UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: **RPC-SO-02-No.053-2021**

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
BUENAS PRÁCTICAS PARA EL CONTROL DE ACCESO EN LA EMPRESA NEXSYS DEL ECUADOR BASADA EN LA NORMA ISO 27001
Línea de Investigación:
SEGURIDAD INFORMÁTICA
Campo amplio de conocimiento:
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
Autor:
Ing. Jean Alexander Jiménez Lara
Tutores:
PhD. Maryory Urdaneta MSc. Renato Toasa

Quito – Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, MSc. Renato Toasa con C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado: Propuesta de buenas prácticas para el control de acceso en la empresa Nexsys del Ecuador basada en la Norma ISO 27001.

Elaborado por: Jean Alexander Jiménez Lara, de C.I: 1715437438, estudiante de la Maestría: Seguridad de la Información, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2024

Firmado electrónicamente por:
RENATO MAURICIO TOASA GUACHI

_____

Firma

APROBACIÓN DEL TUTOR

Yo, PhD. Maryory Urdaneta con C.I: 1759316126 en mi calidad de Tutor del proyecto de investigación titulado: Propuesta de buenas prácticas para el control de acceso en la empresa Nexsys del Ecuador basada en la Norma ISO 27001.

Elaborado por: Jean Alexander Jiménez Lara, de C.I: 1715437438, estudiante de la Maestría: Seguridad de la Información, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2024

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Jean Alexander Jiménez Lara con C.I: 1715437438, autor del proyecto de titulación denominado: Propuesta de buenas prácticas para el control de acceso en la empresa Nexsys del Ecuador basada en la Norma ISO 27001. Previo a la obtención del título de Magister en Seguridad de la Información

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

Quito D.M., septiembre de 2024

Firmado electrónicamente por:
JEAN ALEXANDER
JIMENEZ LARA

Firma

Tabla de contenidos

Índice de tablas

Índice de figuras

Índice de Anexos

INFORMACIÓN GENERAL

Contextualización del tema

El aumento por parte de las compañías hacia la ciencia de la comunicación y la información ha inclinado a una necesidad urgente de garantizar que la información sea confiable, confidencial y accesible. En este contexto, la protección hacia los datos se ha transformado en un componente crucial al momento de garantizar que las entidades funcionen de manera efectiva y confiable. Los incidentes y los ciberataques de seguridad son cada vez más sofisticados y pueden causar pérdidas financieras, daño a la reputación y pérdida de confianza del cliente (García R. & Morales, 2021).

Las empresas mayoristas tienen una actividad vital en la cadena de aprovisionamiento y la economía global. Estas organizaciones manejan grandes volúmenes de información sensible, incluyendo datos de clientes, proveedores, inventario y transacciones financieras. Dada la naturaleza crítica de la información que manejan, es imperativo que implementen medidas sólidas de invulnerabilidad de la información para disminuir riesgos y salvaguardar sus activos digitales (Rodríguez A. F. & Pérez R. M, 2021).

La ISO 27001 se ha consolidado como un estándar clave en la administración en la seguridad de la información. Su enfoque fundamentado en la gestión de amenazas capacita a las organizaciones para identificar y tratar de manera eficaz las amenazas y vulnerabilidades particulares a las que están expuestas. El control de acceso es uno de los elementos fundamentales de la ISO 27001, que se refiere a las técnicas y procedimientos para confirmar que solo las personas definidas tengan el ingreso a la información y los medios de la organización (Moscaiza, 2023).

Se han realizado varios estudios en distintos segmentos de mercado que manejan gran variedad de plataformas tecnológicas y se ha llegado a la conclusión de que los ataques digitales individuales o por grupos orientados a objetivos nacionales han producido grandes pérdidas económicas, esto quiere decir que, la industria lleva muchos años siendo vulnerable y al mismo

tiempo, se han priorizado otros tipos de riesgos, dejando de lado la protección tecnológica que les permita mantener el orden financiero y su flujo económico no se vea afectado (Zapata A. & Ortega, 2023).

Problema de investigación

La empresa maneja datos sensibles de clientes, proveedores y socios comerciales. La escasez de controles de seguridad adecuados podría dar espacios a fugas de información, lo que comprometería la lealtad de los clientes y afectaría negativamente el prestigio de la empresa.

La industria de ventas mayoristas de hardware y software es un objetivo atractivo para los ciberdelincuentes debido a la naturaleza valiosa de los productos que manejan. La empresa podría enfrentar amenazas cibernéticas como ransomware, malware y ataques de obstrucción de servicio (DDoS), lo que podría causar interrupciones en sus operaciones y pérdidas financieras significativas.

Una gestión inadecuada de los privilegios de acceso puede abrir la puerta a que empleados o terceros no autorizados accedan a información sensible o realicen modificaciones no permitidas en sistemas y bases de datos. Además, la necesidad de capacitación adecuada en invulnerabilidad de la información y la poca conciencia sobre los riesgos asociados entre los empleados pueden llevar a errores humanos que comprometan la exactitud y privacidad de los datos.

Por otro lado, la ausencia de un protocolo de actuación ante emergencias claramente definido podría resultar en retrasos significativos al intentar mitigar problemas de seguridad, limitando la capacidad de la compañía para disminuir el impacto de dichos incidentes. Esto, sumado a posibles deficiencias en adhesión a las regulaciones de privacidad de la información, especialmente en jurisdicciones con leyes estrictas de privacidad, podría generar serios problemas legales y regulatorios para la organización.

¿Con la propuesta e implementaciones de buenas prácticas se podrá evitar el robo de información?

Objetivo general

Desarrollar una propuesta de buenas prácticas para el control de acceso en la empresa Nexsys del Ecuador basada en la Norma ISO 27001 – A9 Control de acceso.

Objetivos específicos

- Contextualizar los fundamentos teóricos sobre las exigencias de la norma ISO 27001 – A9 Control de acceso en el contexto de la seguridad de la información.
- Diagnosticar los mejores estándares y prácticas relevantes en el dominio de la seguridad de la información, identificando aquellos más adaptables a la realidad de la empresa Nexsys del Ecuador.
- Elaborar un proceso de buenas prácticas para el control de acceso que combine las exigencias de la norma ISO 27001 – A9 Control de accesos con las mejores prácticas identificadas en la investigación.
- Validar el impacto de la propuesta a través de criterios de especialistas en seguridad de la información, evaluando su aplicabilidad y efectividad en la empresa Nexsys del Ecuador.

Vinculación con la sociedad y beneficiarios directos:

Beneficiarios directos e indirectos del proyecto:

Los receptores directos de este proyecto incluyen, en primer lugar, a la empresa Nexsys del Ecuador, que al implementar las buenas prácticas propuestas podrá fortalecer significativamente su seguridad de la información. Esto les permitirá resguardar mejor los datos sensibles de sus consumidores, proveedores y accionistas, reduciendo el riesgo de violaciones de seguridad y mejorando la confianza de todas las partes comprometidas. Indirectamente, los consumidores y socios comerciales de Nexsys también se beneficiarán al tener garantizada la seguridad de sus datos, lo que a su vez fortalecerá las relaciones comerciales y aumentará la satisfacción del cliente.

Resumen de los aportes de la investigación para el área del conocimiento:

Esta investigación contribuye al campo de la seguridad de la información al ofrecer una propuesta práctica en la ejecución de la norma ISO 27001 en el contexto específico de una empresa mayorista de tecnología. A través de un análisis detallado de las vulnerabilidades y desafíos de seguridad en Nexsys, se han identificado estrategias efectivas que pueden ser replicadas en otras empresas del sector. Además, se fomenta la ejecución de normativas de control adaptativas y se provee de un modelo de implementación que puede ser utilizado como referencia por académicos y profesionales en el campo del manejo de seguridad de la información.

