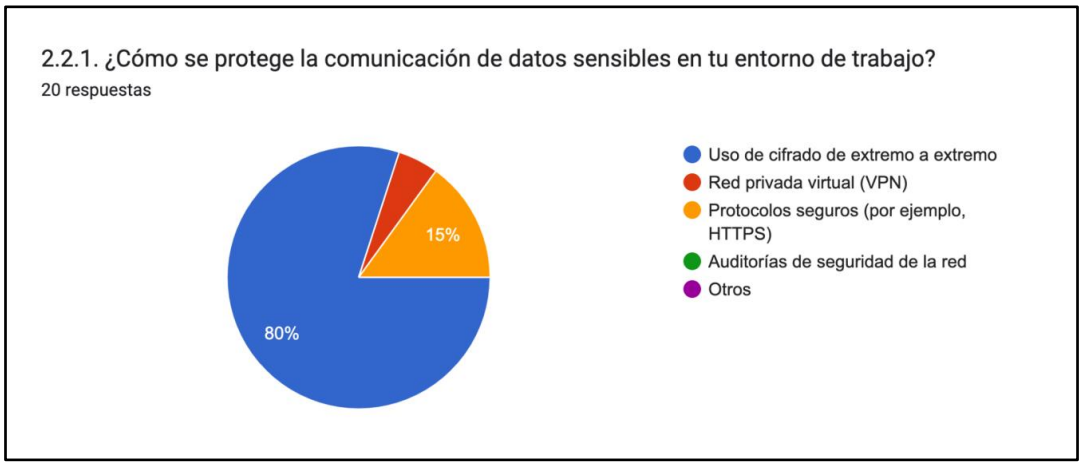
Nota: Elaboración propia.

En la empresa el 80% de miembros de la organización como medida de control aplican el de tener contraseñas fuertes, que se refiere a que son contraseñas complejas para cada correo o sheet que usualmente usan.

Mientras que el 20% y 5% representa un control de acceso físico, con huellas al momento de sacar productos de almacén o al momento de realizar las compras con los tokens digitales, el 5% es de las personas que trabaja por medio de roles que son brindadas por su respectivo head para sacar alguna información requerida previamente, para uso de una sola vez.

Figura 15:

Resultados pregunta 6

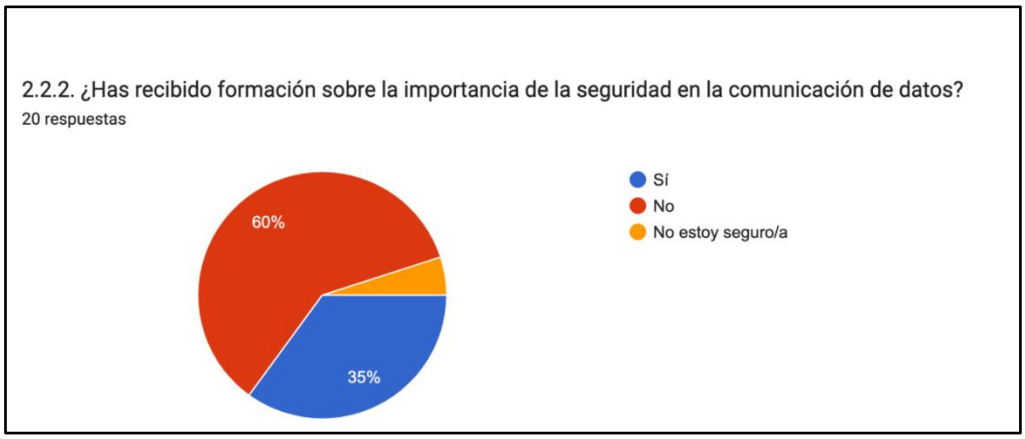


Nota: Elaboración propia.

En la encuesta se evidenció de que los miembros de la organización usan en un 80 % el cifrado de extremo a extremo para proteger datos sensibles, ya que es una medida de seguridad crucial en la comunicación digital. Esto se refiere a un método de cifrado en el que solo los participantes autorizados en una conversación pueden descifrar los mensajes. Mientras que un 15% y un 5% protegen su información mediante protocolos seguros como el https o red privada virtual VPN, esto debido a que posiblemente sepan de estos métodos de protección de la información.

Figura 16:

Resultados pregunta 7

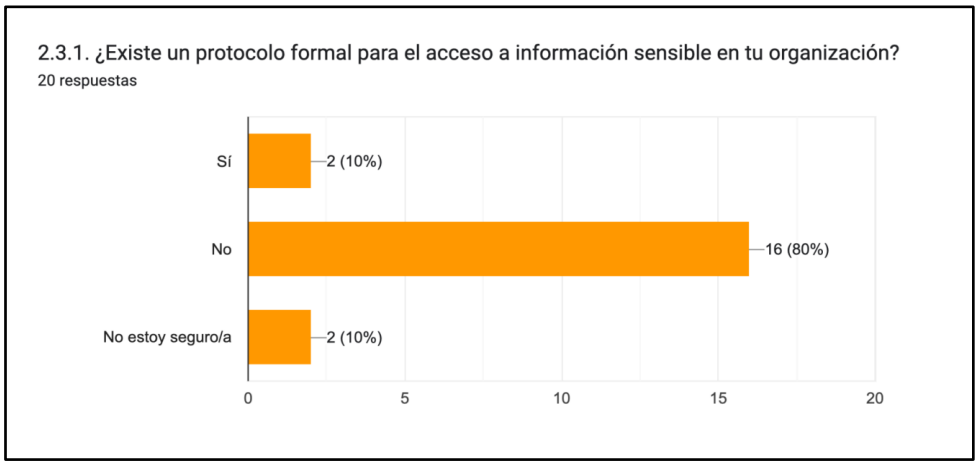


Nota: Elaboración propia.

