UNIVERSIDAD LATINA CAMPUS HEREDIA

TRABAJO FINAL DE GRADUACIÓN(TFG) PARA OPTAR POR EL GRADO DE LICENCIATURA EN

SEGURIDAD INFORMÁTICA

Modalidad Proyecto

Título:

Diseño de políticas y mejores prácticas, basado en el marco de referencia ISO 27001, para la mejora de la seguridad de la información del Departamento de Tecnología de la empresa Soluciones Seguras Costa Rica, en el segundo cuatrimestre del año 2023.

Autor: Jehoshua Rojas Quesada

Heredia, agosto 2023

UNIVERSIDAD LATINA DE COSTA RICA
POWERED BY Arizona State University

TRIBUNAL EXAMINADOR

Este proyecto titulado: Diseño de políticas y mejores prácticas, basado en el marco de referencia ISO 27001, para la mejora de la seguridad de la información del Departamento de Tecnología de la empresa Soluciones Seguras Costa Rica, en el segundo cuatrimestre del año 2023, por el (la) estudiante: Jehoshua Rojas Quesada, fue aprobado por el Tribunal Examinador de la carrera de Seguridad Informática de la Universidad Latina, Sede Heredia, como requisito para optar por el grado de Licenciatura.

KIMBERLY MARIA MUÑOZ ARAYA (FIRMA)
Firmado digitalmente por KIMBERLY MARIA MUÑOZ ARAYA (FIRMA)
Fecha: 2023.10.02 13:59:24 -06'00'

Kimberly María Muñoz Araya
Tutor

RONALD DAVID CAMACHO PEREZ (FIRMA)
Firmado digitalmente por RONALD DAVID CAMACHO PEREZ (FIRMA)
Fecha: 2023.10.02 10:27:06 -06'00'

Ronald David Camacho Pérez
Lector

RANDY ALEXANDER VALVERDE VALVERDE (FIRMA)
Firmado digitalmente por RANDY ALEXANDER VALVERDE VALVERDE (FIRMA)
Fecha: 2023.10.02 13:53:26 -06'00'

Randy Alexander Valverde Valverde
Representante

DECLARACIÓN JURADA

Heredia, 03 de agosto 2023

El suscrito Jehoshua Rojas Quesada con cédula de identidad número 1-1575-0480, declaro bajo fe de juramento, conociendo las consecuencias penales que conlleva el delito de perjurio, que soy el autor del presente trabajo final de graduación, para optar por el título de Licenciatura en Seguridad Informática de la Universidad Latina de Costa Rica y que el contenido de dicho trabajo es obra original del suscrito. Asimismo, autorizo a la Universidad Latina de Costa Rica, a disponer de dicho trabajo para uso y fines de carácter académico, publicitando el mismo en el sitio web; así como en el CRAI. Ni la Universidad ni el jurado que califica este Proyecto Final de Graduación, serán responsables de las ideas expuestas el Autor.

Jehoshua Rojas Quesada

1-1575-0480

Licencia De Distribución No Exclusiva (carta de la persona autora para uso didáctico)

Universidad Latina de Costa Rica

Yo (Nosotros):	Jehoshua Rojas Quesada
De la Carrera / Programa:	Licenciatura en Seguridad Informática
Modalidad de TFG:	Proyecto
Titulado:	Diseño de políticas y mejores prácticas, basado en el marco de referencia ISO 27001, para la mejora de la seguridad de la información del Departamento de Tecnología de la empresa Soluciones Seguras Costa Rica, en el segundo cuatrimestre del año 2023

Al firmar y enviar esta licencia, usted, el autor (es) y/o propietario (en adelante el "**AUTOR**"), declara lo siguiente: **PRIMERO**: Ser titular de todos los derechos patrimoniales de autor, o contar con todas las autorizaciones pertinentes de los titulares de los derechos patrimoniales de autor, en su caso, necesarias para la cesión del trabajo original del presente TFG (en adelante la "**OBRA**"). **SEGUNDO**: El **AUTOR** autoriza y cede a favor de la **UNIVERSIDAD U LATINA S.R.L.** con cédula jurídica número 3-102-177510 (en adelante la "**UNIVERSIDAD**"), quien adquiere la totalidad de los derechos patrimoniales de la **OBRA** necesarios para usar y reusar, publicar y republicar y modificar o alterar la **OBRA** con el propósito de divulgar de manera digital, de forma perpetua en la comunidad universitaria. **TERCERO**: El **AUTOR** acepta que la cesión se realiza a título gratuito, por lo que la **UNIVERSIDAD** no deberá abonar al autor retribución económica y/o patrimonial de ninguna especie. **CUARTO**: El **AUTOR** garantiza la originalidad de la **OBRA**, así como el hecho de que goza de la libre disponibilidad de los derechos que cede. En caso de impugnación de los derechos autorales o reclamaciones instadas por terceros relacionadas con el contenido o la autoría de la **OBRA**, la responsabilidad que pudiera derivarse será exclusivamente de cargo del **AUTOR** y este garantiza mantener indemne a la **UNIVERSIDAD** ante cualquier reclamo de algún tercero. **QUINTO**: El **AUTOR** se compromete a guardar confidencialidad sobre los alcances de la presente cesión, incluyendo todos aquellos temas que sean de orden meramente institucional o de organización interna de la **UNIVERSIDAD SEXTO**: La presente autorización y cesión se regirá por las leyes de la República de Costa Rica. Todas las controversias, diferencias, disputas o reclamos que pudieran derivarse de la presente cesión y la materia a la que este se refiere, su ejecución, incumplimiento, liquidación, interpretación o validez, se resolverán por medio de los Tribunales de Justicia de la República de Costa Rica, a cuyas normas se someten el **AUTOR** y la **UNIVERSIDAD**, en forma voluntaria e incondicional. **SÉPTIMO**: El **AUTOR** acepta que la **UNIVERSIDAD**, no se hace responsable del uso, reproducciones, venta y distribuciones de todo tipo de fotografías, audios, imágenes, grabaciones, o cualquier otro tipo de

presentación relacionado con la **OBRA**, y el **AUTOR**, está consciente de que no recibirá ningún tipo de compensación económica por parte de la **UNIVERSIDAD**, por lo que el **AUTOR** haya realizado antes de la firma de la presente autorización y cesión. **OCTAVO**: El **AUTOR** concede a **UNIVERSIDAD.,** el derecho no exclusivo de reproducción, traducción y/o distribuir su envío (incluyendo el resumen) en todo el mundo en formato impreso y electrónico y en cualquier medio, incluyendo, pero no limitado a audio o video. El **AUTOR** acepta que **UNIVERSIDAD.** puede, sin cambiar el contenido, traducir la **OBRA** a cualquier lenguaje, medio o formato con fines de conservación. **NOVENO**: El **AUTOR** acepta que **UNIVERSIDAD** puede conservar más de una copia de este envío de la **OBRA** por fines de seguridad, respaldo y preservación. El **AUTOR** declara que el envío de la **OBRA** es su trabajo original y que tiene el derecho a otorgar los derechos contenidos en esta licencia. **DÉCIMO**: El **AUTOR** manifiesta que la **OBRA** y/o trabajo original no infringe derechos de autor de cualquier persona. Si el envío de la **OBRA** contiene material del que no posee los derechos de autor, el **AUTOR** declara que ha obtenido el permiso irrestricto del propietario de los derechos de autor para otorgar a **UNIVERSIDAD** los derechos requeridos por esta licencia, y que dicho material de propiedad de terceros está claramente identificado y reconocido dentro del texto o contenido de la presentación. Asimismo, el **AUTOR** autoriza a que en caso de que no sea posible, en algunos casos la **UNIVERSIDAD** utiliza la **OBRA** sin incluir algunos o todos los derechos morales de autor de esta. **SI AL ENVÍO DE LA OBRA SE BASA EN UN TRABAJO QUE HA SIDO PATROCINADO O APOYADO POR UNA AGENCIA U ORGANIZACIÓN QUE NO SEA UNIVERSIDAD U LATINA, S.R.L., EL AUTOR DECLARA QUE HA CUMPLIDO CUALQUIER DERECHO DE REVISIÓN U OTRAS OBLIGACIONES REQUERIDAS POR DICHO CONTRATO O ACUERDO. La presente autorización se extiende el día** 11 **de** setiembre **de** 2023 **a las** 15:30

Firma del estudiante(s):

CARTA DEL FILÓLOGO

Heredia, 23 de agosto del 2023

Sres.

Comité de Trabajos Finales de Graduación

Escuela de Ingeniería en Sistemas de Información

Universidad Latina de Costa Rica

Estimados Señores:

Leí y corregí el Trabajo Final de Graduación, denominado: **Diseño de políticas y mejores prácticas, basado en el marco de referencia ISO 27001, para la mejora de la seguridad de la información del Departamento de Tecnología de la empresa Soluciones Seguras Costa Rica, en el segundo cuatrimestre del año 2023**, elaborado por el estudiante: **Jehoshua Rojas Quesada**; cedula de identidad **1-1575-0480**, para optar por grado académico de **Licenciatura en Seguridad Informática**.

Corregí el trabajo en aspectos, tales como: construcción de párrafos, vicios del lenguaje que se trasladan a lo escrito, ortografía, puntuación y otros relacionados con el campo filológico, y desde ese punto de vista considero que está listo para ser presentado como Trabajo Final de Graduación; por cuanto cumple con los requisitos establecidos por la Universidad.

Suscribe de Ustedes cordialmente,

MARGARITA JIMENEZ CARMONA (FIRMA)

Firmado digitalmente por MARGARITA JIMENEZ CARMONA (FIRMA)
Fecha: 2023.08.23 20:52:17 -06'00'

Margarita Jiménez Carmona

Número de Carné: 8487 COLYPRO

Teléfono 88657662

Email faxani@hotmail.com

AGRADECIMIENTOS

Primeramente, agradecerle a Dios porque en todo momento me cuida y me guía en mi camino y porque me ha permitido vivir y disfrutar cada una de las etapas de mi formación profesional de manera correcta y exitosa.

A mi familia por estar conmigo y apoyarme en todo momento a lo largo del desarrollo de este trabajo, además por ser pacientes y comprensivos durante todo este recorrido de la licenciatura.

A Soluciones Seguras por darme la oportunidad de realizar este trabajo final de graduación dentro de la empresa y por siempre brindarme el apoyo y tiempo necesario para poder finalizar este trabajo

A mi tutora la Ingeniera Kimberly Muñoz Araya quien me apoyó de manera excepcional en la realización de este documento y por siempre ayudarme con la aclaración de todas las dudas que se me presentaron a lo largo de este proyecto.

Al gerente regional de soporte de Soluciones Seguras, Omar González por todo el apoyo brindado en cuanto a la norma ISO 27001, además de la buena disposición en todo momento, así como también por brindarme toda documentación interna necesaria para poder cumplir con el objetivo de este proyecto.

Y a todas las personas que de una u otra manera me apoyaron en este camino de la licenciatura, muchas gracias.

DEDICATORIA

A Dios, por siempre cuidarme y respaldarme y por ser mi guía para toda decisión o circunstancia que tuve que tomar en mi vida.

A mi esposa, Sharon por ser ese apoyo incondicional, por ser una mujer llena de Dios en su corazón, por no dejarme caer nunca y levantarme en los momentos difíciles también por impulsarme a siempre seguir formándome y creciendo profesionalmente y por hacer de mi un mejor hombre, esposo y padre.

A mis hijos, Mathías y Luka por ser mi mayor motivo para seguir adelante, quienes me han dado el gran honor de ser padre y que han hecho un mejor ser humano y por darme ese amor incondicional que me da fuerzas para seguir y luchar día tras día para darle los mejor.

A mi madre, Gabriela por siempre estar a mi lado y ser quien me impulso a iniciar en el mundo de la tecnología desde joven, por ser quien me ha enseñado que nunca hay que rendirse y que nunca es tarde para seguir estudiando y aumentando el conocimiento y también por enseñarme que todo se hace con excelencia y colocando a Dios por delante de todo en la vida.

A mi padre, Jose por enseñarme a ser una buena persona, por mostrarme que uno puede caerse mil veces, pero es obligatorio levantarse mil y una veces más y por enseñarme también que la vida no es fácil, pero que con esfuerzo y dedicación todo se puede lograr.

RESUMEN

La propuesta de este trabajo de investigación se desarrolló en la empresa Soluciones Seguras, misma que cuenta con una trayectoria de más de 20 años y con participación en varios países de Centroamérica, la cual se dedica a la venta de soluciones de seguridad y también el servicio de soporte para esas soluciones, gracias a las grandes alianzas que tiene con los fabricantes. Soluciones Seguras al ser una compañía que se encuentra en el área de la tecnología, específicamente, en el sector de la seguridad informática tiene la necesidad de incorporar normativas que aseguren la información como un activo bastante valioso, así como el aumentar la imagen, reputación y sobre todo la confianza que depositan los clientes que adquieren los servicios y soluciones, por este motivo es que se propone el planteamiento para poder, diseñar y documentar políticas de seguridad, con base en una normativa internacional con el fin de minimizar los riesgos asociados a los activos de valor de la Compañía.

La propuesta además tiene como base los lineamientos y mejores prácticas indicados en la normativa internacional ISO 27001, la cual está directamente asociada con los estándares internacionales de seguridad de la información, además que se utilizará como apoyo las herramientas de análisis de entrevistas y encuestas, con esto se llega a la conclusión, siempre basado en las necesidades de la organización y los resultados obtenidos durante el proceso y subprocesos que fueron incluidos en esta propuesta, además es importante mencionar que la organización tiene como proyecto, a mediano plazo, de poder certificarse en la normativa ISO 27001 por lo que este proyecto será base para el objetivo de la certificación.

En total se realizó el diseño y documentación de seis políticas y 1 procedimiento para los subprocesos seleccionados, así como la creación del machote oficial para estas políticas, ya que no se contaba con una documentación estándar establecida, todo lo anterior se basará esto

basándose en el estándar ISO 27001, además toda la documentación creada fue entregada a la Compañía para su debida adaptación de procesos dentro de esta. la misma.

Por último es importante concluir que pese a que Soluciones Seguras contaba con documentación relacionada con los procesos no existía un diseño de políticas directamente relacionados con las buenas prácticas y lineamientos que indica una norma internacional como lo es la ISO 27001, por lo que la realización de esta propuesta será una base y una mejora para la seguridad de la información que salvaguarda la confidencialidad, integridad y disponibilidad de los activos de valor de la Compañía empleados en el proceso seleccionado para este trabajo.

ABSTRACT

The proposal of this research work was developed in the company Soluciones Seguras which has a history of more than 20 years and with participation in several Central American countries, which is dedicated to the sale of security solutions and, also the support service for these solutions thanks to the great alliances it has with manufacturers. Soluciones Seguras being a company that is in the area of technology specifically in the field of computer security has the continuous need to incorporate regulations to ensure the information that is a very valuable asset, as well as to increase the image, reputation and above all the trust placed by customers who purchase services and solutions, for this reason is that the approach is made to design and document security policies based on international standards in order to minimize the risks associated with the valuable assets of the company.

The proposal is also based on the guidelines and best practices indicated in the international standard ISO 27001 which is directly associated with international standards for information security, in addition to the researcher used as support the tools of analysis of interviews and surveys, with this conclusion based on the needs of the organization and the results obtained from the process and sub-processes that were included in this proposal is also important to mention that the organization has as a future project to be certified in the ISO 27001 standard so this project serves as a basis for that goal of the company.

A total of 6 policies and 1 procedure were designed and documented for the selected sub-processes, as well as the creation of the official template for these policies, all based on the ISO 27001 standard, and all the documentation created was delivered to the company.

Finally, it is important to conclude that although Soluciones Seguras had documentation related to the processes, there was no design of policies directly related to the good practices and

guidelines indicated by an international standard such as ISO 27001, so the realization of this work establishes a basis and an improvement for information security, safeguarding the confidentiality, integrity and availability of the company's valuable assets immersed in the process selected for this work.

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

INDICE DE APÉNDICES

Capítulo 1. Introducción

En la era digital en la que se vive en la actualidad, la seguridad de la información se ha convertido en un elemento relevante para las operaciones y la continuidad de una organización. La creciente dependencia de la tecnología y el aumento de las amenazas cibernéticas resaltan la necesidad de controles y políticas sólidas para proteger la información confidencial y los activos digitales de las organizaciones. Tomando en cuenta lo anterior es que el enfoque principal de este trabajo final de graduación se basa en la seguridad de la información para el Departamento de Tecnologías de la Información de la empresa Soluciones Seguras.

Soluciones Seguras es una compañía con más de 20 años en el sector de tecnologías con movimiento en varios países de Centroamérica que ha experimentado un crecimiento exponencial en los últimos años, en gran parte debido a la integración de tecnología de seguridad informática avanzada a su catálogo de soluciones, así como procesos y operaciones internas. Este avance tecnológico ha permitido a la empresa aumentar la eficiencia, mejorar la toma de decisiones y ampliar el alcance del mercado. Sin embargo, esto conlleva a que también se enfrente a nuevos riesgos y desafíos en el campo de la seguridad de la información. Además, tomando en cuenta que su foco principal es la comercialización de soluciones de seguridad informática es que toma tanta relevancia el que una empresa de este tipo, indispensablemente, cuente con políticas y mejores prácticas para sus procesos internos y externos basados en una norma internacional como lo es la ISO 27001.

Para la elaboración de este proyecto se utilizará como referencia la norma ISO 27001 que fue desarrollada por la Organización Internacional de Normalización (ISO), esta normativa brinda un marco de trabajo completo y reconocido en el nivel mundial para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

Este estándar internacional basa su enfoque en la mejora continua, lo que hace que sea una herramienta indispensable para las organizaciones que buscan fortalecer su posición de la seguridad de la información.

Por último, para el desarrollo de este trabajo se realiza el análisis de la situación actual de la compañía Soluciones Seguras en el campo de seguridad informática y de la mano con los resultados obtenidos, además tomando como referencia lo que indica la normativa ISO 27001 se plantea el diseño y documentación de las políticas de seguridad para esta organización.

Generalidades

Hoy, la seguridad informática como parte de una de las numerosas áreas con las que cuenta la tecnología tiene como objetivo principal el resguardar y proteger la información como uno de los activos más valiosos dentro de toda organización esto además sumando a que también está en la constante búsqueda de que se cumpla con los tres pilares fundamentales de la seguridad, como lo son: la confidencialidad, integridad y disponibilidad, para así garantizar que los datos e información estén siempre seguros, así como los sistemas, activos y personal involucrado en los distintos procesos de las organizaciones.

La protección de los datos e información, así como su veracidad y fácil acceso son puntos que se han vuelto vitales en las organizaciones actualmente es por esto que las normativas y estándares toman más fuerza para ser implementadas y desarrolladas para poder tener un mejor control y manejo de la información.

Soluciones Seguras es una empresa con más de 20 años en el mercado internacional y como bien lo dice en su nombre se encarga de brindar soluciones de seguridad informática a las empresas y que además cuenta con alianzas tecnológicas con muchos de los grandes fabricantes de soluciones de seguridad como Checkpoint, Radware, CyberArk y Barracuda entre otros, es por

esto que es sumamente importante para una compañía que se ubica en esta área de la Seguridad informática debe garantizar que se tienen diseñadas y documentadas políticas y mejores prácticas para sus procesos internos basados en la norma ISO 27001.

Tomando en cuenta que este trabajo se basa en poder diseñar políticas según la norma ISO 27001 es importante profundizar un poco más acerca de lo que este estándar se refiere y el impacto positivo que tiene en cuanto a la seguridad informática es por esto que para comenzar se define como:

> […] norma internacional emitida por la Organización Internacional de Normalización (ISO). Esta se basa en la teoría de gestión de calidad, o por sus siglas en inglés PDCA (Plan, Do, Check, Act. Planificar, Hacer, Verificar, Actuar en español) y describe cómo gestionar la seguridad de la información en una empresa para la mejora continua de los sistemas de información y garantizar la ciberseguridad de los activos de información. (García, 2022. párr. 7).