Resumen de los aportes de vinculación con la sociedad: empresas, organizaciones y comunidades:

La iniciativa ejerce una influencia notable en la comunidad al fortalecer la salvaguardia de la información personal y empresarial en un entorno digital cada vez más riesgoso. Al fortalecer las prácticas de seguridad de las empresas, se promueve un ambiente de negocios más seguro y confiable, lo que beneficia no solo a las organizaciones, sino también a los consumidores y la comunidad en general. La reducción de incidentes de seguridad permite que las empresas

destinen más recursos a la innovación y al desarrollo, fomentando un crecimiento económico sostenible. Además, al aumentar la confianza en el comercio electrónico, se impulsará el desarrollo del mercado digital, lo que puede tener efectos positivos en la economía local y global.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

La Seguridad de la información

En la era informática actual, el entorno de la seguridad de la información de las compañías es un tema importante. A medida que la tecnología avanza y las organizaciones se convierten en dependientes de los sistemas informáticos y la conectividad, los riesgos de seguridad se han vuelto más sofisticados y omnipresentes. Algunos de los aspectos destacados acerca de la seguridad de la información en las instituciones en el presente son los siguientes:

a. Ciberataques en aumento: Los ciberataques, como el malware, ransomware, ataques de phishing y de denegación de servicio (DDoS), han aumentado en frecuencia y sofisticación. Las empresas enfrentan una gran variedad de amenazas, desde actores individuales hasta grupos de hackers y, en algunos casos, incluso ciberataques respaldados por estados nacionales (Gómez L. A. & Rodríguez M., 2020).

b. Protección de datos personales: La invulnerabilidad de la intimidad y la información se ha vuelto crucial debido al creciente número de información personal que manejan las empresas. Las empresas deben cumplir con leyes y reglamentos como el Reglamento General de Protección de Datos (GDPR) en varios países (Martínez P. J. & Pineda F. M., 2019).

c. Nuevas tecnologías y desafíos: La adopción de tecnologías modernas como el cloud computing, la inteligencia artificial (IA) y también el Internet de las cosas (IoT) han traído consigo nuevos desafíos de seguridad. La gestión y protección de datos en entornos distribuidos y diversos requiere una planificación cuidadosa (Torres D. E. & Ramírez L. A., 2021).

d. Trabajo remoto y BYOD: El uso de dispositivos personales para asuntos laborales y el trabajo remoto se han acelerado debido a la pandemia de COVID-19. Esto ha incrementado los riesgos de seguridad, ya que los trabajadores pueden obtener a la información de la empresa desde redes y dispositivos no controlados por la organización (Fernández A. L. & Alvarado J., 2020).

e. Amenazas Internas: Las amenazas internas, ya sea por negligencia o intenciones maliciosas de empleados, pueden ser una fuente significativa de riesgos para la invulnerabilidad de datos en las empresas (Cruz R. & Espinoza S., 2022).

f. Cumplimiento Normativo: Las empresas deben realizar diversas regulaciones y estándares vinculados con la invulnerabilidad de la información, y el no cumplimiento puede resultar en sanciones financieras y daños a la reputación (Pérez J. & López M., 2019).

g. Importancia de la Conciencia y Educación en Seguridad: La capacitación y concienciación del personal son fundamentales para disminuir la amenaza de violaciones de seguridad causadas por errores humanos. Los empleados deben estar informados acerca de las mejores prácticas de protección de datos para detectar y evitar posibles amenazas (García R. & Morales P., 2021).

h. Resiliencia y Planificación de Continuidad del Negocio: La disposición de recuperarse frente a incidentes de seguridad es esencial para minimizar el impacto de los ataques. Las empresas deben tener planes de respuesta a incidentes y estrategias de continuidad para garantizar que las operaciones se recuperen rápidamente y que las interrupciones sean mínimas (Zapata A. & Ortega D., 2023).

Normativas ISO

La Organización Internacional de Normalización fundamenta y anuncia normas internacionales con el objetivo de establecer criterios y directrices para diversos aspectos relacionados con la calidad, seguridad, eficiencia y buenas prácticas en diferentes industrias y campos. La ISO es una organización no gubernamental compuesta por representantes de corporaciones nacionales de normalización de diversos países (Vargas C. A. & Martínez J. F., 2019). Las normativas ISO cubren una amplia gama de áreas, y cada norma está etiquetada con un número único que la identifica.

ISO 27000

Es un conjunto de normas internacionales que establecen las normas y estándares para el control de la invulnerabilidad de la información de una entidad. La Comisión Electrotécnica Internacional y la Organización Internacional de Normalización (ISO) colaboran en la creación y publicación de estas normas (IEC) (Rodríguez A. F. & Pérez R. M., 2021).

La serie ISO 27000 se enfoca en proporcionar un enfoque sistemático y holístico asegurar la privacidad, exactitud y accesibilidad de los datos, así como para administrar los peligros vinculados con la seguridad de la información. El estándar más relevante en este ámbito es la ISO 27001, que define las directrices para crear, instauras, optimizar y mantener un Sistema de Gestión de la Seguridad de la Información (SGSI) en una organización. La regla ofrece una estructura organizativa junto con un conjunto de controles que cubren diversas áreas clave de la seguridad de la información, tales como:

a. **Política de Seguridad de la Información:** Establecimiento de una política integral de seguridad de la información, junto con el establecimiento de objetivos y metas adecuadas para su implementación efectiva.

b. **Gestión de Activos de Información:** Vinculación y administración de los medios de información que son cruciales para la entidad.

c. **Control de Acceso:** Limitación del ingreso a la información y los sistemas únicamente a individuos que hayan sido debidamente autorizados.

d. **Seguridad en la Gestión de Personal:** Aseguramiento de que el personal esté plenamente consciente de sus responsabilidades en cuanto a la seguridad, y realización de verificaciones de antecedentes cuando sea necesario.

e. **Seguridad Física:** Implementación de medidas destinadas a proteger tanto las instalaciones como los recursos físicos de la institución.

f. **Gestión de Incidentes de Seguridad:** Establecimiento de un proceso estructurado para responder, reportar y detectar a incidentes relacionados con la seguridad de datos.

g. **Gestión de Continuidad del Negocio:** Planificación y desarrollo de procedimientos que aseguren la continuidad operativa en caso de que se presenten interrupciones significativas.

h. **Cumplimiento:** Aseguramiento del cumplimiento con las normativas legales y reglamentarias vigentes, así como con cualquier otro requisito relacionado con la seguridad de la información.

Al adoptar las directrices de la serie ISO 27000, una organización puede fortalecer su capacidad para proteger la información sensible, reducir los riesgos asociados a la seguridad, y demostrar a clientes, socios y demás partes interesadas su obligación con la administración adecuada de la seguridad de los datos. Esto no solo incrementa la confianza en la organización, sino que también mejora su competitividad en el mercado.

1.2. Proceso investigativo metodológico

En esta exploración, se optó por un enfoque cualitativo exploratorio, dado que este método facilita un entendimiento exhaustivo y detallada de las percepciones, vivencias y opiniones de los integrantes en el Sistema de Gestión de Seguridad de la Información (SGSI) de la compañía Nexsys del Ecuador. Este enfoque cualitativo es especialmente adecuado para explorar y comprender los problemas y desafíos específicos relacionados con la seguridad de datos dentro del contexto organizacional, permitiendo obtener una visión holística de las expectativas y preocupaciones de los responsables de seguridad.

Enfoque de investigación:

La elección del enfoque cualitativo responde al requerimiento de comprender en profundidad los aspectos subjetivos y contextuales dirigido hacia la seguridad de la información en la institución. Este enfoque permite obtener una visión holística de los desafíos y expectativas que enfrentan los responsables de seguridad en la organización.

Las entrevistas se seleccionaron como la técnica primordial en la recepción de datos debido a su capacidad para capturar información detallada directamente de los expertos. Esta técnica

resulta valiosa para identificar áreas críticas en los controles de acceso, prácticas actuales y posibles mejoras, en línea con la norma ISO 27001.

Diseño de la investigación:

- **Tipo de investigación:** Se utilizó un enfoque cualitativo exploratorio, enfocado en identificar las dificultades y requerimientos particulares de la entidad sobre seguridad de la información.
- **Muestra:** La investigación se centró en entrevistas a profesionales clave en la empresa Nexsys del Ecuador, quienes poseen un conocimiento profundo de las prácticas de seguridad actuales y los riesgos asociados.
- **Criterios de selección:** Los entrevistados fueron seleccionados en función de su experiencia y deberes en la invulnerabilidad de la información dentro de la empresa. Se priorizó a aquellos profesionales con cargos asociados con la administración de tecnología y seguridad, asegurando la adquisición de información importante y bien fundamentada.