Un 60 % de la organización no ha recibido formación sobre la importancia, ni en sus anteriores trabajos ni en la empresa actual, es un punto por tomar en cuenta para la programación y capacitación de las herramientas próximas a implementar en la empresa con relación a seguridad de la comunicación de datos. Un 35% si ha recibido formación de ello, por los diferentes puestos previos a los que han laborado antes de llegar a Saltalto o por capacitaciones previas. El 5% no está seguro debido a que el tema de la importancia de la seguridad lo ven como un tema complejo y por ende no están seguros de haberlo aprendido.

Figura 17:

Resultados pregunta 8

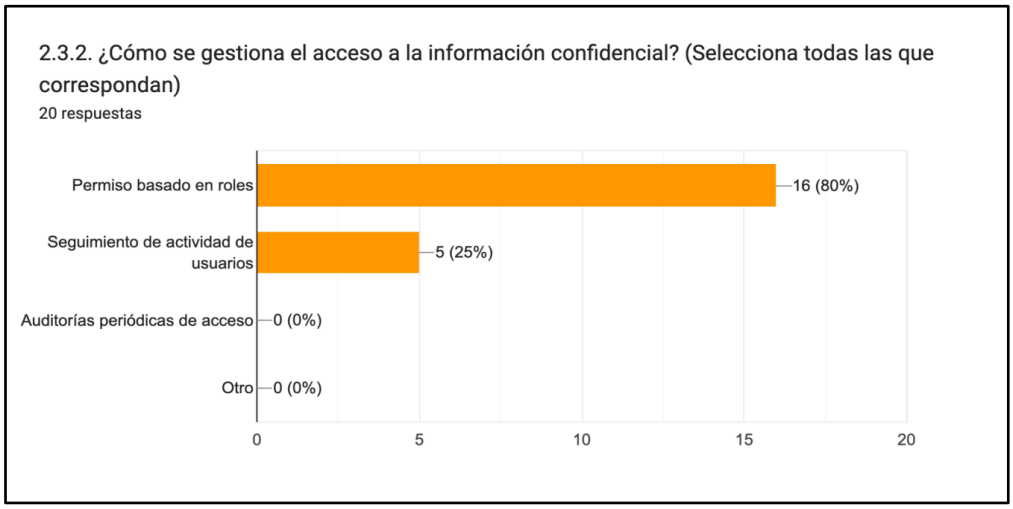


Nota: Elaboración propia.

El 80 % menciona que no existe un protocolo formal para el acceso a información sensible en la organización, El 10 % de personas que dijeron lo contrario, vienen siendo de gerencia y uno de los heats de las áreas, que con esta encuesta también pueden darse cuenta de que no se ha proyectado el protocolo requerido y les sirve para tomar las acciones necesarias y un plan de acción.

Figura 18:

Resultados pregunta 9



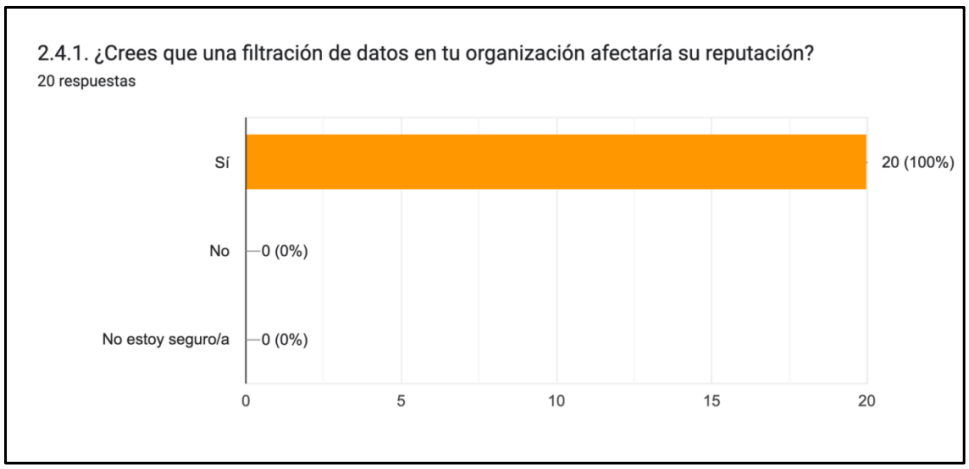
Nota: Elaboración propia.

En Saltalto el acceso a la información se gestiona en su gran porcentaje al permiso basado en roles que representa un 80 %, esto debido a que cada área

tiene los accesos restringidos para áreas que no compartan o tengan relación directa en lo laboral, en su gran mayoría es así, sin embargo, como mencioné otro sector 25% hace un seguimiento a las actividades del usuario mediante accesos compartidos, pero hasta cierto punto de visualización.

Figura 19:

Resultados pregunta 10

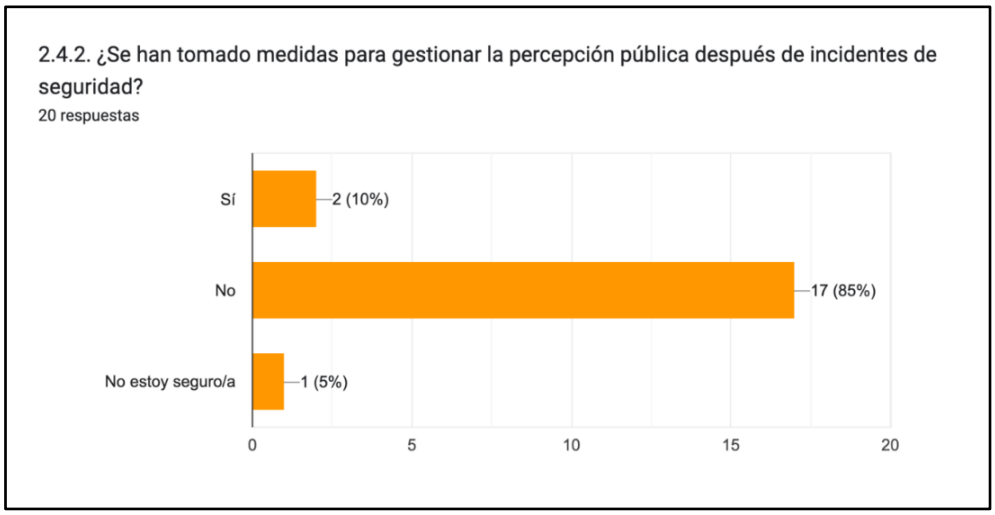


Nota: Elaboración propia.