Además, es importante tener en cuenta que:

> Hoy, la información de una empresa es su mayor tesoro y hay que protegerlos para que no sufran ningún tipo de fraude, hackeo, sabotaje, espionaje, vandalismo o incluso un mal uso por parte del ser humano. Por este motivo, es importante contar con herramientas que permitan evitar este tipo de acciones y gracias a la norma ISO 27001 puedes conocer la metodología que debes seguir para implementarlo y poder cumplir con lo exigido. (Blog Emagister, 2023. párr. 4).

Con lo que respecta a su funcionamiento, básicamente se puede resumir en "[…] una forma de seguridad de información. Entendiendo esto último como las medidas preventivas de resguardo

de información de sistemas. Esto quiere decir que busca mantener la confidencialidad e integridad de los datos, independientemente de su formato.” (García, 2023. párr. 9).

Respecto del tema legal en Costa Rica toda organización debe tener presente que en nuestro país ya existe un reglamento de protección de datos, como lo es la Ley 8968 misma que se debe respetar, ya que su foco principal es velar por la seguridad de la información y de los datos que son un activo muy importante en toda organización actualmente.

Por lo anterior se pretende desarrollar este proyecto mediante el cual se analizará cada uno de los procesos de la Compañía con el fin de obtener información para posteriormente diseñar las políticas y mejores prácticas basadas en la norma ISO 27001, y además que estas queden debidamente documentadas para su futura implementación con el fin de generar mucho más valor y seguridad en los procesos internos de la organización en estudio.

Antecedentes del problema

En la actualidad, la seguridad informática cumple una función importante en las organizaciones, además en los últimos años esta área de la tecnología ha tenido un crecimiento elevado por lo que se ha convertido en un sistema de seguridad de los datos e información así como los activos y personas que pertenecen a una organización, por esto las empresas implementan con más frecuencia dentro de sus esquemas y tecnología distintas normas y estándares que mejoren la seguridad informática dentro de estas.

Soluciones Seguras, actualmente cuenta con políticas y reglas para sus procesos, sin embargo muchas de estas no se encuentran de la mejor manera documentadas o diseñadas, con base a un estándar internacional que ratifique que la manera en que se aborda el proceso sumado a la debida documentación que conlleva sea la más optima además de que con el tiempo estas dejen de aplicarse o se conviertan en desconocimiento por parte de los empleados que conforman

la organización, por esto se busca el actualizar o diseñar y además documentar las políticas y mejores prácticas con base en la norma ISO 27001 aplicadas a los procesos dentro del Departamento de Tecnología con el fin de que a futuro sean aplicadas de la manera más eficiente en pro de favorecer y aumentar la seguridad informática.

En Colombia (2017), Caro, Cubillos realizan una investigación basada en *Diseño del sistema de gestión de seguridad de la información (SGSI) para el proceso de soporte y desarrollo de software de la empresa FINANCOL, basado en la norma ISO/IEC 27001:2013*. Esta tiene como fin el poder crear un SGSI para un proceso en específico de la compañía, en donde plantean identificar activos además de analizar los riesgos, así como documentar los tratamientos y las posibles políticas que aplican para los resultados obtenidos para poder crear una concienciación de la importancia de la seguridad de la información.

Uno de los aspectos más importantes a la hora de realizar los análisis respectivos para las organizaciones es poder tener una claridad de cuáles son las mejores prácticas , así como las políticas que mejor se adecuan a los objetivos y siempre tomando en cuenta un estándar internacional que respalde las decisiones tomadas para el diseño y documentación, además cabe mencionar, que es por medio del material oficial de la norma así como los libros respectivos que se toman como medios de apoyo para generar la ruta de trabajo que se adapte a las necesidades y procesos de la organización.

Definición y descripción del problema

Una correcta definición y descripción del problema para el proceso investigativo hacen que se tenga una mejor visión y claridad, respecto los objetivos, además de establecer cuáles son los puntos que se deben cubrir para solucionar el problema planteado, detalles que se definirán seguidamente en este documento.

Para toda organización, actualmente los temas de seguridad informática, específicamente en el campo que asegura la información buscan cómo mejorar o incluir en sus políticas las mejores prácticas que indican los organismos internacionales.

Soluciones Seguras al ser una compañía que se desempeña en el campo de las soluciones de seguridad informática debe tener dentro de sus planes por seguir la adopción de un estándar internacional que permita diseñar las políticas que no existan para sus procesos, así como rediseñar estas en el caso de las que se tengan implementadas para así evitar situaciones imprevistas que comprometan los activos valiosos de información.

La seguridad de la información, ahora es un campo de la tecnología, relativamente nuevo por lo que las empresas se encuentran adoptando distintas normas y estándares internacionales con la finalidad de salvaguardar uno de los activos más importantes como lo es la información y sus procesos asociados es por esto que se plantea la pregunta ¿Cuáles políticas y mejores prácticas basado en la norma ISO 27001 aplican para el Departamento de Tecnología de la empresa Soluciones Seguras Costa Rica?, con el fin de poder tener más clara la definición y descripción del problema al que se apega la propuesta planteada de trabajo.

Justificación

La normativa ISO 27001 es una de las más importantes e utilizadas en el nivel mundial por las organizaciones, ya que busca garantizar un mejor tratamiento y aseguramiento de la información, procesos, datos, por lo que "[…] estas guías tienen como objetivo establecer las mejores prácticas en relación con diferentes aspectos vinculados a la gestión de la seguridad de la información, con una fuerte orientación a la mejora continua y la mitigación de riesgos." (GlobalSuite Solutions, 2022. párr. 2).

En lo que respecta a la parte metodológica de la norma ISO 27001 para el diseño de políticas de seguridad de la información este permite una gestión sistemática y efectiva de los riesgos asociados con la información que maneja una organización. Además, permite a las organizaciones identificar riesgos, adoptar un enfoque basado en procesos, promover la mejora continua y establecer su reputación en el mercado internacional.

Además, el correcto diseño de políticas y mejores prácticas esto siempre basado en un marco normativo, como lo es en este caso ISO 27001 hace que la información y datos se encuentren de una manera más segura, correcta y ordenada, además esto beneficia para un mayor control de los activos y sus procesos por esto se recomienda el tener el diseño y documentación de estas mejoras prácticas y políticas.

En resumen, el diseño de políticas basadas en la norma ISO 27001 proporciona una estructura sólida y reconocida, internacionalmente para la gestión de la seguridad de la información en una organización. Esto garantiza la protección de los activos de información, el cumplimiento normativo, la mejora continua y la ventaja competitiva.

Viabilidad

Como parte de la viabilidad para el desarrollo de este proyecto se han tenido presente y tomado en cuenta múltiples factores de ambas partes involucradas, si la Compañía y el desarrollador e investigador han tenido conversaciones para definir y tener claro los alcances, que, a su vez, sean viables para su desarrollo y también garantizar que ambas partes salgan beneficiadas de este proyecto.

Es por esto, que parte de la viabilidad comprende tres puntos muy importantes, como lo son: punto de vista técnico, operativo y económico que se abarcarán a continuación en este

documento que además respaldarán que este proyecto se lleve a cabo sin problemas y con la obtención de buenos resultados.

Punto de vista técnico

Respecto del punto de vista técnico el desarrollador e investigador de este proyecto tiene las capacidades técnicas y desarrollo profesional para poder llevar a cabo y realizar el diseño de políticas de seguridad, con base en la norma ISO 27001 para la Compañía Soluciones Seguras.

Tomando en cuenta todo el conocimiento adquirido durante el proceso de aprendizaje para obtener la licenciatura en Seguridad Informática sumado a que por parte del desarrollador e investigador cuenta con las certificaciones de Fundamentos y Auditor Interno de la ISO 27001, esto complementará a que se tenga la capacidad necesaria para plantear un proyecto de esta magnitud.

En conclusión, se puede tener la certeza de que se cuenta con la habilidad sumado a la experiencia que se requiere para poder realizar el diseño de políticas de seguridad con base en la norma ISO 27001 para la Compañía Soluciones Seguras lo que beneficiaría en distintas aristas a la empresa, además de aumentar su imagen y prestigio antes sus clientes y competencia.

Punto de vista operativo

Cuando se habla del punto de vista técnico para este proyecto es importante mencionar que al ser Soluciones Seguras una empresa como lo indica en su nombre orientada a la seguridad informática, el diseño de políticas basado en un marco normativo, como lo es la ISO 27001 genera un valor dentro de los procesos seleccionados, así como un incremento en el prestigio de la Compañía, ya que esto marca el inicio para la preparación y obtención a futuro de la certificación de este marco normativo internacional.

Cabe mencionar que este proyecto no generará un impacto negativo o la pérdida de la disponibilidad de ningún servicio o solución dado que se trabajará en paralelo para analizar, diseñar y documentar los procesos que serán tomados en cuenta para el diseño respectivo de políticas de seguridad.

En resumen, este proyecto es totalmente viable que además no generará ningún inconveniente con la operatividad diaria de la empresa, si no, que al contrario dará mucho valor para compañía.

Punto de vista económico

Con lo que respecta al apartado económico, este proyecto se basará, únicamente bajo el detalle de "hora consultora" teniendo en cuenta que lo que se requiere para desarrollar y poder llevar a cabo el proyecto son horas de investigación, análisis, diseño y documentación.

Es importante tener claridad que todas estas horas de consultor que se requieren corren por parte del investigador y desarrollador del proyecto, por lo que no implica que la empresa tenga que incurrir en alguna carga económica por motivos del desarrollo de este trabajo final de graduación.

Objetivos

Como parte del desarrollo de esta investigación se plantearon los siguientes objetivos.

Objetivo general

a) Diseñar políticas y mejores prácticas basado en el marco de referencia ISO 27001 para la mejora de la seguridad de la información del Departamento de Tecnología de la empresa Soluciones Seguras Costa Rica en el segundo cuatrimestre del año 2023.

Objetivos específicos

a) Analizar los procesos críticos que involucren la seguridad de la información, a través de la realización de encuestas y entrevistas con el propósito de que se evidencien las posibles debilidades o amenazas existentes en estos.

b) Plantear políticas y mejores prácticas basadas en la norma ISO 27001 para los procesos críticos definidos en búsqueda de mayor robustez y mejoría de la seguridad de la información.

c) Diseñar la documentación de las políticas de seguridad basadas en las mejores prácticas para el manejo de la información y la optimización de la seguridad.

Alcances y limitaciones

El propósito fundamental de esta investigación es poder definir y tener claridad en cuáles serán los alcances y limitaciones que este proceso pueda presentar por lo que a continuación se detallan cuáles son los puntos específicos para cada una de las partes indicadas.

Alcances

- Mediante validaciones respectivas encontrar los distintos procesos críticos además de sus posibles debilidades y amenazas para enlistarlos y tomarlos en cuenta en las siguientes etapas.
- Crear las políticas y mejores prácticas, con base a la norma ISO 27001 para los procesos críticos previamente definidos para reforzar y resguardar la información que se utiliza en estos procesos.
- Terminar y entregar la documentación correspondiente a las políticas y mejores prácticas que se diseñaron, esto para que a un futuro sean implementadas paulatinamente dentro de la Compañía, que además garantizará una mejora y

optimización en la seguridad de la información inmersa en los procesos relevantes para los usuarios y la organización.

Limitaciones

Una parte fundamental de este trabajo es tener la claridad acerca de cuáles son las posibles limitaciones que influyen o afectan directa o indirectamente el desarrollo de este, las que se detallan a continuación:

- Acceso a la información: Al realizarse este proyecto dentro de una empresa que se ubica en el sector de la seguridad informática el acceso a la información y a las personas usuarias de esta se complica, por lo que esto incurre en atrasos, ya que se necesita tener acceso a información específica, como: manuales, procedimientos y controles para poder llevar a cabo con éxito este trabajo.
- Disponibilidad para programar reuniones: Este aspecto representa una limitación muy marcada para la realización de este proyecto, ya que por lo general las jefaturas y colaboradores involucrados suelen tener las agendas bastante comprometidas por lo que el obtener un espacio para una sesión se convierte en algo complicado que en ocasiones puede llegar a tardarse hasta más de una semana y esto se convierte en atrasos para poder realizar este trabajo.

Marco de referencia organizacional y socioeconómico

El marco de referencia organizacional y socioeconómico de la empresa Soluciones Seguras se refiere al contexto en el que opera la empresa y los factores que influyen en su estructura, estrategias y desempeño, tanto en el nivel interno como externo. Aquí hay algunos aspectos relevantes para considerar:

La parte organizacional comprende los temas de visión y misión que esto consiste en las declaraciones que definen el propósito y la dirección de la empresa, así como además la estructura organizacional que es la forma en que la Compañía se encuentra estructurada en donde se incluyen todas las unidades de negocio y la jerarquía. Soluciones Seguras, en todas sus líneas cuenta con personal altamente capacitado y profesional para el desarrollo de las tareas y funciones establecidas y por último se debe también tomar en cuenta la cultura empresarial la cual comprende: los valores, comportamientos y normas que se comparten y promueven dentro de la organización, las que influyen directamente en la toma de decisiones y en las actividades que esa desempeña.

Con lo que corresponde a la parte socioeconómica se debe tener en cuenta el sector de la industria en la que Soluciones Seguras opera como lo es el sector de seguridad informática y tecnológica, así como el análisis de la competencia directa e indirecta en el mercado y cómo la organización se posiciona frente a esta, además también los clientes a los que se dirige la empresa, el perfil de estos y cuáles son las necesidades y expectativas y también la importancia del marco regulatorio que afectan a la organización y a todo el sector, como lo son, la protección de datos y la ciberseguridad.

El marco de referencia organizacional y socioeconómico es fundamental para que Soluciones Seguras entienda su posición en el mercado, tome decisiones estratégicas y se adapte a los cambios del entorno.

Historia

Soluciones Seguras S.A. es una empresa de seguridad informática con más de 20 años en el mercado fundada con el objetivo de brindar soluciones confiables y sólidas para proteger la información sensible de las organizaciones.

Desde sus inicios, Soluciones Seguras se destacó por su enfoque en la innovación y la adopción de las mejores prácticas en seguridad. La empresa se especializó en ofrecer servicios de seguridad de redes perimetral y centros de datos, esto por medio de soluciones de Firewall.

A medida que la importancia de la seguridad cibernética aumentaba en todo el mundo, Soluciones Seguras se convirtió en un referente en el mercado. La empresa amplió su gama de servicios para incluir soluciones PAM, Firewalls de nueva generación, balanceo de aplicaciones, criptografía, SOC entre algunos otros.

Con el tiempo, Soluciones Seguras desarrolló alianzas estratégicas con importantes fabricantes de tecnología de seguridad, lo que les permitió ofrecer a sus clientes soluciones de vanguardia y mantenerse con las últimas tendencias en el campo de la ciberseguridad.

La empresa se ganó la confianza de clientes en diversos sectores, incluyendo instituciones financieras, entidades gubernamentales, empresas de telecomunicaciones y organizaciones de salud. Su enfoque en la calidad, la atención personalizada y la entrega de resultados tangibles le permitieron obtener una excelente reputación en el mercado.

Hoy, Soluciones Seguras S.A. se ha convertido en un líder reconocido en el campo de la seguridad informática. Su equipo de expertos altamente capacitados y certificados trabaja en estrecha colaboración con los clientes para comprender sus necesidades y proporcionar soluciones personalizadas que aborden los desafíos de seguridad específicos de cada organización.

La empresa continúa creciendo y evolucionando en respuesta a las amenazas cibernéticas en constante cambio. Su compromiso con la excelencia y su enfoque proactivo en la seguridad de la información aseguran que Soluciones Seguras S.A. siga siendo un socio confiable para sus clientes a futuro.

Tipo de negocio y mercado meta

Soluciones Seguras es una empresa que se dedica a la venta de múltiples soluciones de seguridad informática, con más de 20 años en el mercado y que además como bien lo menciona el slogan en su logo “Empresas Seguras, Empresas Tranquilas”, hacen que se refuerce el concepto del compromiso adquirido por parte de la empresa hacia la búsqueda de la alta satisfacción de los clientes, así como la garantía de la ciberseguridad.

En cuanto al mercado meta Soluciones Seguras se enfoca hacia todas las compañías y organizaciones de todos los sectores de la economía de la región Centroamericana en busca de ser siempre la primera y la mejor opción en temas de ciberseguridad.

Es importante indicar que Soluciones Seguras no solamente se quede con el detalle de la venta de soluciones de seguridad, sino que además brinda planes de soporte con personal altamente capacitado para cada una de estas soluciones, así como el acompañamiento y asesoría en lo que respecta a nuevas soluciones, además de contar con múltiples alianzas con los proveedores de ciberseguridad más importantes en el nivel internacional.

En resumen, el tipo de negocio en el que se encuentra Soluciones Seguras se basa en la venta de soluciones de ciberseguridad, así como también el soporte especializado y de calidad para cada una estas soluciones para todo Centroamérica, así como para todos los sectores económicos de la región.

Misión, Visión y Valores

Misión

Soluciones Seguras en su misión detalla lo siguiente:

> Brindarles a nuestros clientes tranquilidad a través de asesoría y las mejores soluciones de ciberseguridad en la región. Estamos comprometidos con la excelencia, a exceder las

> expectativas de soporte técnico y servicio de nuestros clientes y garantizar un excelente ambiente de trabajo y un alto grado de satisfacción de nuestro personal. (párr.3)

Visión

Como parte de la visión que tiene la Compañía Soluciones Seguras se muestra a continuación: “Ser la primera alternativa en ciberseguridad para las empresas y organizaciones de todos los sectores económicos de Centroamérica”. (párr.4)

Valores

Como parte fundamental de toda organización existen los valores que promueven y que dentro de la misión y visión se encuentran inmersos, por lo que en este caso, se pueden mencionar y detallar los siguientes:

- Integridad: Actuar de manera ética y transparente en todas las interacciones comerciales.
- Calidad: Buscar la excelencia y ofrecer productos o servicios de alta calidad.
- Innovación: Fomentar la creatividad y la búsqueda constante de nuevas soluciones.
- Orientación al cliente: Poner las necesidades y la satisfacción del cliente en primer lugar.
- Responsabilidad social: Contribuir de manera positiva a la sociedad y el medio ambiente.
- Trabajo en equipo: Fomentar la colaboración y el apoyo mutuo entre los miembros de la organización.
- Respeto: Siempre se busca tratar a los demás con respeto y fomentar un ambiente agradable y respetuoso.

- Orientación a resultados: Establecer metas claras y tomar medidas para lograr resultados exitosos.
- Aprendizaje continuo: Promover el desarrollo profesional y el aprendizaje constante.
- Adaptabilidad: Ser flexible y capaz de responder a los cambios en el entorno empresarial.

Con esto se puede concluir que la empresa Soluciones Seguras tiene múltiples valores que hacen que esta sea una empresa fuerte, tanto en lo interno como lo externo, además que gran parte de su renombre y prestigio se respalda en sus valores y que también marcan el camino por seguir por parte de la organización.

Políticas institucionales

En este apartado se abordan las políticas institucionales con las que cuenta Soluciones Seguras, estas se muestran a continuación:

Política de contraseñas: Soluciones Seguras cuenta con política definida para el manejo adecuado de contraseñas. Estos lineamientos se enfocan en garantizar la seguridad y confidencialidad de la información.

Política de seguimiento de tiquetes: En cuanto a la gestión de tiquetes, Soluciones Seguras cuenta con una política establecida. Los empleados encargados de atender las solicitudes de clientes y usuarios deben asegurarse de registrar y gestionar cada tiquete de manera. Además, existe un tiempo máximo establecido para responder a los tiquetes y una pauta para el cierre satisfactorio de estos.