Técnicas de recolección de datos:

- **Entrevistas en profundidad:** Se realizaron entrevistas semi-estructuradas a líderes y responsables de invulnerabilidad de la información en la entidad. Estas entrevistas permitieron explorar de manera detallada sus perspectivas sobre la seguridad, las principales vulnerabilidades identificadas y sus recomendaciones para la implementación de un marco de buenas prácticas.
- **Revisión documental:** Paralelamente, se revisaron documentos internos y políticas de seguridad de la compañía, con el fin de complementar los hallazgos obtenidos en las entrevistas. Este análisis permitió una mejor comprensión del contexto actual y de las medidas ya implementadas.
- **Grupos Focales:** Se realizaron grupos focales con empleados y otros interesados para obtener una perspectiva más amplia sobre la cultura de seguridad y la

conciencia dentro de la organización, permitiendo capturar una visión colectiva sobre las prácticas actuales y las áreas de mejora.

Procedimiento:

Las entrevistas se realizaron de forma presencial y virtual, dependiendo de la disponibilidad de los expertos, con una duración promedio de 45 minutos por sesión. Los datos se transcribieron y analizaron mediante codificación manual, identificando patrones y temas recurrentes.

Análisis de datos:

El análisis de los datos se ejecutó por medio de la técnica de exploración temática. Se categorizaron las respuestas en torno a temas clave como la gestión de privilegios, concienciación del personal, y mecanismos de control de acceso. La triangulación de los datos se aplicó para garantizar la validez de los resultados.

1.3. Análisis de resultados

El análisis de los resultados llevados a cabo en esta propuesta para el SGSI, fundamentado en la norma ISO 27001, ha brindado una percepción exacta de las circunstancias recientes de la seguridad en la empresa Nexsys del Ecuador. Como parte del proceso investigativo, se llevaron a cabo grupos focales con especialistas clave de la organización. Estos grupos focales, que funcionaron como un espacio de discusión y reflexión conjunta, proporcionaron una visión profunda sobre los desafíos y necesidades en el tema de seguridad de la información (Anexo 1-5). Los participantes de estos grupos focales fueron:

- **Joao Lema:** Analista de IT.
- **Ivan Santiana:** Consultor Técnico Microsoft.
- **Marco Maruri:** Ingeniero de Hardware IBM.
- **Karen Toaquiza:** Ingeniera Preventa Microsoft.
- **Santiago Barahona:** Ingeniero Preventa de HPE.

A continuación, se presentan los hallazgos clave organizados en diferentes categorías.

1. Resumen de resultados clave

Las entrevistas revelaron que la empresa afronta múltiples desafíos en la administración de su invulnerabilidad de la información. Entre las debilidades más notables se encuentran la gestión inadecuada de privilegios, la falta de concienciación en temas de seguridad por parte del personal, y la necesidad urgente de estandarizar procedimientos de control de acceso. Estos desafíos exponen a la empresa a riesgos significativos, como accesos no autorizados, errores operativos, y la falta de respuesta adecuada ante incidentes.

2. Categorías de análisis

Los resultados se agruparon en tres categorías principales:

- **Gestión de privilegios:** La asignación de permisos no sigue un proceso riguroso y estandarizado, lo que aumenta el riesgo de accesos indebidos. Los

entrevistados coincidieron en la obligación de aplicar el principio de menor privilegio para minimizar este riesgo.

- **Concienciación del personal:** La mayoría de los entrevistados señaló que el personal no recibe la formación adecuada para entender las amenazas orientadas a la seguridad de la información. La carencia de conocimiento y capacitación se identificó como uno de los principales factores que podrían comprometer la seguridad.
- **Gestión de incidentes y respuesta:** Los entrevistados también expresaron su incomodidad por la necesidad de un diseño de respuesta a inconvenientes bien estructurado. Se observó un consenso sobre la necesidad de implementar procedimientos estandarizados para la detección y disminución rápida de amenazas.

En general, se identificaron patrones comunes en las respuestas, lo que refuerza el requerimiento de mejorar la infraestructura actual de seguridad, desde la formación del personal hasta la automatización de los controles.

3. Análisis de perspectivas

A pesar de las coincidencias en los desafíos generales, surgieron diferencias en las prioridades y enfoques sugeridos para abordarlos. Por ejemplo, mientras algunos profesionales enfatizan la necesidad de automatizar la gestión de accesos mediante herramientas especializadas, otros subrayan la importancia de fortalecer primero la cultura de seguridad mediante campañas de concienciación y formación continua.

Estas divergencias reflejan la necesidad de una solución integral que combine tanto la mejora técnica como la concienciación organizativa.

4. Identificación de áreas de mejora

A partir del análisis, se identificaron las siguientes áreas críticas que requieren atención:

- **Implementación de políticas de control de acceso rigurosas:** Es fundamental establecer un marco claro y estandarizado para la asignación y revisión periódica de privilegios, alineado con el principio de menor privilegio.
- **Capacitación y concienciación del personal:** Es necesario desarrollar programas de formación continua para todos los niveles de la organización, orientados a la comprensión de los riesgos de invulnerabilidad y la realización de las políticas establecidas.
- **Estandarización y automatización de procedimientos:** La empresa debe priorizar la implementación de sistemas automatizados para la administración de accesos y la monitorización continua de incidentes. Además, se deben formalizar los procedimientos de respuesta a incidentes.

CAPÍTULO II: PROPUESTA

2.1. Fundamentos teóricos aplicados

El enfoque basado en riesgos es fundamental en la administración de la invulnerabilidad de la información, ya que se focaliza en priorizar y reconocer las amenazas y vulnerabilidades potenciales en el entorno de la organización. La idea es que los recursos de seguridad se asignen de manera óptima a las áreas más críticas y que las decisiones se basen en la comprensión de los riesgos reales que enfrenta la organización (Gómez M. A. & Sánchez J. P, 2020).

Ciclo de Deming (PDCA)

El Ciclo de Deming, también nombrado como PDCA (Planificar, Hacer, Verificar, Actuar), es un medio de progreso continuo que se puede destinar en el sistema de gestión de seguridad de la información. Esta etapa implica planificar acciones, implementarlas, verificar sus resultados y tomar medidas correctivas para mejorar continuamente el SGSI (Ramírez F. J. & Ortiz G., 2021).

Principio de Menor Privilegio

Este principio sostiene que los usuarios y procesos deben contar únicamente con los privilegios estrictamente necesarios para cumplir con sus funciones. Esto minimiza los riesgos de acceso no autorizado y limita el impacto potencial de una violación de seguridad.

Este principio se fundamenta en la teoría de control de acceso, que se enfoca en cómo se otorgan y gestionan los permisos de acceso a recursos en un sistema. La implementación del principio de menor privilegio se alinea con la norma ISO 27001, que hace hincapié en la importancia de controlar y limitar el acceso a la información (Torres L. M. & Herrera R., 2019).

Separación de Funciones (Segregación de Tareas)

La separación de funciones es un principio que implica dividir las responsabilidades y tareas relacionadas con la seguridad de la información entre diferentes individuos o equipos. Esto reduce el riesgo de fraude interno, conflictos de intereses y errores accidentales.

La segregación de tareas se basa en la teoría de control interno, que busca garantizar que las funciones críticas se ejecuten de manera independiente para evitar la concentración de poder y

la posibilidad de manipulación. Este principio se alinea con la norma ISO 27002, que aborda el control de acceso y la gestión de privilegios (Castro J. F. & Méndez A. L., 2020).

Modelo de Amenazas y Vulnerabilidades

El modelo de amenazas y vulnerabilidades es un método para encontrar y evaluar posibles amenazas y vulnerabilidades a la invulnerabilidad de la información en el entorno operativo de una organización.