Los 20 miembros, que constituyen el 100% de la organización, coinciden en que la filtración de datos perjudicará a la reputación de la empresa, sobre todo ante consumidores y proveedores, ya que será percibida como una entidad incumplidora que puede sufrir reveses financieros y perder alianzas comerciales cruciales.

Figura 20:

Resultados pregunta 11

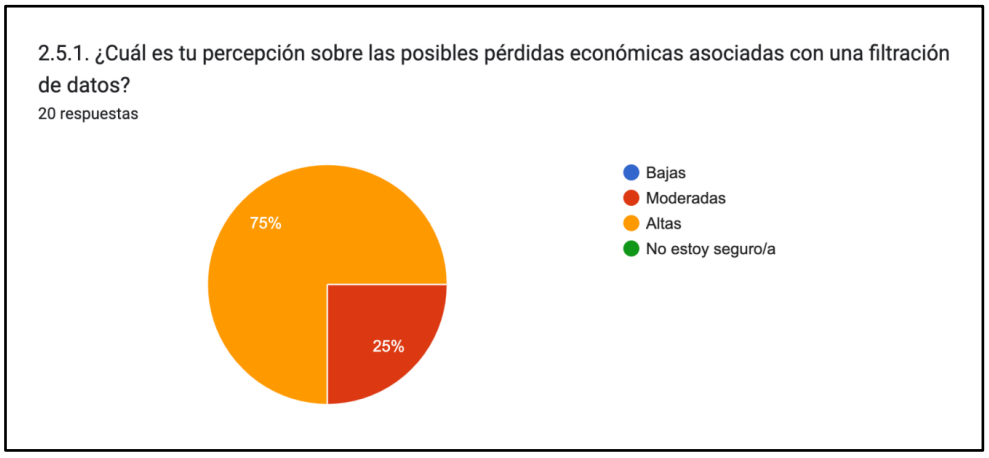


Nota: Elaboración propia.

La organización pasa constantemente por cambios en la rotación de personal, es por ello por lo que se obtuvieron respuestas opuestas, porque las personas más antiguas 10% en la empresa han pasado diferentes situaciones donde se han afrontado de acorde a la situación de aquel momento. Mientras que el 85% son personal que viene laborando desde el primer semestre del 2023.

Figura 21:

Resultados pregunta 12



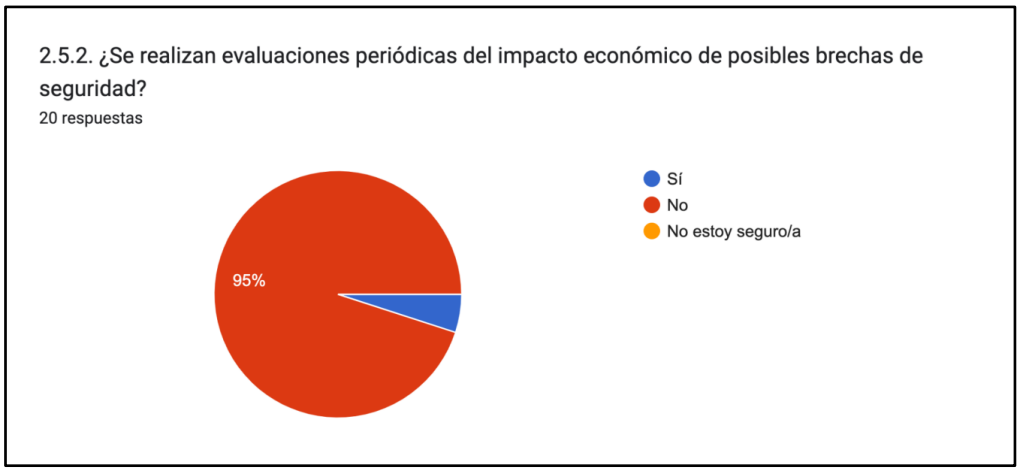
Nota: Elaboración propia.

En la encuesta realizada todos concuerdan en que habrá pérdidas económicas de moderadas 25% a altas 75%, esto debido a que consideran muy

importante la relación que tienen con sus proveedores y clientes, por eso se brinda una comunicación y relación de transparencia para no pasar por situaciones donde perdamos proveedores y clientes estratégicos que posterior a ello nos genere pérdidas monetarias que dificulte el flujo de pedidos de los demás clientes y no tengamos liquidez suficiente para solventar ello.

Figura 22:

Resultados pregunta 13



Nota: Elaboración propia.

Llegamos a la conclusión con esta pregunta que no hay evaluaciones periódicas del impacto económico que pueden generar si no se actúa de forma adecuada con respecto a la seguridad informática, sería bueno que la empresa haga constantes capacitaciones de ello y explicando qué pasaría si se filtran o se pierden datos importantes de los proveedores y clientes.

Tabla 1:

Relación de personal encuestado

Relación de personal encuestado

Nombre	Área laboral	Edad
Preciado Cossio Gianfranco	Gerencia	38
Parvina Malaga Aaron Josue	Comercial	29
Rodas Herrera, Joanny Del Carmen	Administración	34
Ferreyra Chuyo Esthefany Shirley	Administración	29
Mendoza Maturrano, Enzo Jair	Logística	29
Chunga Panduro Sheila Florisa	Comercial	30
Dextre Caro, Gabriel Antonio	Marketing	26
Moscol Zevallos Jefrey Frank Alexis	Logística	24
Huaman Ames, Patricia Ximena	Comercial	25
Chacón Ramirez Gabriel Alfredo	Logística	27
Unzueta Silva, Andrea Paola	Marketing	28
Awada Bayloun Diana Carolina	Marketing	30
Rivas Pablo Richar Manuel	Logística	23
Mantilla Huaylinos Juan Carlos	Logística	27
Ojeda Quicaño Génesis Carmen Rosa	Marketing	24
Medina Bezares Christopher Piero	Comercial	22
Shesira Nayeli Flores Montoya	Administración	24
Gaslac Huaman Kiara Alexandra	Administración	23
Salinas Arevalo Karla Nicole	Logística	23
Wladimir Arcata	Administración	24

Nota: Elaboración propia.