Política de acceso a las instalaciones: Con el fin proteger la seguridad física de las instalaciones, la compañía ha implementado una política de acceso. Los empleados deben utilizar

sistemas de biometría para ingresar a las áreas restringidas de la empresa. También se exige a los visitantes registrarse en la recepción y estar acompañados por un empleado autorizado durante su estadía en las instalaciones.

Política de conectividad y accesos: La empresa tiene definida una política para el acceso a recursos y sistemas informáticos internos. Los empleados tienen asignados roles y permisos específicos según sus funciones, lo que les permite acceder solo a la información y aplicaciones necesarias para realizar sus tareas laborales.

También, Soluciones Seguras cuenta con un Pacto de Integridad que promueve la ética y el comportamiento responsable en todos sus empleados. Este enfoca en la transparencia, honestidad y la lucha contra cualquier forma de corrupción. Esta política se considera una parte fundamental para mantener una cultura organizacional sólida y generar confianza tanto interna como, externamente.

Por último, es importante mencionar que, aunque Soluciones Seguras cuenta con ciertas políticas definidas y manuales de procedimientos establecidos, estas no se encuentran directamente alineadas o basadas en una normativa internacional. Por lo que el objetivo de este proyecto permitirá que la empresa alcance estándares reconocidos en el nivel global y pueda mejorar la eficiencia y la calidad en sus procesos, así como el aumento en la confianza y reputación hacia los clientes.

Estado de la cuestión

Dicho marco de referencia ISO 27001 establece un conjunto de requisitos y mejores prácticas para la gestión de la seguridad de la información. A continuación, se muestran algunos casos de estudio de diseño de políticas de seguridad de la información según la norma:

Como primer caso se habla de la empresa Becomit que recientemente obtuvieron la certificación de la norma ISO 27001 lo que les generó un valor añadido a lo interno como a lo externo y su director ejecutivo (CEO, por sus siglas en inglés) menciona lo siguiente:

> Con esta certificación Becomit garantiza una serie de procesos a la hora de implementar, mantener y mejorar de forma continua la seguridad de la información tanto de nuestra empresa como de nuestros clientes, partiendo de los riesgos que puedan llegar a comprometerla. (Lluis, 2023. párr. 3).

Desde otro punto, otra compañía que se sometió a extensas auditorías y cambios para poder lograr la certificación de la norma fue en DEXMA en (2022), en donde mencionan que "[…] este logro les permite poder dar una garantía a los clientes y socios porque los esto les asegura que los datos se están gestionado de la manera más optima basado en las mejores prácticas a nivel internacional". (párr.3).

Como se puede notar en cada uno de estos casos, la norma ISO 27001 permitió a las organizaciones diseñar políticas de seguridad de la información que abordaban los riesgos específicos de su entorno operativo y establecer controles de seguridad efectivos para mitigar esos riesgos , además de ofrecer una garantía mayor a sus colaboradores y clientes de que la información se está tratando gestionando de una manera segura y adecuada basado en una norma de seguridad informática de carácter internacional.

Desde otra arista, una de las partes fundamentales que favorecen el realizar una correcta investigación se encuentran las fuentes de información que, básicamente se trata de toda aquella documentación que aportan conocimiento e información y que varían según la necesidad que torne con base en el proceso de investigación. Como parte de este proceso se utilizarán tres tipos de fuentes, como lo son: las primarias, secundarias y terciarias.

Además, también se debe tener en cuenta lo que menciona Suarez (2017):

> Es importante tener en cuenta que no todas las fuentes de información son igualmente confiables o relevantes para cada tema o disciplina. Por eso, es fundamental saber cómo evaluar la calidad y pertinencia de las fuentes de información para poder seleccionar las mejores para nuestro trabajo. (párr.5)

Fuente Primaria

Como parte de su definición se puede decir que una fuente de información primaria "[…] contiene información que no ha sido alterada, interpretada o analizada por otros autores, sino que es del propio autor. En otras palabras, información que se mantiene intacta desde su elaboración." (Coll, 2021. párr.1).

Dado lo anterior respecto de la definición para esta investigación se detalla que la fuente primaria en este caso es toda la documentación oficial que existe de la norma por utilizar para el diseño y documentación de políticas en Soluciones Seguras, ISO 27001, ya que esta documentación es la que contiene todos los pasos por seguir con los mejores estándares internacionales.

Fuente Secundaria

Cuando se habla de una fuente secundaria su definición se detalla según indica Coll (2021):

> La fuente de información secundaria, por tanto, contiene información ampliada de los resultados que expone la fuente primaria. En otras palabras, se trata de aquel contenido que se ha ido generando a partir de una fuente primaria. Puede ser un análisis, una valoración, una traducción o algún contenido que nos relacione con la fuente primaria. (párr.1)

Dada la definición anterior se toma en cuenta para este trabajo las fuentes de información secundarias que complementen a las fuentes de información primarias, que en este caso, se puede

referir a otros ensayos e investigaciones que tiene su objetivo basado en la ISO 27001, para así poder ampliar aún más los detalles de la norma internacional por utilizar.

Fuente Terciaria

Las fuentes terciarias son aquellas que tienen la posibilidad de encontrarse en las fuentes de información que ayudan al investigador de una manera un poco más resumida en el análisis que realiza, con lo que respecta a su definición se puede decir que una fuente de información terciaria es:

> Una fuente terciaria consolida y organiza las fuentes primarias y secundarias juntas en una sola fuente para facilitar el acceso rápido a la información. Las fuentes terciarias son buenos puntos de partida para proyectos de investigación porque a menudo extraen el significado esencial o los aspectos más importantes de grandes cantidades de información en un formato conveniente. (Investigadores,2020. párr.19)

En cuanto a esta fuente de información terciaria se basa en todos los datos que sean proporcionados por Soluciones Seguras, como los son: los procesos, minutas de reuniones y documentos relacionados que puedan aportar al proceso de diseño y documentación de políticas y que además tengan un alto grado de importancia para la organización.

En conclusión, en esta labor investigativa se tiene contemplado las tres fuentes de información mencionadas, ya que todas realizan su aporte de valor con el fin de sustentar el objetivo del trabajo, además de contribuir con incrementar el conocimiento.

Capítulo 2. Marco Teórico o Conceptual

En este capítulo se lleva a cabo detalladamente la teoría relacionada con esta investigación la cual sustenta los resultados obtenidos a partir del análisis, hipótesis, antecedentes para generar resultados que a su vez conduzcan a las conclusiones asertivas y objetivas.

Además, es por medio también de un árbol genealógico que se exponen los conceptos teóricos utilizados a en la creación de todo el estudio.

Seguridad de la información

Como parte de la nueva era de la seguridad que se traslada a la tecnología y la búsqueda continua de las organizaciones por resguardar su información conlleva a que este concepto cada vez tome más fuerza y que además se pueda definir como "[…]conjunto de medidas preventivas y procedimientos para controlar el tratamiento de los datos que se utilizan en una empresa." (Grupoacms, 2020. párr. 1).

Además, la seguridad de la información se compone de tres pilares importantes que su equilibrio dentro de las compañías colabora a la seguridad de los datos y los procesos.

Confidencialidad

Uno de los tres pilares que se encuentran inmersos en la seguridad informática es la confidencialidad y que además se puede decir que "[…] la información sólo debe ser conocida por las personas que necesitan conocerla y que han sido autorizadas para ello. Este principio asegura que la información no va a ser divulgada de manera fortuita o intencionada." (Unir México, 2022. párr. 3).

Integridad

La completitud y credibilidad de la información es de suma importancia en los que respecta a la seguridad por lo que en este término se debe tener en cuenta que la misma "[…] no ha sido manipulada por terceros de manera malintencionada. Esto garantiza que la información no será modificada por personas no autorizadas." (Unir México, 2022. párr. 4).

Disponibilidad

La disponibilidad de la información es un aspecto fundamental cuando se habla en temas de seguridad informática, por lo que se refiere a "[…] a que la información debe estar disponible siempre para las personas autorizadas para accederla y tratarla, y además puede recuperarse en caso de que ocurra un incidente de seguridad que cause su pérdida o corrupción." (Unir México, 2022. párr. 5).

Dato

En (2022), Datademia, menciona que un dato se puede definir como "una representación simbólica de un atributo cuantitativa o cualitativa" (párr.1), además es importante mencionar que un dato por sí solo en la mayoría de los casos no significa nada, pues por sí solo no es posible deducir algo de este pues requiere unirse a más datos para poder tener un valor.

Información

La información se compone de muchos datos reunidos o relacionados que toman cierto grado de valor para quien los recibe. También se puede definir como "[…] información (general) es cualquier dato obtenido por una persona, independientemente de su forma de presentación." (Lucena, 2022. párr. 2).

Datacenter

Los datacenter son parte fundamental en cuanto a los temas de tecnología y seguridad informática es por lo que se puede decir que:

> Un datacenter es una infraestructura física o virtual utilizada para alojar sistemas informáticos que puedan procesar, servir o almacenar datos. Data Center dan servicio de

> almacenamiento de datos, respaldo o backup, recuperación de datos y gestión de la información para empresas. (Datos101, 2023. párr. 1).

Política de seguridad

Un concepto que prevalece durante todo este documento y que es parte fundamental del desarrollo de este proyecto es la política de seguridad que se detalla a continuación:

> La política de seguridad define qué es lo que desea proteger y qué espera de los usuarios del sistema. Proporciona una base para la planificación de la seguridad al diseñar nuevas aplicaciones o ampliar la red actual. Describe responsabilidades del usuario como las de proteger información confidencial y crear contraseñas no triviales. La política de seguridad también debe describir cómo se va a supervisar la efectividad de las medidas de seguridad. Esta supervisión le ayudará a determinar si alguna persona podría intentar burlar sus defensas. (IBM, 2021. párr. 2).

ISO

La ISO es la organización que tiene como función crear normas y estándares internacionales que comprenden varios sectores en las empresas, se dice que es:

> La “Organización Internacional de Normalización” o ISO, es el organismo encargado de promover el desarrollo de normas internacionales, tanto de productos como de servicios, a través de la estandarización de normas voluntarias que se usan en las empresas para su mayor eficiencia y rentabilidad económica. (ProChile, 2020. párr. 1).

ISO 27001

La existencia de normativas y estándares internacionales en el nivel de seguridad de la información lleva a poder hablar acerca de la norma ISO 27001 que se puede definir según GlobalSuite Solutions (2023) como:

> […] un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información. La norma proporciona un marco para la seguridad de la información que ayuda a las organizaciones a identificar y gestionar sus riesgos de seguridad de la información de manera efectiva. (párr. 1).

ISO 27002

Tomando en cuenta la existencia de las ISO 27001 que definen los requisitos para un SGSI es importante tener en el radar la ISO 27002, ya que esta complementa la primera y establece la guía de la norma para el diseño y creación del SGSI, por lo que se puede decir que:

> La ISO 27002 proporciona directrices para la implementación de controles requeridos en un SGSI en una organización. La norma ISO 27002 se enfoca en las medidas de seguridad necesarias para proteger la información y cubre una amplia gama de áreas, como la gestión de riesgos, la seguridad física, la seguridad de la red y la seguridad de la información. (Grupo Cynthius, 2023. párr. 3).

Teorías Relacionadas

La norma ISO 27001 establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI) eficaz en una organización. Algunas teorías relacionadas con el diseño de políticas de seguridad basado en la norma ISO 27001 incluyen:

Modelo de Madurez de Seguridad de la Información (CMMI-SVC): Este modelo es un marco de referencia para la mejora del proceso de seguridad de la información. Proporciona un conjunto de prácticas recomendadas que pueden favorecer a las organizaciones a mejorar su capacidad para gestionar los riesgos de seguridad de la información. El modelo se divide en cinco niveles de madurez, desde el nivel inicial hasta el nivel óptimo.

Modelo de Gestión de la Seguridad de la Información (ISMS) de la norma ISO 27001: Este modelo es un marco de referencia para la gestión de la seguridad de la información. Proporciona un conjunto de políticas, procedimientos, directrices y controles para proteger la información de una organización. La norma ISO 27001 establece requisitos específicos para el diseño, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información.

Marco de Ciberseguridad del NIST (National Institute of Standards and Technology): Este marco proporciona un conjunto de directrices, estándares y prácticas recomendadas para mejorar la ciberseguridad de las organizaciones. El marco se divide en cinco funciones principales: Identificar, Proteger, Detectar, Responder y Recuperarse.

Teoría de la Gestión de Riesgos: Esta teoría se centra en la identificación, evaluación y mitigación de los riesgos de seguridad de la información. Proporciona un conjunto de técnicas y herramientas para ayudar a las organizaciones a identificar los riesgos, evaluar su impacto y probabilidad, y desarrollar medidas de mitigación para reducir el riesgo.

Teoría de la Seguridad de la Información: Esta teoría se centra en la protección de la información contra amenazas externas e internas. Proporciona un conjunto de directrices y mejores prácticas para la gestión de la seguridad de la información, incluyendo el diseño de políticas de

seguridad, la implementación de controles de seguridad y la educación y concienciación de los usuarios.

En resumen, estas teorías proporcionan un enfoque sistemático y estructurado para el diseño y la implementación de políticas de seguridad de la información basado en la norma ISO 27001.

Capítulo 3. Marco Metodológico

Tipo de Investigación

Para este proyecto final de graduación se utilizará la investigación de tipo aplicada la cual se puede detallar así:

"La investigación aplicada, por tanto, permite solucionar problemas reales. Además, se apoya en la investigación básica para conseguirlo. Esta le aporta los conocimientos teóricos necesarios para resolver problemas o mejorar la calidad de vida." (Rus, 202. párr. 1)

El objetivo principal de la investigación aplicada es proporcionar respuestas, soluciones o recomendaciones prácticas para problemas o desafíos específicos que enfrenta la sociedad, las organizaciones o las personas. Los resultados de este tipo de investigación suelen ser directamente aplicables y pueden tener un impacto inmediato en la toma de decisiones y en la resolución de problemas prácticos.

Tomando en cuenta lo anterior, además de tener en cuenta las necesidades y alcances de este proyecto es que se opta por utilizar este tipo de investigación, maximizando los resultados de manera positiva y aporta de manera exitosa al cumplimiento de este trabajo.

Alcance investigativo

Con lo que respecta al alcance investigativo se utilizará el tipo exploratorio lo, que favorece a que se tenga una investigación de manera preliminar para así obtener más conocimiento acerca de la situación, la cual tiende a ser poco conocida y que hace parte en la mayoría de los casos de otras investigaciones tomadas como proyecto, pero que tornan a ser más profundas.

El diseño de estas políticas sumado a que en un futuro serán implementadas garantiza que exista un procedimiento de seguridad para la información y los servicios, sin embargo, esto a pesar de que se hace con base en una norma internacional no garantiza que sea infalible, ya que los

riesgos siempre están presentes, las amenazas se actualizan y pueden generar nuevas vulnerabilidades, pero sí, que el adoptar estas mejores prácticas hace que a estas amenazas se les complique mucho más el trabajo de poder explotar vulnerabilidades.

Conforme se actualizan las vulnerabilidades y amenazas los riesgos también tienen el mismo comportamiento por lo que es acá donde se recalca que se debe también tener un esquema de mejora continua que conforme se detallen o se encuentren nuevos riesgos asociados a los procesos y activo de información se defina de inmediato su tratamiento, ya sea en este caso eliminar, transferir, aceptar o mitigar el mismo esto tomando en cuenta todas las aristas del riesgo y su afectación sumando a la probabilidad en tiempo de que el mismo suceda esto también complementa a que por medio de la adopción de estas normas internacionales, que prácticamente obligan a mantener una mejora continua estos procesos de evaluación y análisis de los riesgos se torne de manera periódica.

Por lo cual, se debe tener el detalle con claridad de que la propuesta que presenta a Soluciones Seguras es basada en mejores prácticas y recomendaciones de carácter internacional que son utilizadas por múltiples compañías en el nivel global de diferentes campos y ámbitos que además de buscar proteger su información y recursos también buscan generar una confiabilidad alta en aquellas empresas que deciden adoptar estas normativas y que sobre todo conllevan a tener una mejora continua, pues las amenazas también constantemente se actualizan lo que permite que haya una optimización y resguardo continuo en las compañías.

Enfoque

Con lo que respecta a esta investigación, es de tipo cualitativa lo que hace posible que se pueda obtener la información necesaria para poder llevar a cabo el diseño de políticas mencionadas en el objetivo general, propuesta que además se desarrollará en la compañía Soluciones Seguras

ya que hay que tener claro que al ser una empresa dedicada vender soluciones y servicios de seguridad informática es sumamente importante que sus políticas y procesos estén diseñados con base a una normativa internacional como lo es la ISO 27001 para así poder tener una robustez en la capa seguridad de la información.

El uso de normativas o marcos de referencia internacionales como lo es en este caso ISO 27001 orientado a la seguridad de la información permite a las organizaciones en este caso a Soluciones Seguras poder garantizar que se cumple con los tres pilares más importantes de la seguridad informática como lo son la Confidencialidad, Integridad y disponibilidad además de crear una cultura que busque, constantemente, la protección de sus procesos y la información que conlleva cada uno de estos.

Tomando en cuenta lo anterior, según menciona García Martínez (2023):

> La ISO/IEC 27001 estable que las "Políticas de Seguridad de Información son preceptos que debe cumplir todo el personal de una compañía, de manera que se asegure su: Integridad, garantizando que la información y sus métodos de proceso son exactos y completos". (párr. 2)

En resumen, la importancia de esta investigación radica en varios puntos; con esta no solamente se busca proteger un activo tan valioso como lo es la información y sus activos, sino que además que incrementa la reputación, tanto interna como lo son los empleados, así como externa que se refiere a los clientes actuales y también beneficia la atracción de nuevo clientes.

Diseño

El diseño de la investigación comprende un análisis acerca de cuáles son los procesos más críticos o importantes para la organización que con los resultados obtenidos mediante el análisis se enlisten para poderles diseñar políticas de seguridad teniendo como referencia un marco

internacional de seguridad de la información lo que generará un mayor control en los procesos con base en los activos y la información inmersa en estos procesos y que también aumenta la seguridad informática de la Compañía.

Es por esto por lo que dicha investigación se basara en una metodología de análisis de tipo cualitativa en donde se fundamentara en las fuentes de información propias del marco de referencia internacional, así como fuentes de otros trabajos de diseño y la documentación brindada por la compañía además de que el principal objetivo de dicho trabajo es poder fortalecer la seguridad de la información dentro de la organización por medio de un estándar de tanto renombre internacional así como las mejores prácticas indicados en la norma ISO 27001.

Tomando en cuenta lo anterior es que toma más fuerza el trasfondo de este proyecto en donde se realizará el diseño de políticas sumado a la documentación de las mismas según el marco normativo ISO 27001 que es uno de los estándares internacionales más fuertes con lo que respecta al sector tecnológico en el ámbito de la seguridad informática para así brindar la confianza a sus clientes y así enviar un mensaje más el ejemplo de una empresa que busca constantemente ser lo más segura posible, a lo interno para dar aún más seguridad a lo externo en sus soluciones.

Población y Muestreo

Como parte del desarrollo de este proyecto el cual consiste en poder diseñar políticas de seguridad basadas en el marco normativo ISO 27001 por parte de la Compañía Soluciones Seguras se estará trabajando directamente con el director ejecutivo (CEO, por sus siglas en inglés), el director operativo (COO, por sus siglas en inglés) y Gerente Regional de Ingeniería por medio de reuniones previamente planificadas, correos electrónicos y además de la información que sea compartida por parte de la organización lo que facilita un mejor desarrollo por el hecho de tener contacto directo con la Gerencia de esta.