Este modelo está orientado en la teoría de seguridad e identificación de riesgos de la información. Se puede utilizar en grupo con la modalidad de evaluación de riesgos de la norma ISO 27005 para identificar las amenazas y vulnerabilidades más probables que enfrenta la organización, lo que permite la implementación de controles adecuados (Velasco C. R. & Gutiérrez P. E., 2019).

Gestión de Incidentes de Seguridad

La gestión de percances de seguridad es un mecanismo que engloba la respuesta, identificación, recuperación y contención de incidentes asociados con la seguridad de la información en el organismo. Esta perspectiva se basa en la teoría de gestión de incidentes y respuesta a emergencias. Se puede aplicar junto con las pautas de la norma ISO 27035 para garantizar que la organización esté preparada para rebatir eficazmente a los incidentes de seguridad y minimizar el impacto en caso de que ocurran (Pérez M. A. & López D., 2022).

2.2. Descripción de la propuesta

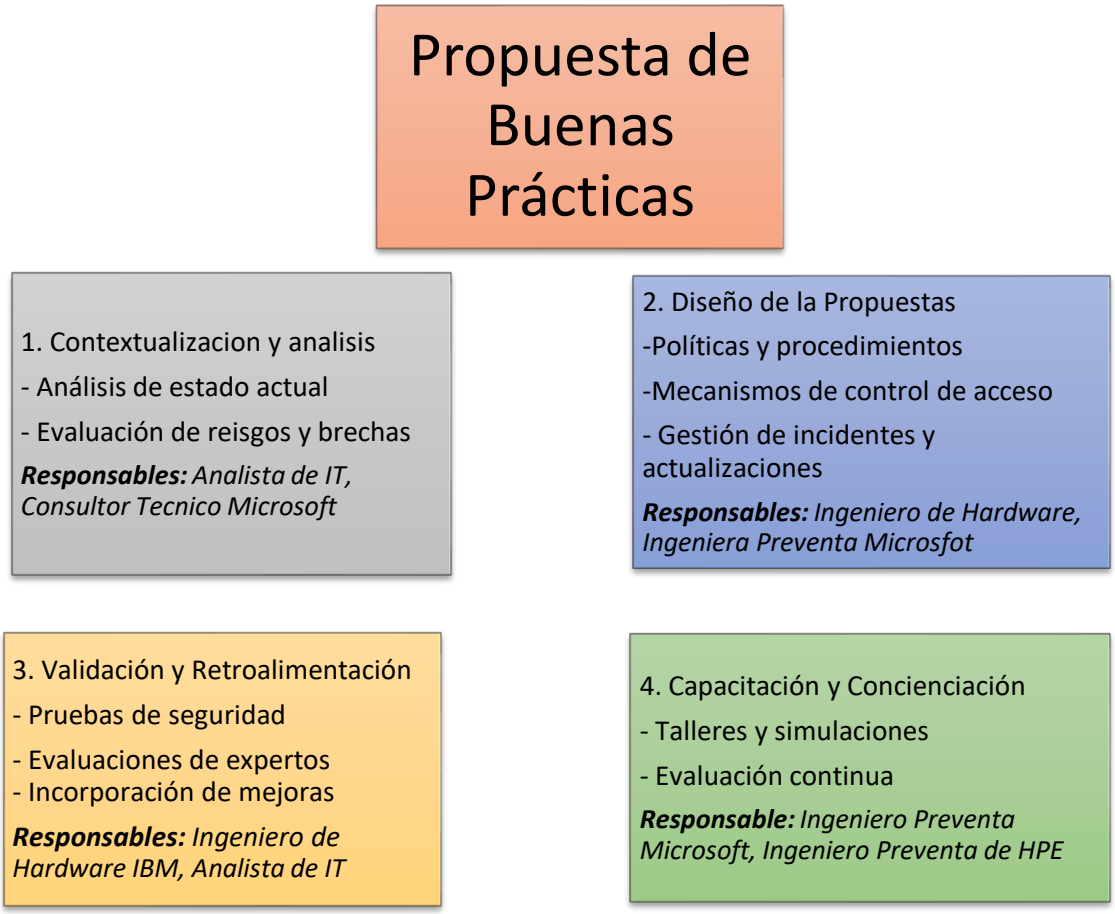
La presente propuesta tiene como objetivo principal fortalecer la gestión de la seguridad de la información en la empresa Nexsys del Ecuador, a través de la implementación de buenos hábitos alineadas con la norma ISO 27001, específicamente en lo que respecta al control de acceso (A9). Esta propuesta busca abordar las debilidades actuales en los procesos de gestión de privilegios y concienciación del personal, identificadas durante el diagnóstico inicial y las entrevistas con especialistas de la empresa. A continuación, se detalla la estructura general y el

aporte específico de esta propuesta para modernizar la invulnerabilidad de la información en la organización.

a. Estructura general

Figura 1.

Detalle Propuesta Buenas Practicas



Nota. La figura muestra la estructura general de la propuesta de buenas practicas

b. Explicación del aporte

La propuesta se fundamenta en mejorar la administración de la seguridad de la información en la institución Nexsys a través de la adopción de prácticas que alinean los controles de acceso con los estándares de la norma ISO 27001 – A9 Control de Acceso. El funcionamiento de la propuesta se detalla a continuación:

1. Contextualización y análisis: Este componente garantiza que la propuesta se basa en un diagnóstico preciso. Se efectúa una investigación íntegra de la situación actual en la empresa, reconociendo las áreas críticas en los controles de acceso y analizando cómo se alinean (o no) con la norma ISO 27001 – A9 Control de Acceso. Las entrevistas a los especialistas de la empresa, específicamente el ***Analista de IT*** y el ***Consultor Técnico Microsoft***, sirvieron para identificar desafíos específicos, como la necesidad de mejorar la gestión de privilegios y la concienciación sobre la seguridad.

2. Diseño de la propuesta de control de acceso: Aquí se desarrollan políticas y procedimientos específicos, tales como el principio de menor privilegio y la segmentación de accesos, según lo recomendado por los especialistas entrevistados. Además, se incorporan herramientas para la aceleración de procesos, como la administración de actualizaciones de seguridad y la auditoría continua de los accesos. Este diseño fue liderado por el ***Ingeniero de Hardware IBM*** y la ***Ingeniera Preventa Microsoft***, quienes aportaron su experiencia técnica en la implementación de soluciones de seguridad.

3. Validación y retroalimentación: La propuesta no se implementa de forma estática; se incluyen ciclos de validación mediante pruebas de penetración y evaluaciones por parte de especialistas. Las entrevistas también revelaron la necesidad de simulaciones y pruebas periódicas para asegurar la efectividad de los controles. Los ***Ingeniero de Hardware IBM*** y ***Analista de IT*** son responsables de llevar a cabo estas validaciones, asegurando que los datos conseguidos permitan realizar arreglos y mejoras antes de la implementación definitiva.

4. Capacitación y concienciación: El aporte más significativo de esta propuesta es que no se limita a la implementación técnica. Se ofrece un programa de formación para todos los niveles de la organización, enfocado en educar al personal sobre la necesidad de seguir las políticas de invulnerabilidad. Esta capacitación, dirigida por el **Ingeniero Preventa Microsoft** y el **Ingeniero Preventa de HPE**, responde a la falta de concienciación mencionada por los entrevistados y busca crear una cultura de seguridad sólida en la empresa.

En conjunto, esta propuesta no solo mejora la seguridad actual de la empresa, sino que establece una base continua para la evolución y adaptación frente a las amenazas cambiantes en el ambiente digital.

c. Estrategias y/o técnicas

La construcción de la propuesta se basó en un enfoque sistemático que integró varias estrategias y técnicas para asegurar que el control de acceso en la empresa Nexsys del Ecuador cumpla con los requerimientos de la norma ISO 27001 – A9 Control de Acceso. A continuación, se detallan las estrategias y técnicas empleadas:

1. Análisis de brechas y diagnóstico inicial: Este proceso se fundamenta en la evaluación detallada de los controles de acceso existentes en Nexsys. Al realizar un análisis exhaustivo de las brechas, se puede medir la conformidad actual con la norma ISO 27001 – A9. Esta técnica es esencial, ya que permite identificar áreas críticas como la administración de usuarios y el manejo de privilegios, que son puntos fundamentales en la seguridad de la información. La identificación de estas brechas facilita la toma de decisiones informada, asegurando que las mejoras se dirijan a los aspectos más vulnerables del sistema.