Parece una buena idea recoger encuestas durante las reuniones mensuales de Saltalto para obtener regularmente aportaciones de todas las áreas de la empresa. Al recurrir a estas reuniones preestablecidas, la organización puede garantizar la participación de todos los miembros del personal y tener un conocimiento más exhaustivo de las ideas y recomendaciones de mejora de los distintos departamentos y niveles jerárquicos.

Se presentó la propuesta y para ello se les mandó el enlace de encuesta realizada por Google Forms, donde todos los miembros de la organización llenaron el formulario solicitado.

Todos hicieron hincapié en lo crucial que es poner en marcha mecanismos de control de la seguridad si se quiere seguir creciendo, como ha venido haciendo en los últimos 11 años.

III. Estimación del costo del proyecto

3.1. Estimación de los costos necesarios para la implementación

Tabla 2:

Relación de costos asociados al proyecto

Concepto	Cantidad	Monto	Frecuencia	Tipo de Gasto
Investigación y recopilación de información (asesor de la marca)	100 horas	S/. 10,000	Único	Variable
Contratación de personal experto en seguridad de la información	480 horas	S/. 15,000	Anual	Variable
Capacitación y talleres	40 horas	S/. 20,000	Anual	Fijo
Desarrollo de material didáctico	40 horas	S/. 5,000	Anual	Variable
Producción de videos informativos (apoyo de la marca)	40 horas	S/. 7,500	*Anual*	Variable
Pago de licencias de asistente virtual (CHARLOTTE AI)	60 horas	S/. 8,000	*Anual*	Fijo
Costo total del proyecto		**S/. 82,500**		

Nota: Elaboración propia.

IV. Sustento del Mercado

4.1. Alcance esperado del mercado

La presente investigación tiene como objetivo velar por la seguridad de la información para la empresa Saltalto y la concientización de los trabajadores a tener una cultura de seguridad para salvaguardar los intereses de esta sin afectar el trabajo de cada uno.

Este objetivo ayudará a la organización a hacerse conocida por la seguridad que manejan y los clientes podrán sentirse seguros de trabajar con la mencionada. De esa manera podremos llegar fácilmente a estar en el mindset de los clientes para de esa forma fidelizarlos y que esto traiga mayores ventas y sobre todo un mantenimiento de cuentas importante.

4.2. Descripción del mercado objetivo real o potencial del producto o servicio de forma de comercialización innovadora

Saltalto tiene como objetivo llegar a hombre y mujeres en el Perú, que utilicen plataformas digitales para la compra de productos, es por ello por lo que el proceso de mejora de seguridad informática es tan crítico, recordemos que el Perú es uno de los países más afectados en filtración de datos en Latinoamérica.

1. **GÉNEROS:** Hombres y mujeres
2. **RANGO ETARIO:** 25 a 60 años
3. **NSE:** A y B

4.3. Descripción del modelo de Negocio con el cual la Innovación o investigación aplicada entraría al mercado

Saltalto es una empresa dedicada a la comercialización mediante el sistema de comercio electrónico por años. En cuanto al modelo de negocio es el siguiente, enfocarnos en la seguridad de los trabajadores y usuarios al momento de realizar sus compras, brindándoles seguridad al momento de realizar sus compras, donde haya confidencialidad al momento de generar sus pagos o registro de datos.

4.3.1. Propuesta de Valor

La propuesta de valor que le damos es la de enseñar y capacitar a nuestros trabajadores sobre la seguridad de sus datos mediante páginas web, donde a la vez puedan evitar estafas o pagos por nuestros productos falsos, lo que buscamos es ser una empresa óptima para casos de estafas y sobre todo tener resolución a cualquier caso presentad**o.**

4.3.2. Fuentes de Ingresos

El presente proyecto de investigación no presentará un ingreso monetario, sin embargo, nos generará no obtener pérdidas para la empresa, esto debido a que con este proyecto que realizaremos, evitaremos fraudes mediante la compra de nuestros productos, o pérdida de nuestra base de datos con beneficio para otras empresas**.**

4.3.3. Canales de Distribución

Con respecto a los canales, se utilizarán los digitales y los presenciales, se hará una venta consultiva para que el cliente pueda obtener la herramienta necesaria acorde a su negocio, ya que cada uno es un mundo distinto con necesidades completamente diferentes. Por otro lado, se utilizarán instructivos en las redes sociales para atraer más clientes potenciales y lograr el nivel de ventas necesario.

4.3.4. Estrategia de Penetración en el Mercado

Corto Plazo

1) Generar publicidad en redes para que las empresas puedan saber quiénes somos mediante videos instructivos, redes sociales en alianza con influencers, de esta manera podemos llegar a más clientes y dar a conocer nuestro servicio.
2) Generación de demostraciones, para que los clientes puedan ver hasta qué punto podemos llegar según la necesidad que puedan tener.
3) Crear workshops para los clientes más importantes y potenciales, de esta manera podremos dar a conocer nuestros servicios y sobre todo el alcance de este.

Mediano Plazo

1) Supervisar el establecimiento de nuevas asociaciones estratégicas con proveedores expertos capaces de comprender las demandas de nuestro mercado objetivo y ofrecer soluciones innovadoras para la protección de los datos de nuestros clientes.

Largo Plazo

1) Generación de bases de datos importantes para el uso de esta información a beneficio del negocio, para esto es necesario tener un nivel de seguridad importante y confiable, ya que se están tratando los datos que son confidenciales y es el corazón de la compañía, la contratación de respaldos en la nube es una herramienta fundamental para el crecimiento del negocio.