Además, también es importante mencionar que se estará trabajando de la mano con los colaboradores y otros departamentos involucrados en los procesos seleccionados de la Compañía para poder censar y analizar toda la información necesaria para obtener resultados que respalden el objetivo de este proyecto, así como el aporte de valor de este trabajo hacia la organización.

Instrumento de recolección de datos

Como parte del desarrollo de este proyecto cuya investigación será de tipo cualitativa por lo que el investigador y desarrollador toma una función fundamental, en cuanto a la obtención de la información, ya que será quien tenga contacto directo con la Compañía, por medio de conversaciones y entrevistas, así como la lectura de documentación interna, convirtiéndose en una manera sumamente practica y útil para la recolección de información para el desarrollo de este trabajo.

Bajo esta línea, como parte de la recopilación de datos se aplicará el recurso de las encuestas y entrevistas, instrumento que funciona como: "[…] sirve para recopilar información valiosa de un grupo de interés, cuyas respuestas te servirán para analizarlas, interpretarlas y tener un panorama que te ayude a tomar decisiones o a generar alguna estrategia o acción específica." (Gómez, 2022. párr. 7), así como "las entrevistas que son una de las herramientas de recopilación de datos cualitativos más comunes, y son excelentes cuando se necesita recopilar información muy personalizada." (Velázquez, 2022. párr. 8).

En resumen, mediante estos métodos de recopilación es que se pretende recabar y recolectar toda la información necesaria para la realización de este proyecto para garantizar que los resultados del diseño de las políticas sean confiables e íntegros.

Técnica de análisis de información

Una vez que se ha realizado la recolección de información necesaria por parte de la organización se estará utilizando la técnica de análisis de la información de mapas conceptuales para poder mapear y tener una visión más clara y concisa de la información que facilite su uso y apoyo para el desarrollo del proyecto.

Los mapas conceptuales se utilizan en diversos contextos, como la educación, la planificación, la resolución de problemas y la toma de decisiones. Por lo que favorecerá al desarrollador e investigador a organizar y relacionar ideas, así como poder visualizar y discutir conceptos clave con los involucrados directos de la empresa quienes también colaboran para comprender y recordar información de manera más efectiva.

En resumen, los mapas conceptuales son representaciones de manera visual que apoyan en la organización e interconexión de los conceptos e ideas y que facilitan la comprensión y el aprendizaje. Son una herramienta de mucho aporte y valor para visualizar y comunicar información de manera clara y efectiva.

Capítulo 4. Análisis del Diagnóstico

Como parte importante de la realización de este trabajo están los datos obtenidos por medio de las técnicas previamente definidas estos tienen el objetivo de suplir las necesidades actuales de la Compañía, en cuanto a la seguridad informática, para el diseño de políticas según el estándar ISO 27001, es por lo que por medio de entrevistas con la Gerencia General y las jefaturas de los procesos involucrados así como la observación de cómo se realizan estos procesos se tendrá un panorama claro y conciso y así de esta manera aplicar lo indicado por la norma de la manera correcta y acorde con lo que la empresa necesita.

Se puede decir que el análisis de datos cualitativos: "[…]es un tipo de investigación que se centra en los pensamientos, comentarios y sentimientos de un individuo. (Navamuel, 2023. párr.1)."

Planteamiento de las entrevistas

Basado en la sesión virtual que se mantuvo con la gerencia general de Soluciones Seguras se indica que el proceso de interés para el desarrollo del objetivo de este proyecto es Servicio de Soporte Técnico a los clientes, una vez que esto quedó definido se procede a programar varias sesiones con la jefatura de este proceso para definir el alcance, en cuanto a cantidad y detalle de las políticas para su respectivo diseño.

Durante las sesiones que se tuvieron con la jefatura del proceso definido con anterioridad se define el alcance, el cual comprende seis políticas basándose en la necesidad que existe en el proceso para el diseño, a partir de la documentación respectiva, así como una sesión con la parte de recursos humanos, ya este departamento se ve involucrado dentro de los subprocesos que se tienen dentro del servicio de Soporte a los clientes.

Como parte de las preguntas realizadas en las sesiones se detalla lo siguiente, así como una breve justificación de estas:

A la parte gerencial se realizaron las siguientes preguntas.

1. ¿Dada la aprobación previa del proyecto, se tiene algún proceso según su criterio, para definirse para el diseño de las políticas? (Véase Anexo 3)

Con esta pregunta lo que se pretende es valorar y entender si la Compañía ya tiene uno o varios procesos en mira para que sean aplicados dentro del desarrollo de este proyecto.

2. ¿Con lo que comprende la parte de seguimiento es posible contar con el apoyo de alguien en la Compañía o encargado del proceso para afinar detalles, conocer más a fondo él o los procesos, así como revisión de la documentación? (Véase Anexo 3)

Con esto lo que se busca es poder tener una persona directa asociada al proceso, con el fin de obtener la información veraz y concisa para poder desarrollar este trabajo.

Durante las sesiones que se tuvieron con la jefatura de Soporte a los clientes se realizaron las siguientes preguntas:

1. ¿Dentro del servicio de soporte a los clientes cuáles podrían ser los subprocesos que dentro de la norma se pueden escoger para este trabajo? (Véase Anexo 4)

Lo que se busca es que una vez que quedó definido el proceso con la Gerencia el poder tener claro cuáles son los posibles subprocesos para incluir en el diseño de políticas.

2. ¿Cuál es la cantidad de políticas esperada o razonables por parte de la organización tomando en cuenta este proyecto? (Véase Anexo 4)

Con esta pregunta se quiere tener una claridad en lo esperado por la empresa, en cuanto a la cantidad de políticas y con esto poder tener un alcance definido para el logro de los objetivos de este trabajo.

3. ¿Existen políticas de seguridad documentadas para los subprocesos, previamente definidos? (Véase Anexo 5)

El enfoque de esta pregunta es obtener información en el caso de que exista documentación de políticas internas asociadas a los subprocesos escogidos para el desarrollo de este proyecto.

4. ¿Existe algún machote de política o documentación oficial donde se debe documentar los diseños de este trabajo? ¿En caso de no existir se puede crear? (Véase Anexo 2 y Anexo 5)

Es importante conocer si la empresa cuenta con un machote de documento de política interno para que sea de apoyo para los objetivos de este trabajo y en el caso de que no exista pues se toma como punto de mejora y se procede a crear un documento oficial para las políticas.

Y por último durante las sesiones con Recursos Humanos se describe a continuación:

1. ¿Se tiene actualmente una política para la selección de ingenieros para soporte a los clientes? (Véase Anexo 6)

Es importante como parte fundamental conocer si la empresa tiene documentación o una política como tal con lo que respecta a la selección del personal que se encuentra inmerso en el proceso definido.

2. ¿Existe alguna documentación o política asociada con las responsabilidades de los ingenieros durante la relación laboral? (Véase Anexo 6)

Para poder realizar este proyecto es importante conocer si existe documentación relacionada con las responsabilidades que tiene el personal que brinda el soporte técnico a los clientes para poder tomarlo en cuenta a la hora del diseño y documentación respectiva.

3. ¿Se cuenta con una política definida cuando se da el fin o el cambio en la relación laboral del personal del Departamento de Ingeniería? (Véase Anexo 6)

Esta pregunta tiene la finalidad de conocer y tener una claridad si existe documentación o política alguna, respecto del cambio o la finalización en la relación laboral del personal del departamento.

Análisis de las entrevistas

Una vez que se tuvieron varias sesiones con cada una de las partes involucradas con el fin de tener un panorama claro y definido de los alcances del proyecto es que con eso se procede con la interpretación de los resultados que se detallan a continuación en cada pregunta.

De la parte gerencial:

1. ¿Dada la aprobación previa del proyecto se tiene algún proceso, según su criterio para definirse para el diseño de las políticas?

Por medio de las conversaciones que se mantuvieron en las sesiones con la gerencia de la empresa, estos me expresan que existe la necesidad de diseñar políticas de seguridad para el proceso de soporte a los clientes, por lo que se toma en cuenta esto y se define como proceso crítico.

2. ¿Con lo que comprende la parte de seguimiento es posible contar con el apoyo de alguien la Compañía o encargado del proceso para afinar detalles, conocer más a fondo el o los procesos, así como revisión de la documentación?

Parte importante dentro de las sesiones con los gerentes de la organización fue el consultar y definir quién sería el contacto directo para obtener la información necesaria para la propuesta de este proyecto con el fin de que también esta misma persona delegada pudiera validar que el producto final cumpla con las expectativas y alcances definidos en los objetivos del trabajo, para este caso la persona que se definió fue la jefatura de Soporte Técnico.

Interpretación de las sesiones realizadas con la jefatura de Soporte a los clientes:

1. ¿Dentro del servicio de soporte a los clientes cuales podrían ser los subprocesos que dentro de la norma se pueden escoger para el trabajo?

Se realizan varias sesiones virtuales con la jefatura que tiene a cargo el servicio de soporte a los clientes, en donde se delimitan cual es el activo por proteger, en este caso la información, así como también se valida contra la norma ISO 27001:2013 apoyado en la ISO 27002 cuáles son las políticas y controles que se acoplan y se pueden enlistar, lo que nos conllevó a tener un profundo análisis, respecto del tema para poder definirlo de manera satisfactoria.

2. ¿Cuál es la cantidad de políticas esperada o razonables por parte de la organización tomando en cuenta este proyecto?

Parte primordial de este proyecto es poder definir la cantidad de políticas por diseñar para tener claro tanto el número total; así como el nombre de estas, con el fin de determinar el alcance claro de este trabajo, es por lo que durante las sesiones con la jefatura a cargo del proceso de soporte al cliente se plantea y se define que sean un total de seis políticas de la mano con la norma se detallan a continuación:

- Política de contraseñas
- Política de selección de candidatos para Ingeniería
- Política de responsabilidades de los ingenieros durante la relación laboral
- Política de cambio o finalización en la relación laboral.
- Política de continuidad del negocio para el proceso de soporte a los clientes.
- Política de capacitación del personal de Ingeniería.

Es importante mencionar que con esto hay tres políticas que dependen, directamente de recursos humanos por lo que además se indica que se debe programar una sesión con la encargada de este departamento para obtener la información necesaria para realizar y desarrollar este trabajo.

3. ¿Existen políticas de seguridad documentadas para los subprocesos, previamente definidos? (ver anexo 5)

En lo que respecta a las sesiones con la Jefatura de Soporte Técnico se realiza la consulta acerca de cuáles de las políticas definidas con anterioridad tienen o han tenido alguna documentación o política, respectivamente, con el fin de tener más información para el desarrollo del trabajo, con el detalle que solamente dos de las tres que corresponde a la jefatura tienen documentación estas son:

- Política de contraseñas
- Procedimiento de continuidad del negocio para el proceso de soporte a los clientes.

Documentación que sirve como material de apoyo en el caso de las dos que existen y con la que no, en este caso, se procede a crear de cero siempre a partir de la documentación oficial de la norma para que cumpla con lo establecido.

Con los otros tres procesos restantes se deben abarcar con la Jefatura del Departamento correspondiente, este es Recursos Humanos.

4. ¿Existe algún machote de política o documentación oficial donde se debe documentar los diseños de este trabajo? ¿En caso de no existir se puede crear?

En cuanto a un documento oficial para una política, según lo que indica el marco normativo indica el encargado del servicio de soporte que no existe a este momento por lo que se tiene plena libertad para crear la plantilla siempre y cuando esta cumpla con lo que rige la norma y sea aprobada por la gerencia.

De la sesión que se mantuvo con la Jefatura de Recursos humanos:

1. ¿Se tiene actualmente una política para la selección de ingenieros para soporte a los clientes?

Por medio de la entrevista realizada a la jefatura del departamento encargado en este caso de recursos humanos si existe documentación y manuales acerca de cómo es el puesto, requisitos, así como la manera en que se debe seleccionar a los candidatos, sin embargo, esta información no se encuentra contenido en una política basada en la normativa escogida para este proyecto por lo que esta información es de mucho provecho para el desarrollo y construcción del proyecto.

2. ¿Existe alguna documentación o política asociada con las responsabilidades de los ingenieros durante la relación laboral?

Con lo que respecta a la política de responsabilidades de los ingenieros durante la relación laboral según lo que nos menciona la persona a cargo no existe una documentación por parte de recursos humanos que defina las responsabilidades e implicaciones por incumplimiento durante la relación laboral del personal de soporte técnico por lo que en este caso con el apoyo de la norma se realizara la política respectiva.

3. ¿Se cuenta con una política definida cuando se da el fin o el cambio en la relación laboral del personal del Departamento de Ingeniería?

Conversando con la Jefatura de Recursos humanos me indican que existe un proceso que se debe seguir cuando se da el cambio o finalización en la relación laboral de un colaborador que pertenece al grupo de ingenieros de soporte técnico que consiste en quitar los accesos correspondientes a la persona de manera inmediata todo eso se hace por medio de tareas que genera una plataforma que tiene el departamento, mas sin embargo, no existe como tal una política que basada en una normativa internacional defina cuál debe ser el procedimiento para este subproceso, cabe mencionar que lo recabado servirá de apoyo para poder desarrollar la política.

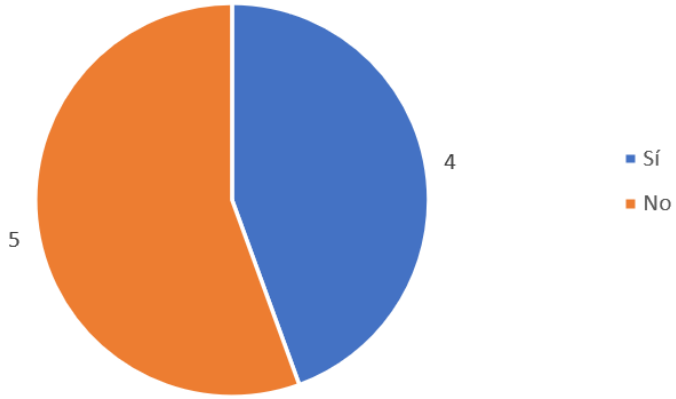
Análisis de la encuesta

Como segundo método utilizado para poder recopilar información y análisis de datos se realizó una encuesta la cual consiste en nueve preguntas combinadas acerca temas de las políticas mencionadas con anterioridad en donde solo se tomaron en cuenta las que tienen una política anterior definida o documentación relacionada con el subproceso. La encuesta cuenta con nueve preguntas y se realizó a las personas que se encuentran directamente relacionadas con los subprocesos que fueron electos para el diseño de política bajo la normativa ISO 27001. A continuación, se realizará la interpretación de resultados de la encuesta que consta de nueve preguntas y que se realizó a un total de nueve personas. Seguidamente se muestran las preguntas realizadas en su orden respectivo (véase anexo 1):

1. ¿Conoce con claridad la política de contraseñas de Soluciones Seguras?
2. ¿Cuál método utiliza para almacenar sus contraseñas?
3. ¿Cómo crea usualmente sus contraseñas?
4. ¿Con qué frecuencia realiza el cambio de sus contraseñas?
5. ¿Qué longitud utiliza usualmente en sus contraseñas?
6. ¿Conoce lo que es una política de continuidad del negocio?
7. ¿Ha participado dentro de Soluciones Seguras en una prueba de continuidad del negocio?
8. ¿Tiene conocimiento de cuáles son los requisitos y obligaciones del puesto que actualmente desempeña?
9. ¿Conoce usted cuáles son los requisitos para ser elegible para un ascenso?

Figura 1

Conocimiento de política interna de contraseñas.



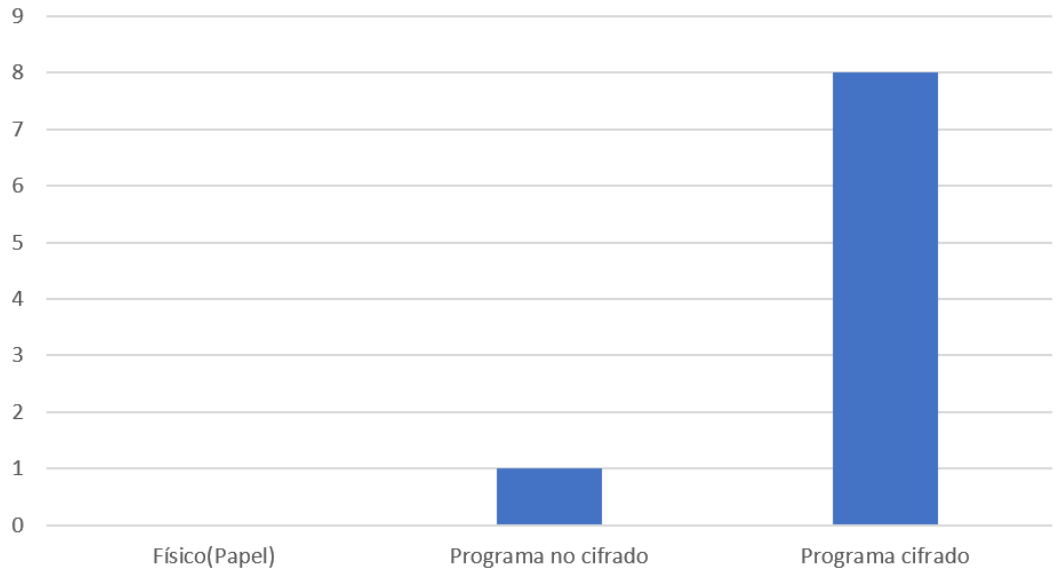
En cuanto a la primera pregunta la misma consistía en "¿Conoce con claridad la política de contraseñas de Soluciones Seguras?", los resultados obtenidos muestran una división entre los participantes. Cuatro de ellos indicaron tener un conocimiento claro sobre esta política, mientras que cinco mencionaron no estar familiarizados con ella.

Estos resultados reflejan una falta de conocimiento o información precisa, respecto de la política de contraseñas de Soluciones Seguras. Aunque una parte de los encuestados parece estar al tanto de esta política y se encuentra informada al respecto, es evidente que la mayoría no se encuentra informada.

Es importante destacar que el conocimiento claro de una política de contraseñas es esencial para garantizar la seguridad en el ámbito digital. Las políticas de contraseñas bien definidas y comunicadas pueden proteger la información confidencial y prevenir el acceso no autorizado a sistemas y datos.

Figura 2

Métodos de almacenamiento de contraseñas



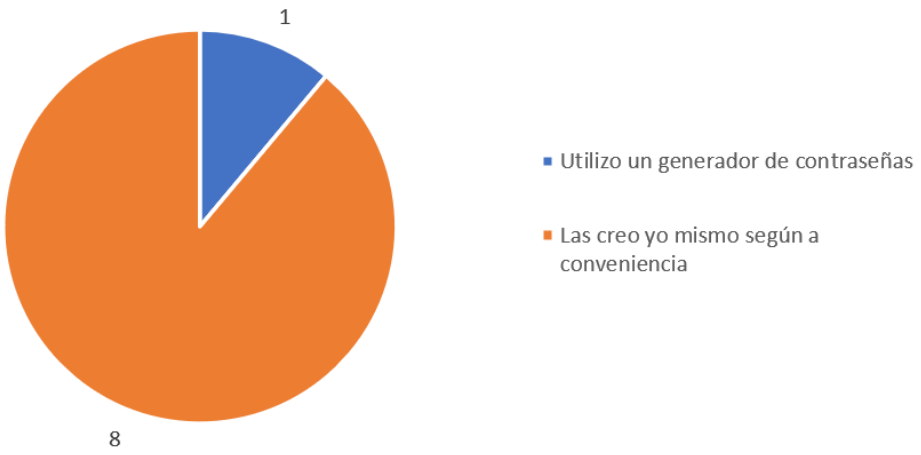
Según los resultados obtenidos de la segunda pregunta "¿Qué método utiliza para almacenar sus contraseñas?", se puede observar que la mayoría de las personas encuestadas, un total de ocho, optan por utilizar un programa cifrado para almacenar sus contraseñas. Esto implica que utilizan una aplicación o software específico diseñado para proteger y cifrar sus contraseñas, lo que proporciona una capa adicional de seguridad para sus datos confidenciales.