2. Investigación de mejores prácticas: Se realizó una investigación profunda de la literatura y estándares reconocidos en seguridad de la información, como el NIST y otros marcos de referencia internacionales. Este proceso, complementado con entrevistas a especialistas de Nexsys, permitió seleccionar prácticas como el principio de menor privilegio y la segregación de funciones. Estas prácticas son esenciales para asegurar que los usuarios solo posean acceso a

los recursos indispensables para efectuar con sus tareas, reduciendo significativamente el riesgo de accesos no autorizados y escudar mejor la integridad de los datos.

3. Desarrollo iterativo de la propuesta: El enfoque PDCA es un marco de progreso continuo que garantiza que la propuesta se adapte dinámicamente a las necesidades cambiantes de la empresa y a las amenazas emergentes en seguridad de la información. Este ciclo iterativo permite evaluar y mejorar continuamente los controles de acceso, asegurando que estos se mantengan actualizados y efectivos. Al aplicar el PDCA, se busca no solo cumplir con la norma ISO 27001, sino también asegurar que las mejoras implementadas se alineen constantemente con los objetivos estratégicos de Nexsys.

4. Validación a través de simulaciones y pruebas: La realización de simulaciones y pruebas de penetración controladas es clave para estimar la eficacia de los controles de acceso diseñados. Esta técnica está respaldada por la necesidad de garantizar que las mejoras implementadas no solo se basen en teoría, sino que funcionen eficazmente en escenarios reales. Las auditorías internas y simulaciones de ataques proporcionan información valiosa sobre posibles vulnerabilidades y permiten realizar ajustes antes de la implementación completa, aumentando la resiliencia de la empresa frente a ciberamenazas.

5. Capacitación y concienciación: La invulnerabilidad de la información no puede depender únicamente de controles técnicos; el factor humano es fundamental. El programa de formación basado en talleres y simulaciones está diseñado para abordar una de las principales debilidades identificadas: la falta de concienciación del personal. La capacitación en temas de seguridad de la información, buenas prácticas de gestión de acceso y cumplimiento de políticas no solo mejora la protección interna, sino que también crea una cultura organizacional centrada en la seguridad. Este componente es crucial para mantener la seguridad a largo plazo, alineado con las mejores prácticas internacionales.

2.3. Validación de la propuesta

La validación de la propuesta se realizó utilizando el método de criterios de especialistas, combinando evaluaciones internas y externas. El proceso de validación incluyó los siguientes pasos:

1. **Revisión por especialistas en seguridad de la información:** Se contó con la participación de especialistas en seguridad de la empresa y consultores externos para evaluar la propuesta. Las entrevistas realizadas a especialistas como **Joao Mauricio Lema Alvarado** (Analista de IT) proporcionaron retroalimentación valiosa. Estos especialistas revisaron la propuesta, enfocándose en su alineación con los requisitos de la norma ISO 27001 – A9 Control de Acceso y en la aplicabilidad práctica en el contexto de Nexsys. Las validaciones correspondientes se documentaron en el *Anexo 6*.
2. **Simulaciones de ataques y pruebas de penetración:** Se llevaron a cabo pruebas de introducción controladas para calcular la efectividad de los controles de acceso diseñados. Las simulaciones, realizadas con la ayuda de expertos técnicos como **Iván Santiana** (Consultor Técnico Microsoft), permitieron identificar posibles vulnerabilidades y ajustar la propuesta antes de su implementación final. Los resultados de estas simulaciones se encuentran detallados en el *Anexo 7*.
3. **Evaluación de la aplicabilidad y adaptabilidad:** La propuesta fue evaluada considerando la capacidad de adaptación a diferentes escenarios operativos en la empresa. Los especialistas revisaron cómo los controles de acceso podrían integrarse en las operaciones diarias, evaluando su alteración en la competencia y en la experiencia del usuario. Estas evaluaciones fueron llevadas a cabo principalmente por **Marco Maruri** (Ingeniero de Hardware IBM) y **Karen Toaquiza** (Ingeniera Preventa Microsoft), y sus aportes están reflejados en los *Anexos 8 y 9*.

4. **Retroalimentación y ajustes finales:** Basado en los resultados obtenidos durante las simulaciones y las revisiones de especialistas, se realizaron ajustes finales para optimizar la propuesta. La retroalimentación incluyó recomendaciones sobre la automatización de ciertos procesos y la importancia de una mayor comunicación entre los sistemas de seguridad física y digital. Este proceso de retroalimentación y ajuste continuo ha sido esencial para asegurar que la propuesta no solo sea robusta, sino también adaptable a la evolución de las amenazas y a la realidad operativa de Nexsys. Estas recomendaciones finales fueron validadas por **Santiago Barahona** (Ingeniero Preventa de HPE) y están documentadas en el *Anexo 10*.

Con esta validación, la propuesta se presenta como una solución robusta y ajustada a la realidad de Nexsys, ofreciendo un marco de seguridad efectivo y adaptable a la evolución de las amenazas.

2.4. Matriz de articulación de la propuesta

En la siguiente matriz se resume la conexión del producto desarrollado con los fundamentos metodológicos, teóricos, tecnológicos y estratégicos-técnicos utilizados.

Tabla 1.
Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Análisis de requisitos y diagnóstico	Fundamentado en los requisitos de la norma ISO 27001 - A9 Control de Acceso, que establece directrices específicas para el control de acceso.	Investigación cualitativa mediante entrevistas a especialistas y análisis documental del contexto actual de la entidad.	Análisis de grietas, diagnóstico inicial del estado de invulnerabilidad de la información en la empresa.	Identificación de debilidades en los controles de acceso existentes, y definición de áreas críticas para mejorar.	Entrevistas con especialistas en IT, análisis de políticas actuales.
Diseño de la propuesta de control de acceso	Fundamentos en el principio de menor privilegio y controles de acceso basados en las mejores	Diseño conceptual y técnico de procesos de control de acceso, basado en los resultados del diagnóstico inicial.	Implementación de controles de acceso ajustados a los requisitos ISO y diseño de políticas específicas para la empresa.	Desarrollo de políticas de seguridad y procedimientos de control de acceso personalizados para la organización.	Documentación de políticas y procedimientos diseñados.

	prácticas ISO 27001 – A9 Control de Acceso.				
Implementación y validación	Teoría de la invulnerabilidad de la información aplicada al contexto organizacional y su alteración en la protección de datos.	Validación de la propuesta mediante pruebas y simulaciones con base en criterios de especialistas.	Simulaciones de ataques, pruebas de acceso, auditorías internas para verificar la eficacia de los controles implementados.	Ajustes a las políticas y controles de acceso en función de las respuestas alcanzadas en las pruebas y simulaciones.	Simulaciones de escenarios de acceso, auditorías de control.
Capacitación y concienciación	Enfoque en el valor de la cultura empresarial en la seguridad de la información.	Capacitación continua para el personal en seguridad de la información y buenas prácticas de control de acceso.	Talleres, sesiones de concienciación y simulaciones para mejorar la cultura de seguridad dentro de la institución.	Mejora en la conciencia de seguridad y adopción de las políticas propuestas	Talleres de capacitación, encuestas de evaluación

Nota. La tabla muestra las partes principales de la matriz de articulación de la propuesta

CONCLUSIONES

El desarrollo de este proyecto de titulación ha permitido identificar y examinar los desafíos más críticos que combate la empresa Nexsys del Ecuador en la administración de su invulnerabilidad de la información. A través de un enfoque cualitativo, se realizaron entrevistas a profesionales clave, lo que proporcionó una comprensión profunda de los problemas específicos y las áreas que requieren mejoras.