4.3.5. Actividades Productivas Propias y Externas

Actividades Productivas Internas

Generar acciones específicas como la de un plan de concienciación sobre la importancia del cuidado de la seguridad de la información, esto por medio de nuestras redes sociales, como TikTok, Instagram, donde incentivemos a las personas al cuidado de las redes sociales, mostrando contenido nuestro sobre las medidas que tomamos. En la empresa Saltalto a cada trabajador que brinde ideas o participe en nuestros tik toks se le da un bono por participación, con eso buscamos ideas frescas y efectivas.

Actividades Productivas Externas

Las acciones mencionadas anteriormente sirven para mejorar el flujo de información en la empresa, tener un mayor control y una mayor satisfacción de seguridad para cada proceso que realicemos, al trabajar de esta manera internamente, comunicaremos a nuestros clientes las diferentes modificaciones que estamos realizando en nuestro flujo interno para que ellos tengan la confianza de brindarnos sus datos personales generando transparencia al momento de realizar sus compras.

4.3.6. Alianzas

1) **Aliados Internos**

Se seleccionará un grupo de personas de la empresa Saltalto para que puedan representar cada una de las áreas de la compañía, de esa manera podremos llegar con un mensaje más claro a cada uno y generar la cultura que necesitamos para mejorar este proceso.

2) **Aliados Externos**

Los principales aliados que requiere la compañía son los proveedores de seguridad, que deben trabajar de la mano con Saltalto para de esa manera implementar las herramientas necesarias para ser una compañía confiable en niveles de seguridad para nuestros clientes, un de estas empresas sería Fortinet quien es uno de los líderes en seguridad de la información.

V. Conclusiones

Gracias al diagnóstico situacional de la filtración de datos obtenida mediante las encuestas realizadas, se ha constatado que en la actualidad es necesario contar con un mayor bagaje de conocimientos y una conciencia más aguda para alcanzar un nivel objetivo de seguridad en cuanto a la información se refiere.

Además, la elaboración de un plan de una cultura de seguridad de la información definitivamente ayudará a los trabajadores de Saltalto a evitar la filtración de datos dado que este comprende medidas preventivas y correctivas para asegurar que los datos de la empresa de salvaguarden de acuerdo con confidencialidad, se mantengan disponibles y sean siempre confiables. También es importante incluir en este plan tecnologías emergentes apoyadas en inteligencia artificial para proteger los datos de la empresa. La inteligencia artificial Charlotte AI, brindará un sustento y apoyo global de una base de conocimientos que elevará el nivel de la seguridad de la información en Saltalto.

También se concluye, que es importante tener en cuenta que una cultura de seguridad de la información no solo traerá beneficios económicos si no también con respecto a reputación empresarial además de contar con trabajadores con mayor confianza y mejor capacitados. Estos conocimientos deben ser una parte imprescindible de la cultura organizacional de la empresa, y así asegurar que se mantenga siempre alineada con su misión y objetivos.

Finalmente, en definitiva, una cultura de seguridad de la información ayudará a evitar la filtración de datos de los trabajadores de la empresa Saltalto si se siguen una implementación de forma consciente y consistente.

VI. Recomendaciones

Luego de realizarse el presente trabajo de investigación se han encontrado algunas recomendaciones que pueden ser útiles para fortalecer una cultura de seguridad de la información efectiva y evitar futuras filtraciones:

- **Políticas y procedimientos actualizados:** Saltalto debe contar con normas bien definidas y procedimientos exhaustivos para gestionar y salvaguardar los datos. Estas directrices deben ser sencillas de comprender y cumplir para los miembros del personal, y deben actualizarse y revisarse periódicamente.
- **Monitoreo y auditoría:** Para detectar posibles peligros y garantizar el cumplimiento de las políticas y procedimientos establecidos, la organización necesita tecnologías que permitan supervisar y auditar continuamente los sistemas y el acceso a los datos.
- **Seguridad física:** La empresa debe asegurarse de que existen suficientes medidas de seguridad física, como cámaras de vigilancia y control de acceso seguro, además de procedimientos de seguridad lógica o digital de la información para impedir el acceso no deseado a los datos.

El establecimiento de una cultura de seguridad de la información en Saltalto mejorará la reputación de la empresa y la confianza de los clientes en su capacidad para manejar los datos de forma segura y fiable, además de prevenir futuras violaciones de datos.

VII. Referencias

Altamirano, K. J. (2021). La seguridad de la información en la administración pública. En Universidad de Lima (Ed.), *Construyendo un mundo inteligente para la sostenibilidad. Actas del III Congreso Internacional de Ingeniería de Sistemas* [Congreso]. Universidad de Lima. https://hdl.handle.net/20.500.12724/13917

Argemi, M. (2019) *Los siete hábitos de la gente desinformada: Como informarse y tomar decisiones en redes sociales*. Editorial Conecta.

Ávila, V. (2022). *Análisis sobre el establecimiento de una Agencia Nacional de Ciberseguridad con base en las recomendaciones de la Estrategia Nacional de Ciberseguridad* [Tesis de maestría, INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación]. Repositorio INFOTEC. https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/565/1/Trabajo%20de%20investigaci%C3%B3n%20MRYCET-VAH.pdf

Bestuzhev, D. (2021, 6 de abril). *Facebook Leaks y sus implicaciones en América Latina.* Linkedin. https://www.linkedin.com/pulse/facebook-leaks-y-sus-implicaciones-en-am%C3%A9rica-latina-dmitry-bestuzhev

Cano, J. J., & Almanza, A. (2020, marzo). Estudio de la evolución de la seguridad de la información en Colombia: 2000 - 2018. *RISTI - Revista Ibérica de Sistemas e Tecnologías de Información*, (e27), 470-483.

https://www.proquest.com/docview/2385758173

Casasempere-Satorres, A., & Vercher-Ferrándiz, M. L. (2020, 2 de julio). Análisis documental bibliográfico. Obteniendo el máximo rendimiento a la revision de la literature en investigaciones cualitativas. *New Trends in Qualitative Research*, (4). 247–257. https://doi.org/10.36367/ntqr.4.2020.247-257