Desde otro punto, una única persona indicó que utiliza un programa no cifrado para almacenar sus contraseñas. Esto indica que esta persona utiliza una herramienta de almacenamiento, como un administrador de contraseñas, pero sin el nivel adicional de cifrado para proteger los datos almacenados. Esto se convierte un riesgo para la seguridad, ya que las contraseñas están más expuestas a posibles ataques o accesos no autorizados.

Es interesante destacar que ninguna de las personas encuestadas mencionó almacenar sus contraseñas en papel. Esto refleja una tendencia acerca de que el método tradicional de anotar las contraseñas en papel está siendo desplazado por opciones digitales más seguras y convenientes.

Figura 3

Métodos utilizados para la creación de contraseñas



Al analizar los resultados de la tercera pregunta sobre cómo las personas suelen crear sus contraseñas, se puede observar que, del total de las respuestas recibidas, el 89% de los encuestados (ocho de nueve) indicaron que crean sus contraseñas por sí mismos, según su conveniencia. Desde otra arista, solo el 11% (uno de nueve) mencionó utilizar un generador de contraseñas.

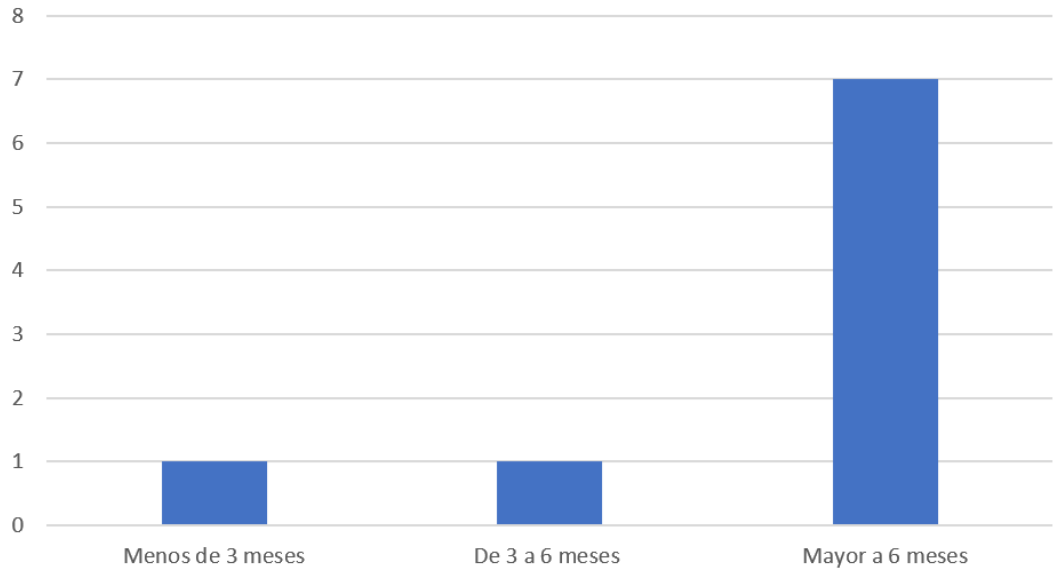
La mayoría de los encuestados prefieren tomar el control y diseñar sus propias contraseñas. Esto se asocia debido a la familiaridad con el proceso y la facilidad de recordar contraseñas personalizadas. Sin embargo, es importante destacar que esta práctica no es recomendable, ya que las contraseñas creadas por los usuarios tienden a ser más débiles y predecibles, lo que los puntos vulnerables a ataques de fuerza bruta o que las mismas sean adivinadas con mayor facilidad.

También, un número significativamente menor de encuestados opta por utilizar un generador de contraseñas[1]. Esto se debe a la conciencia sobre la importancia de contar con contraseñas fuertes y aleatorias para proteger las cuentas y los datos personales.

[1]Los generadores de contraseñas son herramientas que generan combinaciones de caracteres complejas y difíciles de adivinar, lo que mejora la seguridad de las contraseñas.

Figura 4

Frecuencia en la que los usuarios cambian las contraseñas



El análisis de los resultados de la cuarta pregunta sobre "¿Con qué frecuencia realiza el cambio de sus contraseñas?" se puede notar que, de un total de nueve respuestas, la mayoría, es decir, siete personas, indicaron que realizan el cambio de sus contraseñas con una frecuencia mayor a seis meses. Esto muestra que estas personas tienden a tener sus contraseñas sin cambios durante períodos prolongados.

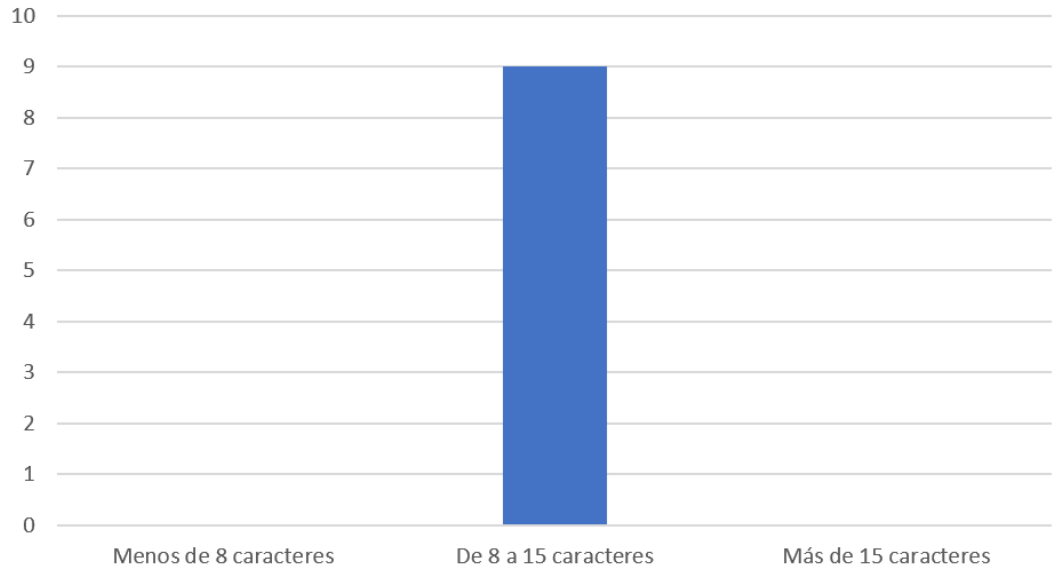
Por otra parte, solamente una persona mencionó que cambia sus contraseñas con una frecuencia menor a tres meses, lo cual indica una actitud proactiva, en cuanto a la seguridad de sus cuentas y datos personales. Esta persona entiende la importancia de mantener contraseñas actualizadas y busca reducir los riesgos asociados con la exposición prolongada de una misma contraseña.

Además, solamente una persona afirmó que cambia sus contraseñas en un intervalo de tiempo comprendido entre tres y seis meses. Esto indica una postura intermedia entre los dos grupos anteriores, demostrando una conciencia moderada sobre la necesidad de cambiar las contraseñas, regularmente.

En general, estos resultados indican que la mayoría de las personas encuestadas no cambian sus contraseñas con la frecuencia recomendada por expertos en seguridad informática, lo que genera una exposición a un mayor riesgo de ser víctimas de ataques cibernéticos. Sin embargo, sí existe la presencia de algunas personas que sí mantienen un pensar proactivo en la protección de sus cuentas y además muestran una comprensión de la importancia de mantener contraseñas actualizadas y seguras.

Figura 5

Cantidad de caracteres utilizada por los usuarios en la creación de contraseñas



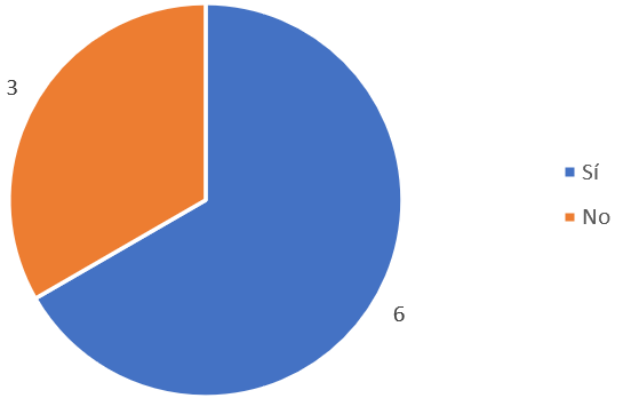
Al analizar los resultados obtenidos de la pregunta número cinco "¿Qué longitud utiliza usualmente para sus contraseñas?", se observa que la mayoría de los encuestados, específicamente el 100% de ellos, indicaron que utilizan contraseñas con una longitud que varía entre ocho y quince caracteres, además no se registraron respuestas que indicaran utilizar contraseñas con menos de ocho caracteres ni con más de quince caracteres.

Estos resultados muestran en que la mayoría de las personas encuestadas tiene preferencia por establecer contraseñas que se consideran de longitud moderada. Es importante destacar que la elección de una contraseña segura y robusta es fundamental para proteger la información personal

y evitar posibles ataques cibernéticos. Utilizar una combinación de caracteres alfanuméricos, incluyendo letras mayúsculas y minúsculas, números y símbolos, puede contribuir a fortalecer la seguridad de las contraseñas.

Figura 6

Conocimiento de los usuarios de una política continuidad del negocio



Al analizar los resultados de la sexta pregunta "¿Conoce lo que es una política de continuidad del negocio?", se observa que, de las nueve respuestas obtenidas, seis participantes indicaron tener conocimiento sobre el tema, mientras que tres manifestaron no estar familiarizados con esta política.

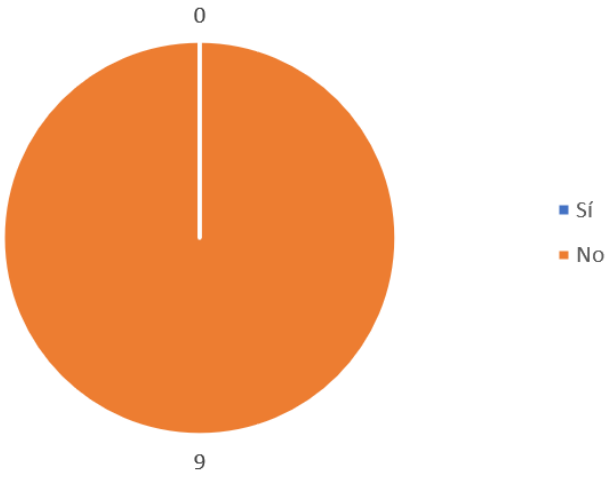
Estos resultados muestran que la mayoría de los encuestados poseen un nivel de comprensión sobre la política de continuidad del negocio, además también es importante mencionar que se observa que más de la mitad de los participantes están familiarizados con esta política, lo que muestra que existe cierto grado de conocimiento y conciencia en el grupo encuestado.

Sin embargo, es importante destacar que un pequeño porcentaje de los encuestados (tres de nueve) indicaron no tener conocimiento acerca de la política de continuidad del negocio.

Esto se atribuye directamente a diversas razones, como falta de exposición previa al concepto o falta de información sobre la importancia y relevancia de la política de continuidad del negocio.

Figura 7

Participación de usuarios en una prueba de continuidad del negocio en la compañía.



Al analizar los resultados de la pregunta siete "¿Ha participado dentro de Soluciones Seguras en una prueba de continuidad del negocio?", se puede observar que, de las nueve respuestas obtenidas, todas indicaron que no han participado en una prueba de continuidad del negocio dentro de Soluciones Seguras.

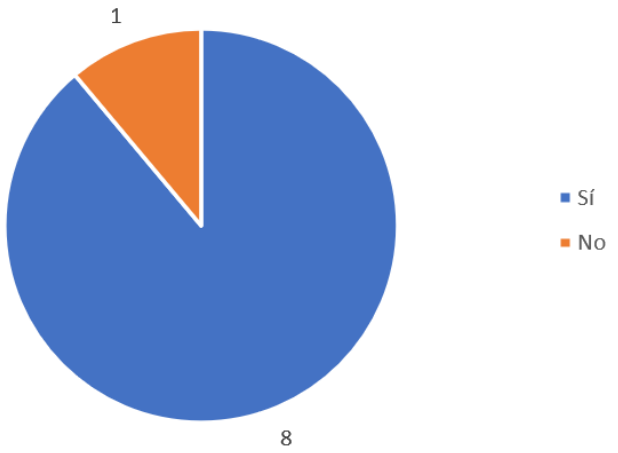
Estos resultados revelan que ninguno de los encuestados ha tenido la oportunidad de participar en una prueba de continuidad del negocio en el contexto de Soluciones Seguras. Esto se puede asociar a causa de varias razones, como la falta de implementación de pruebas regulares de continuidad del negocio en la organización o a la falta de participación de los encuestados en las pruebas existentes.

Es importante destacar que la realización de pruebas de continuidad del negocio es fundamental para evaluar la efectividad y la preparación de una organización ante posibles

desastres o interrupciones del servicio. Estas pruebas permiten identificar áreas de mejora, corregir posibles deficiencias y fortalecer la capacidad de respuesta ante situaciones de crisis.

Figura 8

Conocimiento de los usuarios de los requisitos y obligaciones del puesto que ejercen.



Continuando con el análisis de los resultados de la octava pregunta "¿Tiene conocimiento de cuáles son los requisitos y obligaciones del puesto que actualmente desempeña?", se puede ver que, de las nueve respuestas obtenidas, ocho participantes indicaron tener conocimiento de los requisitos y obligaciones de su puesto actual, mientras que uno manifestó no tener ese conocimiento.

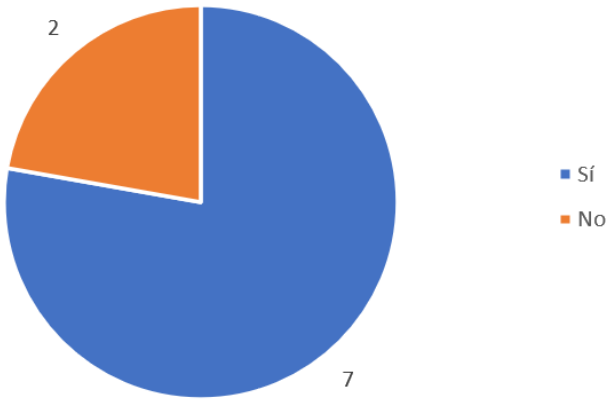
Estos resultados revelan que la mayoría de los encuestados están enterados con los requisitos y las obligaciones asociadas a sus respectivos puestos de trabajo. Esto es una buena señal, ya que indica que la mayoría de los empleados tienen claridad, respecto de sus responsabilidades y las habilidades necesarias para desempeñar su trabajo de manera efectiva.

Sin embargo, es importante tomar en cuenta que un pequeño porcentaje de los encuestados (uno de nueve) indicaron no tener conocimiento de los requisitos y obligaciones de su puesto actual. Esto debido a múltiples razones, como una comunicación inadecuada por parte de la

empresa, en cuanto a las expectativas del puesto o una falta de claridad en los roles y responsabilidades del empleado.

Figura 9

Entendimiento por parte de los usuarios de los requisitos para un ascenso laboral dentro de la empresa.



Por último, los resultados de la novena pregunta "¿Conoce usted cuáles son los requisitos para ser elegible para un ascenso?", se observa que, de las nueve respuestas obtenidas, siete de los participantes indicaron tener conocimiento de los requisitos necesarios para ser considerados elegibles para un ascenso, mientras que dos no manifestaron no estar al tanto de esos requisitos.

Estos resultados revelan que la mayoría de los encuestados están familiarizados con los requisitos que se deben cumplir para ser considerados para un ascenso dentro de la organización. Esta comprensión es un indicador positivo, ya que demuestra que la mayoría de los empleados tienen conocimiento sobre los criterios y las competencias necesarias para avanzar en su carrera profesional.

Sin embargo, es importante tener en cuenta que un pequeño porcentaje de los encuestados (dos de nueve) indicaron no estar al tanto de los requisitos para un ascenso. Esto se debe a causa

de varias razones, como la falta de comunicación clara por parte de la empresa sobre los criterios de promoción o una falta de claridad en cuanto a las oportunidades de crecimiento profesional.

En conclusión, aplicadas las encuestas y entrevistas a las partes interesadas y que se vieron, directamente involucradas en la realización de este trabajo se obtiene información y datos relevantes e importantes, que a su vez, respaldan la necesidad de la Compañía de poseer un diseño de políticas de seguridad para estos subprocesos que se encuentran dentro del procesos de soporte a los clientes , además que toda esta información recopilada es un apoyo y de provecho para el siguiente capítulo en donde se elaborará el diseño y documentación de las políticas de seguridad.

Capítulo 5. Propuesta de Solución

En este capítulo, se propone un diseño de políticas y mejores prácticas basadas en el marco de referencia ISO 27001 que define los requisitos para implementar, mantener y mejorar un sistema de gestión de seguridad de la información en una empresa y, a su vez, brinda un marco de referencia para la gestión de la seguridad de la información, con políticas, procedimientos y mejores prácticas que serán la base fundamental en el diseño y mejora de la seguridad de la información en el Departamento de Tecnología de la Empresa Soluciones Seguras.

La seguridad de la información es un aspecto fundamental, hoy, en el entorno empresarial sumado al diseño y documentación de un conjunto sólido de políticas y mejores prácticas hacen que se genere una garantía en la protección de los activos de información y, a su vez, se reduzcan los riesgos asociados a posibles amenazas y vulnerabilidades que presente la empresa.

Es importante que toda organización cuente con políticas que se basen en una normativa de seguridad internacional como lo es la ISO 27001, ya que los ciberdelincuentes, constantemente se encuentran tratando de encontrar la manera para atacar las organizaciones y provocar daños esto se observa en el nivel de la región, según los datos que menciona el medio digital, *El País* (2022):

> Costa Rica sufrió 513 millones de intentos de intrusión, un aumento del 104% en comparación con el mismo periodo de 2021 (con 251 millones). México el país más atacado de la región (con 85 mil millones), seguido por Brasil (con 31,5 mil millones) y Colombia (con 6,3 mil millones). (párr. 2).

Estos datos son muy alarmantes y reflejan aún más la necesidad de que las organizaciones hoy deben invertir en soluciones y normativas de seguridad de la información con el fin de fortalecer la seguridad y tratar de evitar ser vulneradas por los ciberdelincuentes.

La norma ISO 27001 es aplicable a cualquier tipo de organización, ya sea pequeña, mediana o grande, del sector público o privado. El estándar establece un conjunto de controles y mejores prácticas que las organizaciones deben implementar para administrar de manera efectiva los riesgos de seguridad de la información que enfrentan, además es importante mencionar que la misma es certificable, y a su vez trabaja de la mano con la ISO 27002 que garantiza la seguridad de la información, sin embargo, importante considerar que esta segunda no es certificable.

Desde otro punto, la ISO 27002 proporciona directrices y recomendaciones para el establecimiento, implementación, mantenimiento y mejora de los controles de seguridad de la información dentro del contexto del Sistema de Gestión de Seguridad de la Información definido por la norma ISO 27001. En otras palabras, la ISO 27002 detalla los controles específicos que una organización debe implementar para cumplir con los requisitos de seguridad de la información establecidos en la ISO 27001.

La elección del proceso crítico definido para este proyecto se basó en las necesidades de la empresa como parte fundamental, así como también el análisis obtenido de las entrevistas realizadas a la Gerencia General de Soluciones Seguras, este proceso tiene como nombre servicio de soporte a los clientes y dentro de este proceso se seleccionaron basados en los mismos criterios seis subprocesos a los cuales se les aplicó el diseño y documentación de políticas, además el resultado de este trabajo será tomado en cuenta como base para el proceso de certificación de la norma ISO 27001 a futuro que tiene planeado la organización.