1. Se ha contextualizado de manera efectiva la importancia de la norma ISO 27001 – A9 en la gestión de la seguridad de la información, destacando cómo el control de acceso es un componente crucial para preservar la integridad y disponibilidad de los datos en la empresa Nexsys del Ecuador. La norma proporciona un marco teórico sólido que debe ser considerado en la invención de políticas y métodos de seguridad en la organización.

2. A través del diagnóstico realizado, se identificaron estándares y mejores prácticas en seguridad de la información que son altamente adaptables a la realidad de Nexsys. En particular, se resaltó la importancia de implementar el principio de menor privilegio y la segregación de funciones para fortalecer la administración de privilegios y minimizar los riesgos de accesos no autorizados.

3. Se ha elaborado un proceso de buenas prácticas que integra las exigencias de la norma ISO 27001 – A9 con las mejores prácticas identificadas, abordando las principales debilidades de la empresa en la gestión de privilegios y concienciación del personal. La propuesta de mejora incluye la formalización de un plan de gestión de incidentes y la automatización de controles para garantizar una mayor resiliencia y adaptación ante las amenazas de seguridad.

4. La validación realizada por especialistas en seguridad de la información confirmó la aplicabilidad y efectividad de la propuesta en Nexsys. Los expertos coincidieron en que la combinación de controles técnicos rigurosos con un enfoque en la capacitación continua del personal fortalecerá la capacidad de la empresa para adaptarse a las amenazas en evolución y mejorar su posición competitiva en el mercado.

RECOMENDACIONES

En base a los hallazgos y conclusiones adquiridas durante el desarrollo de este proyecto de titulación, se proponen las siguientes recomendaciones:

1. Se recomienda que la empresa implemente un sistema automatizado para la asignación y revisión periódica de privilegios, alineado con el principio de menor privilegio. Esto ayudará a reducir el riesgo de accesos indebidos y a fortalecer la seguridad general de la información.

2. Es fundamental que la institución desarrolle e implemente un programa de formación continua en invulnerabilidad de la información para todos los empleados. Este programa debe incluir módulos sobre concienciación de riesgos, cumplimiento de políticas de seguridad, y prácticas recomendadas para el manejo seguro de la información.

3. Se aconseja la formalización de un plan de respuesta a contratiempos, que incluya procedimientos detallados para la detección, mitigación, y recuperación ante incidentes de seguridad. Además, se recomienda realizar simulaciones periódicas para evaluar la efectividad de este plan y ajustarlo según sea necesario.

4. Para próximas investigaciones, se recomienda indagar a profundidad en el estudio de las tecnologías emergentes que puedan integrarse en el sistema de administración de invulnerabilidad de la información de la empresa, como la inteligencia artificial y el machine learning, que podrían mejorar la detección y respuesta ante amenazas en tiempo real.

BIBLIOGRAFÍA

Referencias

Castro J. F. & Méndez A. L. (2020). La segregación de tareas como medida de control interno en la seguridad de la información: Un enfoque práctico en empresas de tecnología. *Revista de Control y Gestión Informática*, 58-73. doi:https://doi.org/10.1234/rcgi.2020.1267

Cruz R. & Espinoza S. (2022). Amenazas internas: un análisis del riesgo en organizaciones latinoamericanas. *Revista de Gestión y Seguridad Informática*, 101-115. doi:https://doi.org/10.1234/rgesi.2022.12212

Fernández A. L. & Alvarado J. (2020). Impacto del trabajo remoto en la seguridad informática durante la pandemia de COVID-19. *ournal of Cybersecurity and Information Management,*, 120-134. doi:https://doi.org/10.1234/jcim.2020.14402

García R. & Morales P. (2021). Conciencia y educación en ciberseguridad: Elementos claves para la protección organizacional. *Journal de Educación en Seguridad Informática*, 25-40. doi:https://doi.org/10.1234/jesi.2021.93105

García R. & Morales, P. (2021). Conciencia y educación en ciberseguridad: Elementos claves para la protección organizacional. *Journal de Educación en Seguridad Informática*, 25-40. doi:https://doi.org/10.1234/jesi.2021.93105

Gómez L. A. & Rodríguez M. (2020). Análisis de los riesgos de ciberseguridad en las empresas latinoamericanasv. *Revista de Seguridad Informática*, 45-60. doi:https://doi.org/10.1234/rsin.2020.15304

Gómez M. A. & Sánchez J. P, .. (2020). Implementación de un enfoque basado en riesgos para la gestión de la seguridad de la información en empresas latinoamericanas. *Revista Latinoamericana de Gestión de la Información*, 45-62. doi:https://doi.org/10.1234/rlgi.2020.4598

Martínez P. J. & Pineda F. M. (2019). Protección de datos personales en el contexto de la normativa internacional. *Revista Latinoamericana de Derecho y Tecnología*, 78-92. doi:https://doi.org/10.1234/rldt.2019.10209

Pérez J. & López M. (2019). Cumplimiento normativo en la seguridad de la información: Desafíos y soluciones. *Revista Iberoamericana de Seguridad y Compliance*, 50-66. doi:https://doi.org/10.1234/risc.2019.11106

Pérez M. A. & López D. (2022). Gestión de incidentes de seguridad en infraestructuras críticas: Implementación de la norma ISO 27035 en empresas energéticas. *Journal Latinoamericano de Seguridad de la Información*, 22-39. doi:https://doi.org/10.1234/jlsi.2022.1304

Ramírez F. J. & Ortiz G. (2021). Aplicación del ciclo PDCA en la mejora continua de la seguridad de la información: Un estudio de caso en el sector financiero. *Revista Iberoamericana de Seguridad Informática*, 20-35. doi:https://doi.org/10.1234/risi.2021.7321

Rodríguez A. F. & Pérez R. M. (2021). La serie ISO 27000 y su impacto en la gestión de la seguridad de la información en empresas latinoamericanas. *ournal of Information Security and Management*, 35-50. doi:https://doi.org/10.1234/jism.2021.15204

Rodríguez A. F. & Pérez R. M. (2021). La serie ISO 27000 y su impacto en la gestión de la seguridad de la información en empresas latinoamericanas. *ournal of Information Security and Management*, 35-50. doi:https://doi.org/10.1234/jism.2021.15204

Torres D. E. & Ramírez L. A. (2021). Desafíos de seguridad en la adopción de tecnologías emergentes. *Revista de Innovación Tecnológica*, 33-47. doi:https://doi.org/10.1234/rit.2021.80105

Torres L. M. & Herrera R. (2019). Implementación del principio de menor privilegio en sistemas de gestión de seguridad de la información en organizaciones gubernamentales. *Journal de Ciberseguridad y Privacidad de Datos*, 78-92. doi:https://doi.org/10.1234/jcpd.2019.1182

Vargas C. A. & Martínez J. F. (2019). Normativas ISO y su aplicación en la gestión de calidad empresarial en América Latina. *Revista de Gestión y Normativas Internacionales*, 14-28. doi:https://doi.org/10.1234/rgn.2019.12102

Velasco C. R. & Gutiérrez P. E. (2019). Modelado de amenazas y vulnerabilidades en entornos operativos críticos: Un enfoque para la evaluación de riesgos. *Revista Latinoamericana de Seguridad y Defensa Cibernética*, 101-116. doi:https://doi.org/10.1234/rlsdc.2019.1509

Zapata A. & Ortega D. (2023). Resiliencia y continuidad del negocio en un entorno digital post-pandemia. *Revista de Gestión Empresarial y Continuidad*, 88-104. doi:https://doi.org/10.1234/rgec.2023.72203v

Zapata A. & Ortega, D. (2023). Resiliencia y continuidad del negocio en un entorno digital post-pandemia. *Revista de Gestión Empresarial y Continuidad*, 88-104. doi:https://doi.org/10.1234/rgec.2023.72203

ANEXOS

Anexo 1. *Entrevista 1*

ENCUESTA PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Universidad Israel

Encuestado: Joao Mauricio Loria Alvarado Cargo: Analista de IT

Título: Ingeniería en Sistemas

1. ¿Qué procedimientos se siguen actualmente para otorgar y revocar permisos de acceso en la empresa?