Castro, J., Gómez, L., & Carmargo, E. (2023, 01 de enero). La investigación aplicada y el desarrollo experimental en el fortalecimiento de las competencias de la sociedad del siglo XXI. *Tecnura, 27*(75), 140-174. https://doi.org/10.14483/22487638.19171

Cifre, S. (2020). *Modelo de seguridad para la gestión de vulnerabilidades de servidores en nubes privadas* [Tesis de maestría, Universidad Tecnológica Nacional]. Repositorio Institucional Abierto. https://ria.utn.edu.ar/bitstream/handle/20.500.12272/6050/Tesis%20de%20Maestri%CC%81a%20-%20Cifre%20Simo%CC%81n.pdf?sequence=1&isAllowed=y

Cloudflare. (2023). *¿Qué es la privacidad de los datos?* https://www.cloudflare.com/es-es/learning/privacy/what-is-data-privacy/

Core Business Solutions, Inc. (2023). *ISO 27001 Certification.* *https://www.thecoresolution.com/iso-27001?creative=518833423585&keyword=iso%2027001&matchtype=b&network=g&device=c&gclid=CjwKCAiAr4GgBhBFEiwAgwORraIj*

mDzKPGrd-q1ZdhX-7K9IzZvY2LIzET5UWrwIKmqx439T8NmXuxoCaBIQAvD_BwE

Davila, A. A., & Dextre, B. J. (2021). *Propuesta de una implementación de un programa de gestión de vulnerabilidades de seguridad informática para mitigar los siniestros de la información en el policlínico de salud AMC alineado a la NTP-ISO/IEC 27001:2014 en la ciudad de Lima – 2021* [Tesis de pregrado, Universidad Tecnológica del Perú]. https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/4906/A.Davila_B.Dextre_Tesis_Titulo_Profesional_2021.pdf?sequence=1&isAllowed=y

De León, J. E. (2020). *Mejores prácticas de seguridad en el teletrabajo: una revisión* [Tesis de pregrado, Tecnológico de Antioquia: Institución Universitaria]. Repositorio Digital. https://dspace.tdea.edu.co/handle/tdea/1396

Fortinet. (2022). *Servicio de capacitación y concientización en ciberseguridad de Fortinet* [Archivo PDF]. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/es_la/fortinet-security-awareness-training-service.pdf

Gerencia de Innovación y Desarrollo de Tecnologías de Información y Comunicación. (2017). *Manual de seguridad de la información V. 3*. Universidad EAN [Archivo PDF]. https://universidadean.edu.co/sites/default/files/manuales/manual-de-seguridad-de-la-informacion.pdf

Gonzalez, J. (2020). *Estudio del estado actual de la seguridad informática en las organizaciones de Colombia* [Tesis de pregrado, Universidad Nacional Abierta y Distancia]. https://repository.unad.edu.co/bitstream/handle/10596/36669/jgonzalezlon.pdf?s

Hill, M., & Swinhoe, D. (2022, 01 de noviembre). *Las 15 filtraciones de datos más grandes del siglo XXI*. Computerworld. https://cso.computerworld.es/cibercrimen/las-15-filtraciones-de-datos-mas-grandes-del-siglo-xxi

Huincho, B. (2019). *Sistema de gestión de seguridad de la información para mejorar la protección informática de la Comisaría Región Huancavelica* [Tesis de pregrado, Universidad Nacional Daniel Alcides Carrión]. Repositorio Institucional UNDAC. http://repositorio.undac.edu.pe/bitstream/undac/2017/1/T026_40760254_T.pdf

Kaspersky. (s.f.). *¿Qué es la privacidad de los datos?* https://latam.kaspersky.com/resource-center/threats/internet-and-individual-privacy-protection

Kaspersky. (s.f.). Identity theft prevention tips for Facebook users. https://latam.kaspersky.com/resource-center/threats/facebook-identity-theft-prevention

Linares, F. (2022, 28 de marzo). *Vulnerabilidad en el sector público y la urgencia de pensar en ciberseguridad*. Centro de Investigación de la Universidad del Pacifico. https://ciup.up.edu.pe/analisis/vulnerabilidad-en-sector-publico-la-urgencia-de-pensar-ciberseguridad/

Machuca, S. A., Vinueza, N. V., Sampedro, C. R., & Santillán, A. L. (2022, marzo-abril). Habeas data y protección de datos personales en la gestión de las bases de datos. *Revista Universidad y Sociedad, 14*(2), 244-251. http://scielo.sld.cu/pdf/rus/v14n2/2218-3620-rus-14-02-244.pdf

Mansilla, G. (2022). *Confidencialidad y privacidad* [Archivo PDF]. ResearchGate. https://www.doi.org/10.55209/CElibro2.8

Mendez, M. W. (2022). *Modelo de seguridad de la información para mejorar la gestión informática en la municipalidad provincial de Yungay, 2022* [Tesis de pregrado, Universidad Nacional Santiago Antúñez de Mayolo]. Repositorio Institucional UNASAM. *http://repositorio.unasam.edu.pe/handle/UNASAM/5372*

Meneses-Falcón, C. (2022, julio-diciembre). El proyecto de investigación: La hoja de ruta de la investigación. *Miscelánea Comillas, 80*(157), 429-454. https://doi.org/10.14422/mis.v80.i157.y2022.010

Parra, H. F. (2022). *DLP Data Loss Prevention como estrategia de seguridad empresarial para la detección de pérdida de datos en los sistemas de comunicación y prevenir la filtración de información* [Tesis de

pregrado, Universidad Nacional Abierta y Distancia]. https://repository.unad.edu.co/handle/10596/48931

Perú Retail. (2021, 6 de abril). *Facebook confirma filtración de información privada de más de 8 millones de usuarios peruanos.* https://www.peru-retail.com/facebook-confirma-filtracion-informacion-privada-8-millones-usuarios-peruanos/