En cuanto a los subprocesos contenidos dentro del proceso definido de Soporte a los clientes, sumado al análisis de los resultados obtenidos de las entrevistas y encuestas, basado en las necesidades indicadas por la organización, es que se concluyen los seis subprocesos a los cuales

se les estará aplicando el diseño y documentación respectivo de políticas de seguridad, mismas que se desarrollarán y explicarán a lo largo de este capítulo y que se mencionan a continuación:

1. Política de contraseñas
2. Política de selección de candidatos para Ingeniería
3. Política de responsabilidades de los ingenieros durante la relación laboral
4. Política de cambio o finalización en la relación laboral.
5. Política de continuidad del negocio para el proceso de soporte a los clientes.
6. Política de capacitación del personal de ingeniería en las herramientas de uso diario.

En lo que respecta a la norma, sumado a la necesidad de la organización y el análisis de los resultados obtenidos, se identifican los apartados dentro de la norma y los respectivos controles que se deben cumplir en el diseño y documentación respectiva de las políticas para cada subproceso seleccionado, estos apartados y controles serán detallados a lo largo de este capítulo y son los siguientes:

- A5 Políticas de seguridad de la información.
- A7 Seguridad relativa a los recursos.
- A17 Aspectos de seguridad de la información en la gestión de continuidad del negocio.

A5 Políticas de seguridad de la información

Esta sección establece directrices para desarrollar y mantener políticas de seguridad de la información en una organización. Estas políticas son fundamentales para establecer un marco de referencia claro y coherente en materia de seguridad de la información y para comunicar las expectativas de la organización en relación con la protección de la información.

Respecto del ámbito correspondiente a Soluciones Seguras dentro de este apartado de la normativa para el proceso de Soporte a los clientes se escogió el subproceso de uso correcto y creación de contraseña en donde se definieron todos los lineamientos para creación, cambio y bloqueo de credenciales, así como también los sistemas involucrados en el alcance de la política.

Basados en las encuestas se observó que a pesar de que existía documentación de la organización relacionada al correcto uso de las contraseñas la mayoría de los encuestados no tenía claridad de esto, por lo que denota claramente una necesidad por cubrir en cuanto a este tema se refiere, tomando en cuenta esto, en breve se detalla la documentación respectiva de la política con sus apartados correspondientes.

Política de uso correcto y creación de contraseñas

Objetivo

El objetivo de esta política es establecer lineamientos claros y seguros para la creación, gestión y protección de contraseñas utilizadas en los sistemas y servicios de la organización. Esta política busca garantizar la confidencialidad, integridad y disponibilidad de la información, para minimizar el riesgo de acceso no autorizado y el uso indebido de los recursos.

Alcance

Esta política se aplica a todos los ingenieros, jefaturas y cualquier otra persona que tenga acceso a los sistemas y servicios involucrados en el proceso de Soporte a los clientes. También se aplica a todos los dispositivos y aplicaciones utilizados para el almacenamiento, procesamiento y transmisión de datos.

Los sistemas involucrados son:

- Kayako
- Checkpoint VPN

- Checkpoint Infinity Portal
- Checkpoint User Center
- Customers Force CyberArk
- Privileged Cloud Cyberark
- Aplicaciones de Microsoft 365
- Microsoft Active Directory
- Radware CloudWAF

Responsables

La dirección de la organización es responsable de respaldar y hacer cumplir esta política.

Los empleados que se encuentran dentro del proceso de soporte a los clientes son responsables de crear y mantener contraseñas seguras, así como de cumplir con las directrices establecidas.

Lineamientos

Longitud y complejidad de contraseñas

Las contraseñas deben tener una longitud mínima de ocho y máxima de 15 caracteres.

Las contraseñas deben contener una combinación de al menos tres de los siguientes elementos:

- Letras mayúsculas (A-Z)
- Letras minúsculas (a-z)
- Números (0-9)
- Caracteres especiales (!@#$%^&*()-_=+[]{}|;:,.<>?)

Se recomienda el uso de frases o secuencias de palabras que sean fáciles de recordar para el usuario, pero difíciles de adivinar para otros.

Cambio y renovación de contraseñas

Se requiere que los usuarios cambien sus contraseñas cada 90 días.

Las contraseñas no deben reutilizarse antes de al menos cinco cambios consecutivos.

Las contraseñas deben cambiarse inmediatamente si se sospecha que han sido comprometidas o si se ha producido una violación de seguridad.

Bloqueo de contraseñas

Se realizará el bloqueo de manera automática al usuario que realice 5 intentos inicio de sesión fallidos por lo que la persona deberá enviar un correo al personal encargado de la contraseña para el desbloqueo pertinente o cambio de credenciales en caso de que olvidaran de las mismas, además dicha solicitud debe ser verificada de manera telefónica corroborando la identidad del solicitante y así evitar un posible caso de suplantación de identidad o cualquier actividad fraudulenta.

Prohibición de contraseñas predeterminadas

Se prohíbe el uso de contraseñas predeterminadas o genéricas proporcionadas por los sistemas o aplicaciones.

Las contraseñas deben ser únicas y no deben ser compartidas entre usuarios.

Autenticación Multifactor

Se promueve el uso de la autenticación multifactor (MFA) siempre que sea posible.

Se requiere la configuración de MFA para todos los sistemas y aplicaciones que lo admitan.

Protección de contraseñas almacenadas

Las contraseñas deben almacenarse de forma segura utilizando técnicas de cifrado robustas.

Se prohíbe el almacenamiento en texto plano o cualquier forma que permita una fácil recuperación de las contraseñas.

Las contraseñas no deben enviarse por correo electrónico, mensajes instantáneos u otros medios de comunicación no seguros.

Educación y concientización

Se proporcionará capacitación y concienciación cada cuatro meses a los usuarios, acerca de la importancia de las contraseñas seguras, la protección de la información y las mejores prácticas de seguridad.

Los usuarios deben ser conscientes de los riesgos asociados con el uso de contraseñas débiles y de la necesidad de cumplir con esta política

Cumplimiento

Se llevará a cabo una supervisión regular para garantizar el cumplimiento de esta política.

Se aplicarán sanciones disciplinarias en caso de incumplimiento intencional o negligente de esta política.

Esta política será aprobada y modificada en caso de que se requiera por la gerencia y estará disponible en todo momento para todos los empleados, a través del sitio web interno, el cual es el medio de comunicación oficial del Departamento de Recursos Humanos.

Control de cambios

Se debe documentar todo cambio, modificación y aprobación que se realice a esta política con el fin de llevar un control riguroso y ordenado.

En resumen, esta política comprende los lineamientos y directrices que se apegan a la normativa en donde fueron utilizadas todas las mejores prácticas y recomendaciones de la norma con su respectivo acomodo y redacción según el contexto de Soluciones Seguras, que además es

importante mencionar que esta también se encuentra diseñada y documentada en el formato interno de la Compañía.

A7 Seguridad relativa a los recursos

La normativa ISO 27001 apoyada en los controles que se mencionan en la ISO27002 contiene un apartado que regula el recurso humano y que consiste en establecer medidas de seguridad para garantizar la adecuada gestión de los recursos humanos en relación con la seguridad de la información. Este apartado reconoce que los empleados de la Compañía pueden representar una amenaza potencial para la seguridad de la información, ya sea con o sin intención.

La seguridad orientada a los recursos humanos según la normativa comprende varios aspectos los cuales se estarán abarcando durante esta propuesta, aspectos que detallan como debe realizarse la selección de personal, así como cuales son las responsabilidades de los empleados durante la relación laboral, otro punto importante dentro de este apartado es como se debe realizar el cambio o finalización de la relación por parte de la organización, todo esto debidamente apegado y redactado según el contexto de la organización y por último se tiene dentro de este aspecto el apartado, los lineamientos para las capacitaciones de los empleados en las herramientas de uso diario.

Además, es importante mencionar que la elección de los subprocesos se da con base en las necesidades de la organización, pero también respaldado en los resultados de las entrevistas , así como las encuestas realizadas en las que ,específicamente, dos preguntas se basaron en la documentación existente sobre los lineamientos para cambios o ascensos en la relación laboral así como el conocimiento de las labores que el puesto que los empleados del proceso de Soporte a los clientes refiere, es por esto que el diseño y documentación de las políticas definidas crean una

mejora considerable en los procesos, a continuación, se detallará cada una de las políticas, que son un total de cuatro.

Política de selección del personal

Objetivo

El objetivo de esta política es establecer un proceso de selección de personal que garantice la contratación de individuos competentes y confiables, que cumplan con los requisitos de seguridad de la información de la organización, que minimice los riesgos de seguridad y que se proteja la confidencialidad, integridad y disponibilidad de los activos de información.

Alcance

Esta política se aplica a todos los procesos de selección y contratación de personal, ya sea que se trate de empleados permanentes, temporales u otros colaboradores, que tengan acceso a los activos de información de la organización.

Responsables

El Departamento de Recursos Humanos será responsable de implementar y gestionar el proceso de selección de personal de acuerdo con esta política, garantizando la identificación y evaluación adecuada de los candidatos en términos de competencia y confiabilidad.

El Gerente Técnico de la Compañía participará en el proceso de selección de personal, proporcionando orientación y evaluando los requisitos de seguridad de la información en el perfil de los candidatos.

Lineamientos para el proceso de selección de personal:

Definición de perfil de puesto

Antes de iniciar el proceso de selección, se elaborará un perfil de puesto que incluya los requisitos técnicos y de seguridad de la información necesarios para el puesto.

Anuncio de vacante

Las vacantes se anunciarán de manera clara y precisa, se deben indicar los requisitos del perfil de puesto, incluyendo los aspectos relacionados con la seguridad de la información.

Solicitud y evaluación de candidatos

Se establecerán procedimientos para la solicitud y recepción de currículos, así como para la evaluación de los candidatos en función de los requisitos del perfil de puesto, incluyendo la verificación de antecedentes laborales y referencias.

Entrevistas y Evaluaciones

Se llevarán a cabo entrevistas y evaluaciones técnicas y de seguridad de la información para evaluar las habilidades y competencias de los candidatos, así como su conciencia y compromiso con la seguridad de la información.

Verificación de antecedentes

Se realizará una verificación exhaustiva de los antecedentes de los candidatos, incluyendo antecedentes penales, educativos y laborales, según lo permitido por la legislación aplicable de Costa Rica.

Cumplimiento legal

Se deben cumplir todas las leyes y regulaciones aplicables en el proceso de selección de personal, incluyendo la protección de datos personales según el país.

Toma de decisiones

La selección final se realizará con base en la evaluación integral de los candidatos, considerando tanto sus competencias técnicas como su idoneidad para cumplir con los requisitos de seguridad de la información.

Capacitación e Inducción

Una vez contratado, se proporcionará a los empleados una capacitación inicial en seguridad de la información, con el fin de crear conciencia sobre las políticas y procedimientos de seguridad de la información de la organización, así como también se impartirá la inducción respectiva con el fin de integrar a la persona contratada en los procedimientos y políticas de la organización.

Confidencialidad y Acuerdo de no divulgación

Los empleados deberán firmar un acuerdo de confidencialidad y no divulgación, comprometiéndose a mantener la confidencialidad de la información de la organización durante y después de su empleo.

Cumplimiento

Se llevará a cabo una supervisión regular para garantizar el cumplimiento de esta política.

Se aplicarán sanciones disciplinarias en caso de incumplimiento intencional o negligente de esta política.

Esta política será revisada, periódicamente por el gerente técnico para garantizar su vigencia y eficacia.

Los cambios y actualizaciones serán comunicados a todos los usuarios relevantes.

Control de cambios

Se debe documentar todo cambio, modificación y aprobación que se realice a esta política con el fin de llevar un control riguroso y ordenado.

Política de responsabilidades durante la relación laboral

Objetivo

El objetivo de esta política es establecer las responsabilidades de los empleados durante la relación laboral, respecto de la seguridad de la información, a fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información, así como prevenir cualquier uso inadecuado, divulgación no autorizada o pérdida de información, de acuerdo con los requisitos establecidos en la norma ISO 27001.

Alcance

Esta política se aplica a todos los empleados de la organización, incluidos los empleados a tiempo completo, a tiempo parcial, temporales, que tengan acceso a los recursos y activos de información de la organización.

Responsables

Gerencia

La Gerencia es responsable de establecer y mantener un entorno de trabajo seguro y de promover una cultura de seguridad de la información. Debe asignar los recursos necesarios para implementar y mantener los controles de seguridad de acuerdo con los requisitos de ISO 27001 y revisar, periódicamente la efectividad de la política.

Recursos Humanos

Recursos Humanos debe asegurar que todos los empleados sean conscientes de esta política y proporcionarles la capacitación necesaria en seguridad de la información. También debe asegurarse de que se implementen y mantengan los controles de seguridad correspondientes y de que se realicen las evaluaciones de riesgos periódicas.

Empleados

Todos los empleados deben cumplir con las políticas y procedimientos de seguridad de la información establecidos por la organización. Deben proteger la información confidencial a la que tengan acceso durante su empleo y reportar cualquier incidente de seguridad de manera oportuna a las autoridades correspondientes.

Lineamientos

Uso adecuado de los recursos de información

Los empleados deben utilizar los recursos de información de la organización, únicamente para fines autorizados y de acuerdo con las políticas y procedimientos establecidos. No deben divulgar, compartir o utilizar la información de manera inapropiada o no autorizada.

Acceso y control de la información

Los empleados deben proteger la confidencialidad, integridad y disponibilidad de la información a la que tengan acceso durante su empleo es por lo que como parte de la política de selección de personal los empleados deben firmar un acuerdo de confidencialidad. Deben utilizar contraseñas seguras, no compartir sus credenciales de acceso y utilizar los mecanismos de autenticación establecidos.

Cumplimiento legal y normativo

Los empleados deben cumplir con todas las leyes, regulaciones y normativas aplicables en materia de seguridad de la información durante la relación laboral. Los empleados deben respetar los derechos de autor, las licencias de software y proteger la propiedad intelectual de la organización y de terceros.

Protección contra malware y amenazas:

Los empleados deben utilizar el software que brinda Soluciones Seguras el cual se encuentra debidamente licenciado y controlado esto en los dispositivos de trabajo y evitar la

descarga o instalación de software no autorizado o proveniente de fuentes no confiables. También deben estar atentos a los posibles ataques de malware y reportar cualquier incidente a las autoridades competentes.

Uso seguro del correo electrónico y la internet:

Los empleados deben utilizar el correo electrónico institucional y la conectividad a internet de manera responsable y segura. No deben abrir archivos adjuntos o enlaces sospechosos, ni divulgar información confidencial a través de estos medios sin la debida autorización, así como reportar cualquier comportamiento anómalo o sospecha que se dé por medio del correo electrónico y el uso del internet.

Cumplimiento y consecuencias

El incumplimiento de esta política puede dar lugar a acciones disciplinarias, que pueden incluir sanciones, hasta la terminación de la relación laboral o contractual. La organización se reserva el derecho de tomar las medidas legales correspondientes en caso de incumplimiento grave que ponga en riesgo la seguridad de la información.

Esta política de responsabilidades durante la relación laboral se implementará y comunicará a todos los empleados y proveedores relevantes. Será revisada periódicamente para asegurar su idoneidad y se actualizará según sea necesario para reflejar los cambios en los requisitos legales que sean aplicables y las mejores prácticas de seguridad de la información, además que estará disponible en todo momento para todos los empleados, a través del sitio web interno el cual es el medio de comunicación oficial del Departamento de Recursos Humanos.

Control de cambios

Se debe documentar todo cambio, modificación y aprobación que se realice a esta política con el fin de llevar un control riguroso y ordenado.

Política de cambio o finalización en la relación laboral

Objetivo

El objetivo de esta política es establecer directrices y procedimientos para garantizar la finalización o cambio adecuado de la relación laboral de los empleados en el contexto de la seguridad de la información, conforme con los requisitos de la norma ISO 27001.

Alcance

Esta política se aplica a todos los empleados que tengan acceso a los activos de información de la organización y cuya relación laboral llegue a su fin o sea modificada.

Responsables

La alta dirección es responsable de garantizar que se establezcan y mantengan los procedimientos adecuados para la finalización o cambio en la relación laboral de los empleados.

El Departamento de Recursos Humanos será responsable de coordinar los procesos de finalización o cambio en la relación laboral de los empleados, además, deberá notificar a los responsables de seguridad de la información, acerca de la finalización o cambio de empleo de un empleado y tomar las medidas necesarias para proteger los activos de información de la organización.

El Gerente de la Compañía será responsable de asegurar que se implementen los controles necesarios para proteger los activos de información durante la finalización o cambio de la relación laboral de un empleado, así como trabajar de la mano con Recursos Humanos para garantizar que se sigan los procedimientos establecidos y se realicen las acciones adecuadas para proteger la información.

Lineamientos en caso de terminación de la relación laboral

Proceso de finalización

Antes de la finalización de la relación laboral de un empleado, se debe llevar a cabo una revisión exhaustiva de los privilegios y accesos del empleado a los activos de información.

El Departamento de Recursos Humanos debe notificar al Departamento de Seguridad de la Información con suficiente antelación, respecto de la finalización de la relación laboral.

El Departamento de Seguridad de la Información debe coordinar con el Departamento de Recursos Humanos para realizar una terminación controlada de los accesos físicos y lógicos del empleado.

Se deben revocar o modificar los privilegios de acceso a los sistemas y activos de información de acuerdo con los procedimientos establecidos.

Devolución de activos

El empleado que finaliza su relación laboral debe devolver todos los activos de información en su posesión, lo que incluye: tarjetas de acceso, dispositivos móviles, laptops, llaves USB, entre otros.

Se deben realizar inventarios periódicos de los activos de información asignados a los empleados para asegurar su devolución.

Comunicación de la finalización

El Departamento de Seguridad de la Información debe comunicar a los equipos relevantes, acerca de la finalización de la relación laboral y la revocación de los privilegios de acceso del empleado.

La comunicación debe incluir información, respecto de cualquier restricción o medida de seguridad adicional que se deba tomar en cuenta.

Lineamientos en caso de cambio en la relación laboral

Proceso de cambio

En caso de cambio en la relación laboral de un empleado, como una transferencia a otro departamento o cambio de responsabilidades, se deben realizar evaluaciones de seguridad de la información apropiadas.

El Departamento de Seguridad de la Información debe garantizar que los cambios en los roles o responsabilidades no comprometan la seguridad de la información

Retiro de privilegios

Si el cambio en la relación laboral implica un cambio en los privilegios de acceso, el Departamento de Seguridad de la Información debe modificar o revocar los privilegios de acceso en consecuencia.

Cumplimiento

La finalización o cambio en la relación laboral debe cumplir con todas las leyes y regulaciones laborales aplicables, así como con cualquier cláusula contractual relevante.

La organización brindará de manera trimestral capacitación y conciencia adecuadas a todos los empleados, acerca de los procedimientos de finalización o cambio en la relación laboral y las implicaciones de seguridad de la información asociadas.

Esta política será aprobada y modificada en caso de que se requiera por la gerencia y estará disponible en todo momento para todos los empleados, a través del sitio web interno, el cual es el medio de comunicación oficial del Departamento de Recursos Humanos.

Control de cambios

Se debe documentar todo cambio, modificación y aprobación que se realice a esta política con el fin de llevar un control riguroso y ordenado.

Política de capacitación del personal en herramientas de uso diario

Objetivo

El objetivo de esta política es establecer un marco de capacitación en herramientas de uso diario para todos los empleados, con el fin de garantizar la seguridad de la información y el cumplimiento de los requisitos establecidos en la norma ISO 27001.

Alcance

Esta política se aplica a todos los empleados de la organización que tengan contacto con la información de la empresa.