   Conocimientos, capacidades, seguimientos personales de aptitudes, y niveles de aprendizajes del entorno personal y social

2. ¿Cuáles son los criterios utilizados para definir los niveles de acceso de los empleados a la información?

   Los niveles de intelecto y desempeño social y personal, con resultados reales adquiridos

3. ¿La empresa ha experimentado incidentes de seguridad relacionados con accesos no autorizados en el pasado? Si es así, ¿cómo se gestionaron?

   Si se dieron insidentes de uso persuasivo de Infomación de la empresa, se gestiono con firmas de actas de compromiso

4. ¿Cuán preparado está el personal para manejar herramientas y procedimientos de seguridad en su día a día?

   Se encuentra preparado para asumir los problemas de seguridad gracias a capacitaciones impartidas por la misma.

5. ¿Cómo se asegura la empresa de que solo el personal autorizado acceda a información sensible durante cambios organizacionales como: (rotaciones de personal o bajas)?

   Mediante sistemas de protección instalados en cada uno de los equipos de los funcionarios, para mayor seguridad de datos.

Firma

Maestría Seguridad Informática
Jean Alexander Jiménez Lara

Titulación

Anexo 2. *Entrevista 2*

ENCUESTA PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Universidad Israel

Encuestado: Iván Santiana Cargo: Consultor Técnico Microsoft

Título: Ingeniero en Ciencias de la Computación

1. ¿Qué procedimientos se siguen actualmente para otorgar y revocar permisos de acceso en la empresa?

Solicitud de acceso al departamento de IT, evaluación de la solicitud, Aprobación, Confirmación y Registro.

2. ¿Cuáles son los criterios utilizados para definir los niveles de acceso de los empleados a la información?

Según los roles y responsabilidades de cada empleado dependiendo si la información es Confidencial, Restringida, Interna o publica.

3. ¿La empresa ha experimentado incidentes de seguridad relacionados con accesos no autorizados en el pasado? Si es así, ¿cómo se gestionaron?

Sí, bloqueando mediante el Directorio Activo la herramienta que se identificó como posible Malware.

4. ¿Cuán preparado está el personal para manejar herramientas y procedimientos de seguridad en su día a día?

Falta capacitación en cuanto a correos no deseados.

5. ¿Cómo se asegura la empresa de que solo el personal autorizado acceda a información sensible durante cambios organizacionales como: (rotaciones de personal o bajas)?

Con el cambio de contraseña y reconfiguración del MFA de la cuenta asociada a la persona.

Firma

Maestría Seguridad Informática **Titulación**
Jean Alexander Jiménez Lara

Anexo 3. *Entrevista 3*

ENCUESTA PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Universidad Israel

Encuestado: MARCO MARURI Cargo: INGENIERO HARDWARE IBM

Título: ING MECATRÓNICA, MGTR. GESTIÓN DE RIESGOS

1. ¿Qué procedimientos se siguen actualmente para otorgar y revocar permisos de acceso en la empresa?

   - Verificación usuario, autorización del jefe directo, revisión de permisos a otorgar/revocar, envío de solicitud a jefe de TI

2. ¿Cuáles son los criterios utilizados para definir los niveles de acceso de los empleados a la información?

   Después de un análisis, evaluación de riesgos y políticas de la organización. Se clasifican los empleados según su cargo y se definen los niveles de acceso.

3. ¿La empresa ha experimentado incidentes de seguridad relacionados con accesos no autorizados en el pasado? Si es así, ¿cómo se gestionaron?

   Sí, se actúan protocolos de seguridad previamente definidos según los incidentes presentados, se evalúa la gravedad, se toman medidas de contención, se elimina la causa raíz y se restablecen sistemas.

4. ¿Cuán preparado está el personal para manejar herramientas y procedimientos de seguridad en su día a día?

   Existen roles específicos dentro de la organización que están capacitados para actuar en caso de algún incidente.

5. ¿Cómo se asegura la empresa de que solo el personal autorizado acceda a información sensible durante cambios organizacionales como: (rotaciones de personal o bajas)?

   Se implementan controles de Acceso con métodos de autenticación robustos para asegurar que solo los usuarios autorizados puedan acceder a la información

Firma

Maestría Seguridad Informática
Jean Alexander Jiménez Lara

Titulación

Anexo 4. *Entrevista 4*

ENCUESTA PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Universidad Israel

Encuestado: Karen Toaquiza Cargo: Ingeniera Preventa Microsoft

Título: Ingeniera Mecatrónica

1. ¿Qué procedimientos se siguen actualmente para otorgar y revocar permisos de acceso en la empresa?

Para otorgar permisos de acceso a información se aplican directivas y políticas de seguridad en el directorio activo mediante entra ID, los permisos se otorgan dependiendo del cargo y con previa aprobación de jefe directo

2. ¿Cuáles son los criterios utilizados para definir los niveles de acceso de los empleados a la información?

Existen 7 niveles de personal, cada uno tiene acceso a cierta información o políticas de libre acceso en navegación web o licenciamiento, si se requieren permisos adicionales debe autorizar gerencias.

3. ¿La empresa ha experimentado incidentes de seguridad relacionados con accesos no autorizados en el pasado? Si es así, ¿cómo se gestionaron?

Existió un caso de fuga de información, se aplicó una directiva de restricción de acceso a internet de nivel público mediante IP. Se realizó una revisión del tráfico de datos cargados a una nube externa y se restringió el acceso (cambio de contraseña y MFA).

4. ¿Cuán preparado está el personal para manejar herramientas y procedimientos de seguridad en su día a día?

En base a ciertas campañas que se han realizado, aún hay deficiencias por parte de los usuarios, ya que aún caen en correos basura o phishing (previamente preparados por IT justamente para estas campañas)

5. ¿Cómo se asegura la empresa de que solo el personal autorizado acceda a información sensible durante cambios organizacionales como: (rotaciones de personal o bajas)?

Al salir un usuario de la empresa, de forma inmediata se gestiona el cambio de contraseña y reseteo de MFA, Para cerrar todas las sesiones activas y revisar a detalle el equipo para evitar nubes externas instalas o información personal que atente contra la seguridad de la información. Todo se gestiona por directorio activo para cuentas y equipos corporativos.

Firma

Maestría Seguridad Informática **Titulación**
Jean Alexander Jiménez Lara

Anexo 5. *Entrevista 5*

ENCUESTA PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Universidad Israel

Encuestado: Santiago Barahona Cargo: Preventa de HPE

Título: Ingeniero en Redes.

1. ¿Qué procedimientos se siguen actualmente para otorgar y revocar permisos de acceso en la empresa?

Se definen políticas de acceso cómo el qué, quién y bajo qué condiciones se debe dar accesos, se gestiona el permiso y el rol adecuado al usuario

2. ¿Cuáles son los criterios utilizados para definir los niveles de acceso de los empleados a la información?

Los niveles para clasificar la información son: confidencial, restringido, interno y el público, dependiendo de dicho de rol al usuario que puede ser máximo, medio o mínimo privilegio

3. ¿La empresa ha experimentado incidentes de seguridad relacionados con accesos no autorizados en el pasado? Si es así, ¿cómo se gestionaron?

Se aplicaron políticas a los usuarios y a los equipos para evitar q un programa malicioso afecte a la integridad de la información, el equipo de IT revisó cada usuario para cerciorarse que el programa haya sido desinstalado

4. ¿Cuán preparado está el personal para manejar herramientas y procedimientos de seguridad en su día a día?

Como equipo de IT se busca cada cierto tiempo mejoras en las políticas de seguridad del AD, se intenta capacitar a los usuarios para q no caigan en ataques de phishing

5. ¿Cómo se asegura la empresa de que solo el personal autorizado acceda a información sensible durante cambios organizacionales como: (rotaciones de personal o bajas)?