Programa Nacional de Becas y Crédito Educativo. (2023). *Sistema de Gestión de Seguridad de la Información*. PRONABEC. https://www.pronabec.gob.pe/sistema-de-gestion-de-seguridad-de-la-informacion/

Rodriguez, L. S., Cruzado, C. F., Mejía, C., & Alarcón Diaz, M. A. (2020, septiembre-diciembre). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *Propósitos y Representaciones,* *8*(3), e786. http://www.scielo.org.pe/pdf/pyr/v8n3/2310-4635-pyr-8-03-e786.pdf

Rohall, P. J. (s.f.). *Estadísticas mundiales de fraude en el robo de cuentas en 2022*. SEON. https://seon.io/es/recursos/estadisticas-de-robos-de-cuentas-a-nivel-mundial/

Rojas-Gutiérrez, W. J. (2022, 01 de enero). La relevancia de la investigación cualitativa. *Studium Veritatis,* *20*(26), 79–97. https://doi.org/10.35626/sv.26.2022.353

Samaniego, E. A., & Ponce, J. A. (2021). *Fundamentos de seguridad informática.* Editorial Grupo Compas. Ecuador.

https://www.researchgate.net/publication/354054517_Libro_Fundamentos_de_seguridad_informatica

Sánchez, C. (2017). *Valoración de intangibles para la ciberseguridad en la nueva economía* [Tesis de doctorado, Universidad de Sevilla]. Depósito de Investigación Universidad de Sevilla. http://hdl.handle.net/11441/63996

Sentonas, M. (2023, 30 de mayo). Introducing Charlotte AI, CrowdStrike's generative AI security analyst: ushering in the future of AI-powered cybersecurity. *Crowdstrike, Blog*. Crowdstrike.com. https://www.crowdstrike.com/blog/crowdstrike-introduces-charlotte-ai-to-deliver-generative-ai-powered-cybersecurity/

Statista. (2024). Usuarios mundiales de las redes sociales líderes. https://es.statista.com/estadisticas/600712/ranking-mundial-de-redes-sociales-por-numero-de-usuarios/

Terán, Y. J. (2021). *Seguridad en la gestión de la información para las organizaciones públicas desde el enfoque ISO/IEC 2700: un mapeo sistemático* [Tesis de pregrado, Universidad Politécnica Salesiana, Ecuador]. https://dspace.ups.edu.ec/handle/123456789/20333

Ureña, V. (2020). *Importancia de la seguridad informática para proveer teletrabajo seguro en Costa Rica* [Trabajo de fin de grado para maestría, Universidad Latinoamericana de Ciencia y Tecnología]. https://hdl.handle.net/20.500.14230/10804

Valoyes, A. (2019). *Ciberseguridad en Colombia* [Trabajo de especialización, Universidad Piloto de Colombia]. http://repository.unipiloto.edu.co/handle/20.500.12277/6370

VIII. ANEXOS

Anexo 1. Reporte Turnitin

Similarity Report

PAPER NAME
DOCUMENTO FINAL - Proyecto de investigaci%C3%B3n 2024 - Grupo 13 - F sin declaracion.docx

AUTHOR
JOSUE FEDERICO QUINTO HUANQQUE

WORD COUNT
11827 Words

CHARACTER COUNT
67916 Characters

PAGE COUNT
74 Pages

FILE SIZE
2.3MB

SUBMISSION DATE
Mar 8, 2024 1:55 AM GMT-5

REPORT DATE
Mar 8, 2024 1:56 AM GMT-5

20% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

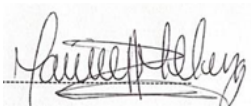
- 14% Internet database
- 4% Publications database
- Crossref database
- Crossref Posted Content database
- 18% Submitted Works database

Excluded from Similarity Report

- Bibliographic material
- Quoted material

Firmas de los autores

Nombres	Apellidos	Dni	Firma	Huella
Jean Jairo	La Torre Cordero	71451621		

Brayan Manuel	Mechan Gonzales	73449426		
Mauricio Jose	Melendez Adames	61116752		
Josue Federico	Quinto Huanqque	46219313		

Firma del asesor

Nombres	Apellidos	Dni	Firma	Huella
Celes Alonso	Espinoza Rúa	42750231		

- Matriz de consistencia

PROPUESTA DE UN PLAN DE CULTURA DE SEGURIDAD DE LA INFORMACIÓN PARA EVITAR LA FILTRACIÓN DE DATOS DE LOS TRABAJADORES DE LA EMPRESA SALTALTO, 2023				
PROBLEMAS	**OBJETIVOS**	**Supuestos hipotéticos**	**Categorías analíticas**	**METODOLOGÍA**
PROBLEMA GENERAL	**OBJETIVO GENERAL**	**HIPÓTESIS GENERAL**		Enfoque: Cualitativo Tipo de investigación: descriptivo Diseño: Investigación-acción Técnicas de recolección de datos: - Encuestas Instrumentos de recolección de datos: - Ficha de encuesta
¿Cómo generar una estrategia clara y consolidada para generar una nueva cultura de seguridad de la información?	Proponer un plan de cultura de seguridad de la información para evitar la filtración de datos de la empresa Saltalto, 2023	-		
PROBLEMAS ESPECÍFICOS	**OBJETIVOS ESPECÍFICOS**	**HIPÓTESIS ESPECÍFICAS**	**Categoría analítica**	
¿Cómo podemos saber en qué situación está la empresa y que herramientas necesita para mejorar en los puntos de seguridad de la información?	Elaborar el diagnóstico situacional de la filtración de datos para identificar cómo se encuentra actualmente la organización.	No hay, debido a la naturaleza de la investigación.	***Filtración de datos***	
¿Cuáles son los puntos que se deben tocar para evitar la filtración de datos en la empresa y que este sea un desarrollo sostenible en el futuro?	Desarrollo de un plan de cultura de seguridad de la información para evitar la filtración de datos.	No hay, debido a la naturaleza de la investigación.		
¿De qué manera podemos ayudar a los empleados de la empresa para que no tengan tanta resistencia al cambio?	Describir los beneficios de la cultura de seguridad de la información los trabajadores de la empresa Saltalto, 2023.	No hay, debido a la naturaleza de la investigación.		