Responsables

Gerencia

Establecer un programa de capacitación en herramientas de uso diario que cumpla con los requisitos de la norma ISO 27001.

Asignar los recursos necesarios para implementar y mantener el programa de capacitación.

Supervisar y evaluar regularmente la efectividad del programa de capacitación.

Recursos Humanos

Colaborar con los responsables de los departamentos para identificar las necesidades de capacitación en herramientas de uso diario de los empleados.

Coordinar la planificación, programación y entrega de los programas de capacitación.

Mantener registros de la capacitación realizada por los empleados.

Jefaturas de los departamentos

Identificar las necesidades de capacitación de su personal en relación con las herramientas de uso diario y la seguridad de la información.

Proporcionar información y recursos necesarios para apoyar la capacitación adecuada de sus empleados.

Supervisar y evaluar el cumplimiento de la capacitación por parte de sus empleados.

Empleados

Participar activamente en los programas de capacitación en herramientas de uso diario.

Aplicar los conocimientos adquiridos durante la capacitación en su trabajo diario.

Informar a su supervisor o al Departamento de Recursos Humanos, acerca de cualquier necesidad adicional de capacitación.

Lineamientos del proceso de capacitación

Identificación de necesidades de capacitación

Los responsables de los departamentos, en colaboración con el Departamento de Recursos Humanos, identifican las necesidades de capacitación de los empleados.

Diseño y desarrollo de programas de capacitación

Con base en las necesidades identificadas, se diseñan y desarrollan programas de capacitación adecuados, estos incluyen los aspectos relacionados con las herramientas de uso diario y la seguridad de la información.

Entrega de la capacitación

Los programas de capacitación se imparten, a través de métodos apropiados, como: sesiones presenciales, cursos en línea y tutoriales.

Evaluación de la capacitación

Se realizan evaluaciones periódicas para medir la efectividad de la capacitación y realizar mejoras si fuese necesario.

Registro de la capacitación

El Departamento de Recursos Humanos debe mantener registros actualizados de las capacitaciones realizadas por los empleados, así como la documentación respectiva, en cuanto a: certificados, cláusulas y contratos que los empleados firmen, pues son temas relacionados con la capacitación.

Cumplimiento

Todos los empleados deben cumplir con esta política y participar en los programas de capacitación establecidos.

La gerencia revisará regularmente esta política para garantizar su adecuación y efectividad, y realizará las modificaciones necesarias en caso de cambios en los requisitos o en las herramientas de uso diario.

Esta política será aprobada y modificada en caso de que se requiera por la gerencia y estará disponible en todo momento para todos los empleados, a través del sitio web interno, el cual es el medio de comunicación oficial del Departamento de Recursos Humanos.

Cualquier incumplimiento de esta política puede resultar en medidas disciplinarias o sanciones, de acuerdo con las políticas y procedimientos establecidos por la organización.

Control de cambios

Se debe documentar todo cambio, modificación y aprobación que se realice a esta política con el fin de llevar un control riguroso y ordenado.

Para concluir con este apartado, la seguridad de la información en si misma representa un aspecto fundamental por tomar en cuenta en la actualidad por las organizaciones y aún más importante la seguridad en lo que respecta a los recursos humanos, esto debido a que los empleados dentro de una organización representan un gran foco cuando se habla de amenazas y

vulnerabilidades, ya sea de manera directa o indirecta es por esto que, actualmente los ciberdelincuentes buscan por medio de ingeniera social, obtener acceso a una organización, a través de un empleado que de forma consciente o inconscientemente brinde acceso, por lo cual el diseño y documentación de políticas comprendidas en este apartado pretende minimizar estos riesgos y aumentar el grado de seguridad a la Compañía.

A17 Aspectos de seguridad de la información en la gestión de continuidad del negocio

La correcta gestión de la continuidad del negocio es un aspecto fundamental para garantizar que una compañía pueda mantener sus operaciones más críticas incluso en situaciones de emergencia o ante un desastre. Este apartado se enfoca en los aspectos de seguridad de la información relacionados con la gestión de la continuidad del negocio. Estos aspectos se refieren a las medidas y controles que la organización debe implementar para asegurar la disponibilidad, integridad y confidencialidad de la información crítica durante cualquier interrupción significativa.

Para este apartado de la normativa, el cual comprende el diseño y documentación de una sola política, el proceso de elección se dio de la misma manera que las políticas mencionadas con anterioridad en este documento, basándose como primer criterio en las necesidades de la organización así como también en el análisis de las entrevistas y la encuesta, específicamente en este último instrumento de análisis mencionado se contemplaron dos preguntas relacionadas con este tema y que arrojo resultados en donde la mayoría de los usuarios no están completamente al tanto de lo que significa una política de continuidad del negocio y mucho menos el haber sido participes en una prueba de continuidad del negocio dentro de la organización, es por esto que al diseñar esta política se está creando la base para que la organización y los empleados sepan cómo responder y actuar en caso de que se pierda la disponibilidad de un servicio crítico, todo esto

posterior a la implementación de esta política a futuro por parte de la organización. La política correspondiente a este aparatado será mencionada y detallada a continuación.

Política de continuidad del negocio para el proceso de soporte a los clientes.

Objetivo

La Política de Continuidad del Negocio (BCP, por sus siglas en inglés) establece los lineamientos generales para garantizar la continuidad de las operaciones críticas en caso de interrupciones o desastres. Esta política tiene sus bases en la norma ISO 27001, que proporciona un enfoque para la gestión de la seguridad de la información y busca minimizar el impacto de los incidentes y asegurar una rápida recuperación.

Alcance

Esta política se aplica a todos los empleados que tienen acceso a los sistemas de información y recursos críticos de la organización. Se implementará en todas las áreas y procesos de la organización, independientemente de su ubicación.

Responsables

Gerencia:

Establecer y mantener la política de continuidad del negocio.

Asignar los recursos necesarios para implementar y mantener un programa de continuidad del negocio eficaz.

Revisar y aprobar los planes de continuidad del negocio.

Responsable de la Continuidad del Negocio

Desarrollar, implementar y mantener el programa de continuidad del negocio.

Identificar los procesos críticos y los recursos necesarios para su recuperación.

Realizar pruebas semestrales de los planes de continuidad del negocio y actualizarlos según sea necesario.

Mantener y difundir la documentación relacionada con la continuidad del negocio.

Empleados

Conocer y cumplir con los planes de continuidad del negocio.

Informar, inmediatamente, cualquier incidente o situación que pueda afectar la continuidad de las operaciones.

Participar, activamente, en las pruebas y ejercicios de continuidad del negocio.

Evaluación de riegos

Se realiza una evaluación de riesgos semestral para identificar las amenazas y vulnerabilidades que pueden afectar la continuidad del negocio para el proceso de soporte a los clientes. Esta evaluación está basada en los siguientes pasos:

- Identificación de activos críticos y procesos clave.
- Evaluación de las amenazas y vulnerabilidades que podrían afectar a estos activos y procesos.
- Análisis del impacto potencial de los incidentes.
- Determinación de la probabilidad de que ocurran los incidentes.

Planes de continuidad del negocio

Realizar el desarrollo de planes de continuidad del negocio para garantizar la recuperación rápida y efectiva de los procesos críticos. Estos planes contienen:

- Procedimientos de respuesta a incidentes.
- Procedimientos de recuperación de desastres.
- Procedimientos de comunicación interna y externa.

- Roles y responsabilidades definidos durante una interrupción.
- Procedimientos de activación y desactivación de los planes de continuidad del negocio.

Pruebas y ejercicios

Se debe llevar a cabo pruebas periódicas de los planes de continuidad del negocio para evaluar su eficacia y realizar mejoras. Estas pruebas incluirán:

- Simulacros de desastres.
- Pruebas de recuperación de sistemas y datos.
- Ejercicios de comunicación y coordinación interna y externa.
- Evaluación de la capacidad de respuesta y tiempo de recuperación.

Capacitación y concienciación

Brindar capacitación y sensibilización regular a todos los empleados, respecto de la importancia de la continuidad del negocio y su función en la implementación de los planes de contingencia. Estas incluyen:

- Sesiones de capacitación trimestrales sobre los procedimientos respectivos ligados a la continuidad del negocio.
- Campañas de sensibilización por medio del correo electrónico sobre la importancia de informar incidentes y mantener la seguridad de la información.

Cumplimiento

La organización se compromete a cumplir en caso de que aplique esto por el tipo de mercado en el que se encuentra, con todas las leyes, regulaciones y requisitos contractuales relacionados con la continuidad del negocio y la seguridad de la información.

Esta política será aprobada y modificada en caso de que se requiera por la gerencia y estará disponible en todo momento para todos los empleados, a través del sitio web interno, el cual es el medio de comunicación oficial del Departamento de Recursos Humanos.

Cualquier incumplimiento de esta política puede resultar en medidas disciplinarias o sanciones, de acuerdo con las políticas y procedimientos establecidos por la organización.

Control de cambios

Se debe documentar todo cambio, modificación y aprobación que se realice a esta política con el fin de llevar un control riguroso y ordenado.

Procedimientos

Dentro del apartado A17 de la normativa internacional ISO 27001 el detalla los lineamientos que debe tener una política de continuidad del negocio, se habla dentro de esta que existen ciertos procedimientos que deben contemplarse para poder garantizar la continuidad del negocio para los procesos críticos de la organización razón por la cual con el fin de apoyar y guiar a la organización acerca de cómo se deben realizar los procedimientos según lo que indica la norma así como sentar una base, es que se brinda el apoyo en el diseño y documentación del plan de continuidad para el proceso crítico de soporte a los clientes.

Este procedimiento contiene todos los detalles basados en el entorno de Soluciones Seguras todos los lineamientos para asegurar de que exista la continuidad en el servicio de soporte a los clientes en caso de una interrupción mayor, a continuación, se detalla el procedimiento.

Procedimiento de continuidad del negocio para el proceso de soporte a los clientes

Objetivo

Este Plan de Continuidad de Negocio tiene como objetivo establecer las medidas y procedimientos necesarios para garantizar la continuidad de las operaciones, en caso de eventos

adversos o situaciones de emergencia. El plan se basa en los requisitos y mejores prácticas establecidos por la norma ISO 27001, con el fin de proteger la información y asegurar la continuidad de los servicios críticos de la organización.

Alcances

Energización

Garantizar la disponibilidad continua de energía para mantener las operaciones de la empresa Soluciones Seguras.

Mesa de soporte a clientes

Garantizar la continuidad de los servicios de soporte a los clientes de la empresa.

Conectividad

Mantener la conectividad de los sistemas de información y proveedores, navegación en internet y soporte remoto a los clientes.

Correo

Garantizar la disponibilidad y seguridad de los servicios de correo electrónico de la organización.

Central telefónica

Asegurar la continuidad de los servicios telefónicos de la Compañía.

On-call

Garantizar la disponibilidad de personal técnico en caso de emergencias o eventos adversos.

Sitio Web

Asegurar la disponibilidad y seguridad del sitio web de la empresa.

Presencialidad

Facilitar la continuidad de las operaciones en situaciones en las que el trabajo presencial no sea posible.

Teletrabajo

Garantizar la disponibilidad del servicio de soporte en caso de afectación del personal que se encuentra en modalidad no presencial.

Responsables

Se asignarán funciones y responsabilidades claras a los miembros del equipo de gestión y a los responsables de cada área funcional mencionada anteriormente. Esto incluirá la designación de un coordinador del plan de continuidad, la identificación de personas de respaldo en caso de ausencia y la capacitación adecuada del personal para la ejecución de las actividades del plan.

Acciones

Análisis y evaluación de Riesgos

Identificar los posibles riesgos que podrían afectar el servicio de soporte a los clientes, así como la infraestructura, tanto en el nivel físico como lógico que se utiliza en medio del proceso de soporte.

Evaluar el impacto potencial de cada riesgo en la disponibilidad del servicio de soporte a los clientes y la integridad de los datos e información.

Energización

Soluciones Seguras cuenta con un suministro de electricidad de manera continua esto por medio del abastecimiento de la corriente alterna proveniente del proveedor se servicios eléctricos de la zona, que en caso de falla de este suministro se cuenta con dos suministros alternativos que se detallan a continuación:

El primer suministro alternativo consiste en alimentación por medio de una batería de conmutación automática en caso del que el suministro de electricidad principal falle, este método mantiene la energización del centro de datos por un lapso de cinco minutos y en el momento que este se active se enviará una alerta a los responsables de continuidad del negocio para poder tomar las medidas necesarias en caso de ser requerido.

El segundo suministro de energía alternativo se refiere a una planta de combustible con la que cuenta el edificio donde actualmente se tienen las oficinas y este servicio según lo que indica el dueño del edificio debe entrar a funcionar en cinco minutos después de que el fluido eléctrico principal no regrese esto sirve de apoyo para poder recargar y alimentar la batería con la que se cuenta en el centro de datos es importante mencionar que la activación de este suministro se da de manera automática y por parte del proveedor mantiene un riguroso esquema de mantenimiento con el fin de que esta esté disponible y funcional siempre que se requiera.

Mesa de Soporte a los clientes

En la actualidad Soluciones Seguras cuenta con un portal web en premisas ubicado en el Centro de datos de la Oficina de Panamá al que tienen acceso todos los clientes para dar seguimiento a sus casos.

En lo que respecta al fallo del portal web para la mesa de ayuda se debe activar la gestión de casos, por medio del correo oficial de la empresa en donde los casos nuevos llegan, como lo indica el manual de creación y gestión de Tickets al correo destinado para casos y con los casos que ya se encontraban siendo gestionados por un ingeniero estos seguirán siendo actualizados por medio del correo oficial de la Compañía, es importante tener claro que este procedimiento se debe seguir hasta que el portal web sea restablecido de manera exitosa.

En cuanto a la actualización y gestión de nuevos tiquetes que se realizaron mientras la herramienta se encontraba el portal web caído estos serán ingresados por el personal de soporte a la herramienta web con el fin de que la documentación y seguimiento siempre queden respaldados en la herramienta.

Conectividad

Soluciones Seguras cuenta con dos proveedores de servicios de internet, así como la configuración respectiva para conmutación de las comunicaciones en caso de que uno de los dos proveedores falle lo que ocasiona que se mitigue el riesgo de una posible amenaza en uno de los servicios además garantizando con esto el acceso a los portales Web internos y de proveedores, correo y soporte remoto a los clientes.

Con lo que respecta al reporte por fallo en uno de los enlaces de conectividad a internet, una vez que se tiene identificado y descartado que sea un fallo interno se proceder a crear un caso con el proveedor del servicio esto con el fin de poder tener la redundancia en las comunicaciones de manera activa la mayoría del tiempo posible.

Correo

Soluciones Seguras tiene contratado un servicio de correo en la nube con la empresa Microsoft en donde según indica esta empresa ellos manejan un acuerdo de nivel del servicio de 99.9% para los servicios en la nube, esto significa que el servicio cuenta con un alto nivel de disponibilidad.

En el posible escenario que este servicio llegará a presentar inconvenientes el primer paso consiste en realizar un aviso a los clientes vía telefónica para que los reportes y averías que presenten en los servicios contratados se realicen por medio del número telefónico destinado para

el servicio de soporte además la comunicación Ingeniero-Cliente y viceversa se estará realizando por medio de los teléfonos móviles corporativos con los que cuenta el personal.

Central telefónica

La organización cuenta con un servicio de telefonía de voz sobre IP(VoIP) en premisas administrado por el personal de soporte técnico y en donde se cuenta con un aplicativo instalado para llamadas en las computadoras de los ingenieros, así como teléfonos físicos.

En el caso de que se dé un problema con la central telefónica que afecte los teléfonos IP físicos y los aplicativos instalados en las computadoras la jefatura de ingeniera emitirá un correo hacia los clientes con el fin de poner en aviso sobre el problema presentado con la central telefónica y, a su vez, recordarles el contacto por medio del número de On-call en caso de necesitar comunicarse vía telefónica.

Es importante mencionar que los ingenieros también cuentan con un teléfono móvil empresarial por lo cual en caso de necesitar conversar con un cliente y la central esté presentando inconvenientes podrán hacer uso de este dispositivo corporativo para poder comunicarse sin ningún problema lo que garantiza una comunicación hacia los clientes de manera exitosa.

Una vez, recuperado el sitio Web y validado su correcto funcionamiento, los clientes podrán nuevamente contar con las opciones de contacto e información de la mesa de soporte.

On-call

Como parte del servicio de On-call con el que cuenta la empresa, se les brinda a los clientes un número para el reporte de emergencias fuera de horario y dentro de horario en el caso de que la urgencia lo amerite.

Soluciones Seguras cuenta con un rol de ingenieros semanal definido por semestre para el servicio de disponibilidad por lo que en el caso de las llamadas que realicen los clientes al número mencionado con anterioridad serán atendidas por el ingeniero a cargo del On-call a ese momento.

En el caso de que el cliente realice tres llamadas seguidas sin obtener respuesta por parte del servicio de On-call el cliente procederá a escalar con el siguiente nivel jerárquico e intentar tres veces el llamado telefónico con cada uno de los contactos con el fin de que sea atendido con la brevedad correspondiente los contactos de escalación se detallan a continuación y en orden de la siguiente manera:

- Contacto Escalación 1
- Contacto Escalación 2
- Contacto Escalación 3

Sitio Web

Soluciones Seguras cuenta con un sitio web que tiene como objetivo guiar a los clientes al sitio de la mesa de soporte, así como también brindar toda la información para el contacto respectivo, en el caso de que este sitio web no se encuentre operativo los clientes tienen la posibilidad de ponerse en contacto, a través de los demás medios indicados en el manual de creación de casos de soporte brindado a los clientes, estos son los siguientes:

- Correo electrónico
- On-call
- Vía telefónica

Presencialidad

Con lo que corresponde a la presencialidad para el proceso de recuperación de desastres se tomará en cuenta dos escenarios los cuales se profundizarán en breve.

El primer escenario consiste en el caso de un incidente o desastre natural que impida el trabajo presencial con personal en las oficinas, en este escenario la jefatura del Departamento de Ingeniería en conjunto con el encargado de la continuidad del negocio se comunicarán con el personal de Soluciones Seguras ubicado en Panamá para que puedan soportar paulatinamente el servicio de soporte de Costa Rica y al mismo tiempo establecerán un plan de desalojo de las oficinas por parte de los ingenieros hacia sus domicilios, con base en la distancia desde a la oficina en donde los que vivan más cerca sean los primero y así sucesivamente garantizar el orden en el proceso esto para que se puedan retomar en el menor tiempo posible las operaciones del servicio de soporte a los clientes del país.

Y el segundo escenario corresponde al caso de incidente o desastre que impida ir a las oficinas se realizará teletrabajo de la manera que normalmente se realiza lo que garantiza que las operaciones continúen sin afectación en el servicio brindado.

Teletrabajo

En caso del personal que se encuentre realizando las labores diarias de manera remota, les suceda algún inconveniente en la residencia con la conectividad hacia internet o el fluido eléctrico y el problema persiste por más de treinta minutos el ingeniero debe movilizarse a un lugar donde cuente con las condiciones para poder continuar con su labor diaria y si este escenario lo amerita se puede trasladar a las oficinas para continuar laborando además es importante recalcar que si la afectación de los factores indicados con anterioridad se debe a un trabajo previamente programado

por parte de los proveedores de servicio el personal afectado deberá acudir a las oficinas para realizar sus labores desde el inicio de la jornada laboral.

Mantenimiento y Actualización

Este procedimiento del plan de continuidad de negocio será revisado y actualizado de manera semestral por el responsable asignado de la Continuidad del Negocio y aprobado por la Gerencia de la organización.

Esta política será aprobada y modificada en caso de que se requiera por la gerencia y estará disponible en todo momento para todos los empleados, a través del sitio web interno el cual es el medio de comunicación oficial del Departamento de Recursos Humanos.