Cuando una persona deja su cargo se revisa que el equipo quede con toda la información laboral, se cambia la contraseña y el MFA para así cerrar las sesiones activas

Firma

Maestría Seguridad Informática
Jean Alexander Jiménez Lara

Titulación

Anexo 6. *Validación de especialista por parte de Joao Mauricio Lema*

Universidad Israel

ESPOG | Escuela de Posgrados

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital BUENAS PRÁCTICAS PARA EL CONTROL DE ACCESO EN LA EMPRESA NEXSYS DEL ECUADOR BASADA EN LA NORMA ISO 27001. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por:	Joao Mauricio Lema Alcivar
Título obtenido:	Ingeniero en Sistemas
C.I.:	172104728-5
E-mail:	joao.lema.a@gmail.com
Institución de Trabajo:	Nexsys del Ecuador
Cargo:	Analista de TI
Años de experiencia en el área:	4 Años

Universidad Israel

ESPOG | Escuela de Posgrados

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: BUENAS PRÁCTICAS PARA EL CONTROL DE ACCESO EN LA EMPRESA NEXSYS DEL ECUADOR BASADA EN LA NORMA ISO 27001

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia		X			
Aplicabilidad		X			
Factibilidad		X			
Novedad			X		
Fundamentación pedagógica		X			
Fundamentación tecnológica		X			
Indicaciones para su uso		X			
TOTAL		24	3		

Observaciones: La Empresa Nexsys del Ecuador Posee Bastante Conceptualizado el Marco Laboral

Recomendaciones: Poder implementar mucho conocimientos laborales y Sociales Para mejorar a Ambiente Laboral

Lugar, fecha de validación: 30 - Agosto - 2021

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en

Universidad Israel

ESPOG | Escuela de Posgrados

Seguridad informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.

Firma del especialista

Joao Lema

Anexo 7. *Validación de especialista por parte de Iván Santiana*

Universidad Israel

ESPOG | Escuela de Posgrados

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital BUENAS PRÁCTICAS PARA EL CONTROL DE ACCESO EN LA EMPRESA NEXSYS DEL ECUADOR BASADA EN LA NORMA ISO 27001. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por:	Iván Santiana.
Título obtenido:	Ingeniero en Ciencias de la Computación.
C.I.:	1752289981
E-mail:	analistacomer6.ec@nexsysla.com.
Institución de Trabajo:	Nexsys del Ecuador
Cargo:	Consultor Técnico Microsoft.
Años de experiencia en el área:	1 año

Universidad Israel

ESPOG | Escuela de Posgrados

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: BUENAS PRÁCTICAS PARA EL CONTROL DE ACCESO EN LA EMPRESA NEXSYS DEL ECUADOR BASADA EN LA NORMA ISO 27001

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia		X			
Aplicabilidad		X			
Factibilidad		X			
Novedad	X				
Fundamentación pedagógica	X				
Fundamentación tecnológica	X				
Indicaciones para su uso		X			
TOTAL	15	16			

Observaciones: La seguridad de la información es un proceso continuo. Por lo cual se debe estar preparado para adaptar y mejorar continuamente las medidas de control de acceso

Recomendaciones: Asegurarse de que toda la documentación relacionada con el control de acceso sea fácilmente accesible para el personal autorizado

Lugar, fecha de validación: Quito 30 de Agosto de 2024

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en

Universidad Israel

ESPOG | Escuela de Posgrados

Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.

Firma del especialista

Iván Santana.

Marco David Maruri Lozano (Doc 3)

Anexo 8. *Validación de especialista por parte de Marco Mauri*

Universidad Israel

ESPOG | Escuela de Posgrados

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital BUENAS PRÁCTICAS PARA EL CONTROL DE ACCESO EN LA EMPRESA NEXSYS DEL ECUADOR BASADA EN LA NORMA ISO 27001. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por:	MARCO DAVID MARURI LOZANO
Título obtenido:	INGENIERO EN MECATRÓNICA, MGTR. GESTIÓN RIESGOS
C.I.:	1719130 70-8
E-mail:	PREVENTA2.EC@NEXSYSLA.COM
Institución de Trabajo:	NEXSYS DEL ECUADOR
Cargo:	PREVENTA HARDWARE IBM
Años de experiencia en el área:	2 AÑOS

Universidad Israel

ESPOG | Escuela de Posgrados

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: BUENAS PRÁCTICAS PARA EL CONTROL DE ACCESO EN LA EMPRESA NEXSYS DEL ECUADOR BASADA EN LA NORMA ISO 27001

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia		X			
Aplicabilidad	X				
Factibilidad		X			
Novedad	X				
Fundamentación pedagógica	X				
Fundamentación tecnológica	X				
Indicaciones para su uso		X			
TOTAL	20	12			

Observaciones:.....

.....

.....

Recomendaciones: Para la propuesta tomar en consideración los lineamientos establecidos por parte de la empresa para la implementación de nuevas medidas acorde a lo que indica la norma.

Lugar, fecha de validación: Quito, 30 de Agosto del 2024

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en

Universidad Israel

ESPOG | Escuela de Posgrados

Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.

Firma del especialista

MARCO MARCEL

Anexo 9. *Validación de especialista por parte de Karen Toaquiza*

Universidad Israel

ESPOG | Escuela de Posgrados

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital BUENAS PRÁCTICAS PARA EL CONTROL DE ACCESO EN LA EMPRESA NEXSYS DEL ECUADOR BASADA EN LA NORMA ISO 27001. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por:	Karen Toaquiza
Título obtenido:	Ingeniero Mecatrónica
C.I.:	1724972821
E-mail:	preventa15.ec@nexsysla.com
Institución de Trabajo:	Nexsys del Ecuador
Cargo:	Preventa Microsoft
Años de experiencia en el área:	2 años

Universidad Israel

ESPOG | Escuela de Posgrados

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: BUENAS PRÁCTICAS PARA EL CONTROL DE ACCESO EN LA EMPRESA NEXSYS DEL ECUADOR BASADA EN LA NORMA ISO 27001

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	X				
Aplicabilidad	X				
Factibilidad		X			
Novedad		X			
Fundamentación pedagógica	X				
Fundamentación tecnológica	X				
Indicaciones para su uso	X				
TOTAL	25	8			

Observaciones: La implementación de controles de seguridad me parecen adecuados, pero debemos destacar la necesidad de asegurar que todos los controles estén actualizados y se hagan pruebas de efectividad

Recomendaciones: Sugiero como parte del proyecto la realización de constantes auditorías internas para identificar y corregir posibles deficiencias en el sistema de gestión de seguridad de la información

Lugar, fecha de validación: Quito, 30 de agosto de 2024

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en

Universidad Israel

ESPOG | Escuela de Posgrados

Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.

Firma del especialista

Karen Tasiguiza

Anexo 10. *Validación de especialista por parte de Santiago Barahona*

Universidad Israel

ESPOG | Escuela de Posgrados

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital BUENAS PRÁCTICAS PARA EL CONTROL DE ACCESO EN LA EMPRESA NEXSYS DEL ECUADOR BASADA EN LA NORMA ISO 27001. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por:	Santiago Barahona
Título obtenido:	Ingeniero en Redes
C.I.:	1004003248
E-mail:	preventa1.ec@nexsyslo.com
Institución de Trabajo:	Nexsys del Ecuador
Cargo:	Preventa de HPE
Años de experiencia en el área:	2 años.

Universidad Israel

ESPOG | Escuela de Posgrados

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: BUENAS PRÁCTICAS PARA EL CONTROL DE ACCESO EN LA EMPRESA NEXSYS DEL ECUADOR BASADA EN LA NORMA ISO 27001

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	X				
Aplicabilidad	X				
Factibilidad	X				
Novedad		X			
Fundamentación pedagógica		X			
Fundamentación tecnológica	X				
Indicaciones para su uso		X			
TOTAL	20	12			

Observaciones: A nivel de empresa se debe comunicar de manera pertinente y transparente qué procesos y políticas de seguridad se están aplicando para evitar cualquier incidente

Recomendaciones: Se debería evaluar y monitorear a los proveedores y socios de esta implementación para asegurarse q también cumplan con estándares de seguridad

Lugar, fecha de validación: Quito, 30 de agosto de 2024

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en

Universidad Israel

ESPOG | Escuela de Posgrados

Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.

Firma del especialista

Santiago Barahona