- Matriz de operacionalización de variables

VARIABLES	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES	N°	ITEM	ALTERNATIVAS A RESPUESTAS
Seguridad de la información	Conjunto de técnicas e instrumentos de seguridad que protegen la información confidencial de la empresa contra el abuso, el acceso ilegal, la perturbación o la destrucción.	Confidencialidad	Control de acceso	2.1.1	¿En tu entorno de trabajo se implementan medidas de control de acceso para proteger la información sensible?	● Si ● No ● No estoy seguro/a
				2.1.2	¿Qué tipo de medidas de control de acceso se utilizan?	● Contraseñas fuertes ● Autenticación de dos factores ● Control de acceso físico ● Políticas de acceso basadas en roles ● Otros
		Integridad	Seguridad de la comunicación	2.2.1	¿Cómo se protege la comunicación de datos sensibles en tu entorno de trabajo?	● Uso de cifrado de extremos a extremo ● Red privada virtual (VPN) ● Protocolos seguros (por ejemplo, HTTPS) ● Auditorías de seguridad de la red ● Otros
				2.2.2	¿Has recibido formación sobre la importancia de la seguridad en la comunicación de datos?	● Si ● No ● No estoy seguro/a
		Disponibilidad	Acceso a la información	2.3.1	¿Existe un protocolo formal para el acceso a información sensible en tu organización?	● Si ● No ● No estoy seguro/a
				2.3.2	¿Cómo se gestiona el acceso a la información confidencial?	● Permiso basado en roles ● Seguimiento de actividad de usuarios ● Auditorías periódicas de acceso ● Otro

Filtración de datos	Cualquier incidente de seguridad en el que partes no autorizadas obtengan acceso a datos o información confidencial, incluidos datos personales (números de seguridad social, números de cuentas bancarias, datos de atención médica) o datos corporativos (registros de datos de clientes, propiedad intelectual e información financiera).	Impacto	Pérdida de reputación	2.4.1	¿Crees que una filtración de datos en tu organización afectaría su reputación?	• Si • No • No estoy seguro/a
				2.4.2	¿Se han tomado medidas para gestionar la percepción pública después de incidentes de seguridad?	• Si • No • No estoy seguro/a
		Consecuencias	Pérdidas económicas	2.5.1	¿Cuál es tu percepción sobre las posibles pérdidas económicas asociadas con una filtración de datos?	• Bajas • Moderadas • Altas • No estoy seguro/a
				2.5.2	¿Se realizan evaluaciones periódicas del impacto económico de posibles brechas de seguridad?	• Si • No • No estoy seguro/a

- Ficha de encuesta sobre Seguridad de la Información y Filtración de Datos

Introducción:

Estimado participante, le agradecemos su participación en esta encuesta, cuyo fin es examinar cómo se percibe y practica la seguridad de la información en su lugar de trabajo, así como cualquier posible filtración de datos. Sus respuestas son cruciales para el avance de este estudio.

Sección 1: Información Demográfica

1.1. Género:

- Masculino
- Femenino

1.2. Edad:

- 18-25 años
- 26-35 años
- 36-45 años
- 46-55 años
- Más de 55 años

1.3. Área de trabajo:

- Gerencia
- Administración
- Comercial
- Marketing
- Logística

Sección 2: Seguridad de la Información y Filtración de Datos

2.1. Control de Acceso:

2.1.1. ¿En tu entorno de trabajo se implementan medidas de control de acceso para proteger la información sensible?

- Sí
- No
- No estoy seguro/a

2.1.2. ¿Qué tipo de medidas de control de acceso se utilizan? (Selecciona todas las que correspondan)

- Contraseñas fuertes
- Autenticación de dos factores
- Control de acceso físico
- Políticas de acceso basadas en roles
- Otro (especificar): _____

2.2. Seguridad de la Comunicación:

2.2.1. ¿Cómo se protege la comunicación de datos sensibles en tu entorno de trabajo?

- Uso de cifrado de extremo a extremo
- Red privada virtual (VPN)
- Protocolos seguros (por ejemplo, HTTPS)
- Auditorías de seguridad de la red
- Otro (especificar): _____

2.2.2. ¿Has recibido formación sobre la importancia de la seguridad en la comunicación de datos?

- Sí
- No
- No estoy seguro/a

2.3. Acceso a la Información:

2.3.1. ¿Existe un protocolo formal para el acceso a información sensible en tu organización?

- Sí
- No
- No estoy seguro/a

2.3.2. ¿Cómo se gestiona el acceso a la información confidencial? (Selecciona todas las que correspondan)

- Permiso basado en roles
- Seguimiento de actividad de usuarios
- Auditorías periódicas de acceso
- Otro (especificar): _____

2.4. Pérdida de Reputación:

2.4.1. ¿Crees que una filtración de datos en tu organización afectaría su reputación?

- Sí
- No
- No estoy seguro/a

2.4.2. ¿Se han tomado medidas para gestionar la percepción pública después de incidentes de seguridad?

- Sí
- No
- No estoy seguro/a

2.5. Pérdidas Económicas:

2.5.1. ¿Cuál es tu percepción sobre las posibles pérdidas económicas asociadas con una filtración de datos?

- Bajas
- Moderadas
- Altas
- No estoy seguro/a

2.5.2. ¿Se realizan evaluaciones periódicas del impacto económico de posibles brechas de seguridad?

- Sí
- No
- No estoy seguro/a

Conclusión:

Valoramos mucho su participación en esta encuesta. Sus respuestas son cruciales para ampliar nuestros conocimientos sobre la filtración de datos y la seguridad de la información en muchos contextos. Los resultados se mantendrán en secreto y se utilizarán exclusivamente para la investigación académica.