Cualquier incumplimiento de esta política puede resultar en medidas disciplinarias o sanciones, de acuerdo con las políticas y procedimientos establecidos por la organización.

Control de cambios

Se debe documentar todo cambio, modificación y aprobación que se realice a esta política con el fin de llevar un control riguroso y ordenado.

En conclusión la propuesta planteada para la empresa Soluciones Seguras se basó primordialmente en las necesidades indicadas en el apartado anterior sustentado y respaldado por las herramientas de análisis que se utilizaron, por lo que el diseño y documentación de las políticas para los subprocesos seleccionados además del procedimiento creado aportan valor a la Compañía y a los procesos así como también el incremento y optimización de la seguridad informática dentro de esta que a su vez protegen los activos más críticos de la organización.

Todas las políticas diseñadas y documentadas para este proyecto se hicieron con base en las buenas prácticas y controles que indica la norma de seguridad de la información ISO 27001, la

cual busca reducir los riesgos de seguridad, así como promover una cultura de seguridad en la que prevalezca en todo momento la integridad, disponibilidad y confidencialidad de la información.

Capítulo 6. Conclusiones y Recomendaciones

El objetivo de este capítulo es presentar las conclusiones derivadas del desarrollo de este trabajo final de graduación, así como también brindar recomendaciones relacionadas, con el objetivo de hacer una contribución significativa al campo de investigación.

Las conclusiones y recomendaciones que se mencionan absolutamente todas tienen su fundamento y respaldo en las necesidades de la organización y en el análisis de la información recopilada.

Conclusiones

Durante la realización de este proyecto, como primer paso se realizó los análisis correspondientes para establecer el estado real de la Compañía Soluciones Seguras, con base en los controles y políticas según lo que indica la norma ISO 27001 en donde se observó que a pesar de que algunos procesos tuvieran documentación relacionada, en cuanto a controles estos no se encontraban alineados con la norma o carecían de detalles acerca de las buenas prácticas que esta norma dicta.

Es importante indicar que Soluciones Seguras al ser una empresa como su nombre lo indica que se ubica en el sector de seguridad informática cuando se conversó con el director ejecutivo (CEO, por sus siglas en inglés) de la Compañía acerca del objetivo principal de este proyecto, nos indicó que existen conversaciones a lo interno para poder crear un plan para certificar el proceso de soporte a los clientes a futuro por lo que ve provechoso este trabajo, ya que funciona como base y de valor para ese proyecto a futuro que se piensa implementar dentro de la organización.

Además, se observa que existe cierto grado de desconocimiento por parte usuarios acerca de la documentación existente de los varios subprocesos, así como la inexistencia de documentación relacionado con políticas de los subprocesos restantes que están contenidos dentro

del proceso seleccionado de soporte a los clientes lo que se convierte en una vulnerabilidad que puede ser aprovechada por los ciberdelincuentes para ocasionar daños a la organización.

Conclusiones objetivo específico 1

En conclusión, el objetivo específico de analizar los procesos críticos relacionados con la seguridad de la información se logró alcanzar con éxito. En el proceso de desarrollo de este proyecto, se llevaron a cabo análisis a profundidad basándose en las necesidades de la organización y resultados obtenidos de los instrumentos de análisis utilizados a los diferentes procesos involucrados dentro de este trabajo.

El principal propósito de este análisis fue identificar y seleccionar los procesos y subprocesos críticos a los cuales se les debía aplicar el objetivo principal el cual era poder diseñar y documentar políticas de seguridad de la información basándose en los lineamientos y mejores prácticas que indica la ISO 27001.

Conclusiones objetivo específico 2

En resumen, el objetivo específico de plantear políticas y mejores prácticas basadas en la norma ISO 27001 para los procesos críticos definidos se convirtió en una estrategia para fortalecer y mejorar la seguridad de la información dentro de Soluciones Seguras.

El plantear las mejores prácticas y lineamientos que establece la norma ISO 27001 hace que se obtenga como resultado un marco de seguridad más sólido que a su vez garantiza la protección de los activos para la Compañía, además que es algo muy valioso para Soluciones Seguras, también es importante mencionar que la identificación y selección de los procesos críticos permitió que los esfuerzos realizados en este proyecto se dieran, específicamente en los aspectos en los que la necesidad de la empresa y resultados de los análisis requirieron.

Conclusiones objetivo específico 3

Para finalizar, el objetivo específico de diseñar la documentación con las políticas planteadas tiene un propósito muy importante el cual es unificar en un documento oficial de la organización, las mejores prácticas y lineamientos que indica la norma ISO 27001 para cada una de las políticas con el fin de mejorar de la seguridad de la información.

Al diseñar una documentación bien estructurada y clara, las políticas de seguridad son comprendidas y adoptadas más fácilmente por todos los empleados, lo que minimiza la posibilidad de errores o malentendidos. La uniformidad en las prácticas de gestión de la información también fomenta la colaboración entre los miembros de una organización y una cultura de seguridad.

Recomendaciones

En este apartado se mencionará y detallará posibles recomendaciones para la organización tomando en cuenta el trabajo realizado, estas se basan en los resultados de los análisis y además en el contexto de la organización y tienen como fin el aportar valor a la organización además de preservar la confidencialidad, integridad y disponibilidad de la información, lo que garantiza la seguridad.

Como primera recomendación muy importante es que se busque cómo promover la sensibilización y capacitación en periodos establecidos esto para temas de seguridad de la información para todos los miembros de la organización. Una organización con colaboradores bien informados tiene una línea de defensa crucial contra posibles ataques y errores no intencionados.

Desde otra arista, una segunda recomendación es que se fomente una cultura de seguridad en la en toda la organización, donde el cuido y resguardo de la información sea una prioridad para todos los empleados y que además promueva un ambiente de seguridad para la Compañía que se refleja en la reducción de riesgos y vulnerabilidades dentro de esta.

Y por último velar por el cumplimiento las recomendaciones anteriores, políticas y procesos de seguridad existentes en la organización es sumamente importante que se realicen auditorías internas y revisiones regulares que permitan identificar no solo el cumplimiento, sino las áreas de oportunidad y a la vez, permitir que se corrijan posibles debilidades.

Capítulo 7. Trabajos a Futuro

En este capítulo, se abordará todas las posibles tareas que se contemplan para el futuro con el objetivo de fortalecer la seguridad de la información de la empresa Soluciones Seguras siempre de la mano con los estándares internacionales y mejores prácticas.

La primera tarea importante que debe llevarse a cabo en el futuro es la implementación de las políticas de seguridad diseñadas y debidamente documentadas durante la realización de este proyecto, además es importante en la búsqueda garantizar la efectividad de estas, se debe establecer un plan detallado para el despliegue, que, a su vez, involucre la sensibilización y capacitación de los empleados, así como la asignación de responsabilidades claras para su cumplimiento.

Junto con la tarea anterior es importante que se realice la planificación y preparación para la certificación de proceso de soporte a los clientes, además esto también conlleva revisar, diseñar e implementar las políticas y controles para los demás subprocesos que existen dentro de este proceso y que no se incluyeron en este proyecto, ya que al obtener esta certificación el proceso será acreditado con los más altos estándares en materia de seguridad de la información lo que aumentaría los niveles de seguridad internos y la reputación de la organización.

Otro punto importante para tomar en cuenta a futuro son los procedimientos que debe contener la política relacionada con la continuidad del negocio y que aún no han sido creados por lo que tomando como base el procedimiento que se creó para este trabajo, estos procedimientos abarcan desde la respuesta a incidentes y la comunicación interna y externa y la definición de roles y responsabilidades en situaciones de crisis. Es importante que la creación de estos procedimientos se lleve a cabo en conjunto con los departamentos respectivos, para asegurar su viabilidad y que además se adecuen a las necesidades específicas del proceso de soporte a los clientes.

Para finalizar, una vez que se hayan implementado las políticas y procedimientos, es primordial que se establezca un programa de evaluación semestral y de mejora continua. La seguridad de la información contiene aspectos que, continuamente, están cambiando y renovándose por lo que es necesario que la organización se mantenga actualizada de cara a nuevas amenazas y desafíos. Asimismo, también se debe buscar cómo establecer una cultura de mejora continua, en la cual el personal sea impulsado a reportar incidentes o sugerencias con el fin de fortalecer aún más la seguridad de los datos propios de la organización.

Referencias

Alonso, C. (2023, marzo 30). *ISO 27000 y el conjunto de estándares de Seguridad de la Información*. GlobalSuite Solutions. https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/

Caro, C., & Cubillos, M. (2021). *DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL PROCESO DE SOPORTE Y DESARROLLO DE SOFTWARE DE LA EMPRESA FINANCOL, BASADO EN LA NORMA ISO/IEC 27001:2013* [Trabajo de grado, UNIVERSIDAD PILOTO DE COLOMBIA]. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/11356/DISE%C3%91O%20DEL%20SISTEMA%20DE%20GESTI%C3%93N%20DE%20SEGURIDAD%20DE%20LA%20INFORMACI%C3%93N%20%28SGSI%29%20PARA%20EL%20PROCESO%20DE%20SOPORTE%20Y%20DESARROLLO%20DE%20SOFTWARE%20DE%20LA%20EMPRESA%20FINANCOL%2C%20BASADO%20EN%20LA%20NORMA%20ISOIEC%20270012013.pdf?sequence=1&isAllowed=y

Chen, R. (s/f). *Soluciones seguras - acerca de nosotros*. Solucionesseguras.com. Recuperado el 23 de mayo de 2023, de https://www.solucionesseguras.com/empresa/acerca-de-nosotros

Coll, F. (2021a, febrero 17). *Fuente primaria*. Economipedia. https://economipedia.com/definiciones/fuente-primaria.html

Coll, F. (2021b, febrero 21). *Fuente secundaria*. Economipedia. https://economipedia.com/definiciones/fuente-secundaria.html

Cómo proteger la seguridad de la información en una empresa. (2020, diciembre 11). GRUPO ACMS Consultores. https://www.grupoacms.com/blog/seguridad-la-informacion

Cr, P. E. (2022, agosto 22). *Costa Rica registró 513 millones de intentos de ciberataques en la primera mitad del año*. Diario Digital Nuestro País. https://www.elpais.cr/2022/08/22/costa-rica-registro-513-millones-de-intentos-de-ciberataques-en-la-primera-mitad-del-ano/

Datademia. (2022, mayo 9). *¿Qué son los datos?* Datademia. https://datademia.es/blog/que-son-los-datos

Emagister, B. (2022, junio 30). *Norma ISO 27001: qué es, ventajas y desventajas*. Blog Emagister; Emagister. https://www.emagister.com/blog/norma-iso-27001-que-es-ventajas-y-desventajas/

García, J. (2022, julio 28). *Norma ISO 27001: Qué Es, Beneficios y Proceso de Certificación*. Deltaprotect.com; Delta Protect. https://www.deltaprotect.com/blog/que-es-iso-27001

GlobalSuite Solutions. (2023, marzo 20). *¿Qué es la norma ISO 27001 y para qué sirve?* GlobalSuite Solutions. https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/

Gómez, M. C. (2023, junio 28). *Qué es una encuesta, para qué sirve y qué tipos existen*. Hubspot.es. https://blog.hubspot.es/service/que-es-una-encuesta

Grupo Cynthus. (2023, marzo 5). ISO 27002: qué es y diferencias con la ISO 27001. *Grupo Cynthus*. https://www.cynthus.com.mx/iso-27002-diferencias-con-iso-27001/

IBM Documentation. (2021, abril 14). Ibm.com. https://www.ibm.com/docs/es/i/7.3?topic=security-policy-objectives

Investigadores. (2020, marzo 23). *Fuentes de información primarias, secundarias y terciarias*. Técnicas de Investigación. https://tecnicasdeinvestigacion.com/fuentes-de-informacion-primaria-y-secundaria-y-terciaria/

ISO 27001 - Certificado ISO 27001 punto por punto - Presupuesto Online. (s/f). ISO 27001. Recuperado el 15 de mayo de 2023, de https://normaiso27001.es/

Lluis, J. (s/f). *Becomit obtiene la certificación ISO 27001 de Seguridad en la Información*. Becomit. Recuperado el 10 de abril de 2023, de https://becomit.com/iso-27001/

Lucena, P. (2023, mayo 3). *¿Qué es la información en informática y otras ciencias?* Maestrías y MBA. https://www.cesuma.mx/blog/que-es-la-informacion-en-informatica-y-otras-ciencias.html

Martínez, J. G. (2023, enero 11). *Políticas de Seguridad: Por Qué Son Importantes Para tu Negocio*. Deltaprotect.com; Delta Protect. https://www.deltaprotect.com/blog/politicas-de-seguridad

Navamuel, J. (2023, abril 19). *Análisis de datos cualitativos: qué es y su importancia*. Análisis de datos cualitativos: qué es y su importancia. https://www.incentro.com/es-ES/blog/analisis-de-datos-cualitativos

Palomo, H. (2022, mayo 18). *DEXMA Obtiene la Certificación ISO 27001*. Spacewell Energy. https://www.dexma.com/es/noticias-es/dexma-obtiene-la-certificacion-iso-27001/

Principios de la seguridad informática ¡Lo que debes conocer! (2022, octubre 18). UNIR México. https://mexico.unir.net/ingenieria/noticias/principios-seguridad-informatica/

Que Es Un Data Center Y Que Opciones Tengo Para Almacenar. (2023, abril 30). *Datos 101*. https://www.datos101.com/blog/que-es-un-data-center/

¿Qué son las normas ISO y para qué sirven? (2020, junio 9). Gob.cl. https://centrodeayuda.prochile.gob.cl/hc/es-419/articles/360047722114--Qu%C3%A9-son-las-normas-ISO-y-para-qu%C3%A9-sirven-

Rus, E. (2020, diciembre 10). *Investigación aplicada*. Economipedia. https://economipedia.com/definiciones/investigacion-aplicada.html

Sánchez, C. (2020, enero 29). Normas-apa.org. https://normas-apa.org/estructura/figuras/

Suárez, E. (2023, marzo 27). Fuentes de Información: qué son, tipos y ejemplos. *Experto Universitario*. https://expertouniversitario.es/blog/fuentes-de-informacion/

Velásquez, W. (2022, marzo 4). Herramientas de recolección de datos cualitativos en investigaciones de mercado. *MindTec Neuromarketing*. http://mindtecbolivia.com/herramientas-recoleccion-datos-cualitativos/

Apéndices

Anexo 1

Encuesta

Diseño de Políticas ISO 27001

Encuesta para TFG Jehoshua Rojas - Licenciatura en Seguridad Informática

1. ¿Conoce con claridad la política de contraseñas de Soluciones Seguras?

Sí

No

2. ¿Cuál método utiliza para almacenar sus contraseñas?

Físico (Papel)

Programa no cifrado

Programa cifrado

3. ¿Cómo crea usualmente sus contraseñas?

Utilizo un generador de contraseñas

Las creo yo mismo según a conveniencia

4. ¿Con qué frecuencia realiza el cambio de sus contraseñas?

Menos de 3 meses

De 3 a 6 meses

Mayor a 6 meses

5. ¿Qué longitud utiliza, usualmente, sus contraseñas?

Menos de 8 caracteres

De 8 a 15 caracteres

Más de 15 caracteres

6. ¿Conoce lo que es una política de continuidad del negocio?

Sí

No

7. ¿Ha participado dentro de Soluciones Seguras en una prueba de continuidad del negocio?

Sí

No

8. ¿Tiene conocimiento de cuáles son los requisitos y obligaciones del puesto que, actualmente desempeña?

Sí

No

9. ¿Conoce usted cuáles son los requisitos para un ser elegible para un ascenso?

Sí

No

Anexo 2

Machote Política ISO 27001

Fecha de creación:

Código:

Nombre de la Política:

Departamento encargado:

Objetivo:

Alcance:

Responsables:

Acciones y Lineamientos:

Cumplimiento:

Control de cambios:

Anexo 3

Entrevista Gerencia

Nombre: Reunión TFG Jehoshua Rojas

Lugar: Microsoft Teams

Fecha: 19/5/23

Asistentes:

- Eli Faskha
- Joey Milgram
- Jehoshua Rojas

Tema: Reunión TFG Jehoshua Rojas

Puntos tratados:

- Se conversa acerca del objetivo del alcance del TFG.
- Se define el proceso crítico para el desarrollo del trabajo.
- Se establece la persona que fungirá de apoyo para acceso a la información y recursos necesarios.

Acuerdos:

- Crear Repositorio Central con información para validar los avances de la documentación. Encargado Jehoshua
- Programar Reunión con gerente regional de soporte para comenzar con el análisis de la información. Encargado Jehoshua

Anexo 4

Entrevista 1 Gerente Regional de Soporte

Nombre: Reunión TFG Jehoshua Rojas

Lugar: Microsoft Teams

Fecha: 22/5/23

Asistentes:

- Omar Gonzalez
- Jehoshua Rojas

Tema: TFG Jehoshua Rojas

Puntos tratados:

- Se revisa en conjunto la documentación oficial de norma ISO 27001 para validar los procesos que pueden ser seleccionados.
- Se analizan la cantidad de políticas, así como los procesos que pueden ser alcanzables para el desarrollo del proyecto.

Acuerdos:

- Validar con la universidad si existe un mínimo de políticas requerido. Encargado Jehoshua
- Lectura de los controles de la norma ISO27001 para la próxima reunión. Encargado Jehoshua
- Programar siguiente reunión para dejar definidos los alcances del proyecto. Encargados Omar y Jehoshua.

Anexo 5

Entrevista 2 Gerente Regional de Soporte

Nombre: Reunión TFG Jehoshua Rojas

Lugar: Microsoft Teams

Fecha: 30/5/23

Asistentes:

- Omar González

- Jehoshua Rojas

Tema: TFG Jehoshua Rojas

Puntos tratados:

- Se conversa y se define la cantidad de políticas, para un total de 6.
- Se realiza la selección de los subprocesos para el desarrollo de este proyecto.
    - Política de contraseñas
    - Política de selección de candidatos para Ingeniería
    - Política de responsabilidades de los ingenieros durante la relación laboral
    - Política de cambio o finalización en la relación laboral.
    - Política de continuidad del negocio para el proceso de soporte a los clientes.
    - Política de capacitación del personal de Ingeniería.
- Se valida y se recopila la información y documentación relacionada con los procesos como políticas, manuales y controles existentes.
- Se conversa acerca de las políticas que involucran al Departamento de Recursos Humanos y a quien se debe contactar.
    - Política de Selección de candidatos para Ingeniería
    - Política de responsabilidades de los ingenieros durante la relación laboral
    - Política de cambio o finalización en la relación laboral.

Acuerdos:

- Análisis de la documentación brindada por Omar. Encargado Jehoshua
- Realizar diseño y documentación de Políticas para los subprocesos seleccionados Encargado Jehoshua

- Reunión con Recursos Humanos para las políticas que involucran este Departamento. Encargado Jehoshua

Anexo 6

Entrevista 3 Gerente Regional de Recursos Humanos

Nombre: Reunión TFG Jehoshua Rojas

Lugar: Microsoft Teams

Fecha: 30/5/23

Asistentes:

- Yolet Sánchez
- Jehoshua Rojas

Tema: TFG Jehoshua Rojas

Puntos tratados:

- Se conversa a detalle sobre el objetivo del proyecto y acerca de las políticas seleccionadas en conjunto con el Gerente Regional de Soporte.
- Se validan y recopilan los manuales y procedimientos existentes para los subprocesos:
    - Política de Selección de candidatos para Ingeniería
    - Política de responsabilidades de los ingenieros durante la relación laboral
    - Política de cambio o finalización en la relación laboral.

Acuerdos:

- Análisis de la documentación brindada por Yolet. Encargado Jehoshua
- Realizar diseño y documentación de Políticas para los subprocesos seleccionados. Encargado Jehoshua