UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN NOVIEMBRE 2023 – ABRIL 2024

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE: INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS DE PROCEDIMIENTOS PARA PREVENIR LA FILTRACIÓN DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE CONTROLES DE LA NORMA ISO 27001 EN EL CENTRO OPERATIVO LOCAL ECU 911 BABAHOYO

ESTUDIANTE: ARIEL OSWALDO PENDOLEMA ESPINOSA

TUTOR:

ING. HARRY ADOLFO SALTOS VITERI

AÑO 2024

Contenido

Resumen

El caso de estudio examina los procedimientos implementados en el Centro Operativo Local ECU 911 Babahoyo para prevenir la filtración de datos mediante la aplicación de controles de la norma ISO 27001. Se realizó una entrevista con el jefe encargado, para analizar estos procedimientos. Los resultados de la entrevista revelaron la implementación de controles de acceso físico y lógico, firewalls, sistemas de detección de intrusiones y encriptación de datos sensibles. Se destacaron políticas de seguridad de la información y procedimientos de gestión de incidentes.

Entre las novedades encontradas se puede identificar el desarrollo de los peligros informáticos, la deficiencia en la educación al personal y al uso de celulares en la institución; adicional a esto se identifican problemas en el reconocimiento de usuarios, el manejo de contraseñas y a la vigilancia de los sistemas del centro. Con todo lo indicado se entablo una conversación con los interesados para determinar la probabilidad de lograr certificar a la institución con la normativa ISO 27001 para mejorar los controles de este y de la misma manera crear jornadas de capacitación al personal.

El estudio proporciona un análisis exhaustivo de los procedimientos de seguridad de la información, los desafíos y las iniciativas para fortalecer la protección de datos en el Centro Operativo Local ECU 911 Babahoyo. Esto establece una base sólida para implementar mejoras continuas en la seguridad de la información, garantizando la confidencialidad, integridad y disponibilidad de los datos críticos en el centro operativo.

Palabras clave

- Controles
- Norma ISO 27001
- Centro Operativo Local ECU 911 Babahoyo
- Seguridad de la información

Summary

Demanding study examines the procedures implemented at the ECU 911 Babahoyo Local Operations Center to prevent data leakage through the application of ISO 27001 controls. An interview was conducted with the assigned head to analyze these procedures. The interview results revealed the implementation of physical and logical access controls, firewalls, intrusion detection systems, and encryption of sensitive data. Information security policies and incident management procedures were highlighted.

Challenges were identified such as evolving malware, staff training and mobile device management. Weaknesses were noted in user authentication, password management and system monitoring. The possibility of certifying the center to ISO 27001 was discussed, which would entail additional controls, regular risk assessments and training programmes.

This study found a solid basis for the execution, improving the information security, ensuring the confidentiality, integrity, and availability of critical information in the operation center. The study provides us a comprehensive analysis of information security procedures and initiatives to reinforce information protection at the ECU 911 Babahoyo Local Operation Centre.

Planteamiento del problema

En el Centro Operativo Local ECU 911 Babahoyo la seguridad de la información es un aspecto importante para garantizar la protección de datos confidenciales.

Un aspecto importante para garantizar la protección de datos sensibles está relacionado con la seguridad pública y la gestión de emergencias seguridad pública y emergencia. Las medidas de seguridad deficientes pueden tener consecuencias negativas que van desde la divulgación de información confidencial hasta violaciones de la integridad. En un entorno cada vez más amenazado por los ciberdelincuentes, el tiempo que se pierde para abordar las violaciones de seguridad puede tener un impacto significativo en la eficiencia operativa de una instalación, en la confianza de la comunidad y en las fuerzas del orden.

Constantes desafíos para el Centro de Operaciones Local ECU 911 Babahoyo son salvaguardar sus datos confidenciales de filtraciones y accesos sin autorizar. Llevar a cabo medidas de seguridad de acuerdo con la norma ISO 27001:2022 es decisivo para evitar estas salidas de información. Pero, surgen dudas sobre la verdadera capacidad y eficacia de estos controles sobre la instalación para prevenir fugas de manera adecuada. Esto preocupa y se agravaría si se considera la posible pérdida de tiempo en caso de una infracción importante.

El corregimiento de fallos en datos puede consumir demasiado tiempo y recursos. Desde el primer descubrimiento de una infracción hasta la adopción de medidas correctivas y la recuperación de la confianza en la base de datos, todo paso es primordial y podría tener un impacto directo en alguna función y en la percepción del centro operativo sobre los servicios a la comunidad.

Las adaptaciones necesarias para abordar este problema son variadas y complejas. Internamente, se requiere una evaluación exhaustiva de los procedimientos existentes, posibles cambios en la infraestructura de TI, capacitación del personal en seguridad de la información y la implementación de políticas más estrictas de manejo de datos.

Por fuera se podría necesitar establecer alianzas con expertos en ciberseguridad, reforzar la cooperación con otras agencias gubernamentales y mejorar la comunicación con el público sobre las posibles nuevas medidas de seguridad que se implementarían.

Al exterior del Centro Operativo Local ECU 911 Babahoyo podría apoyarse de asociaciones estratégicas con agencias gubernamentales, expertos y agencias de aplicación de la ley en seguridad cibernética para fortalecer su postura de seguridad. La asociación con entidades externas puede proporcionar recursos, experiencia, auxilios adicionales en la detección temprana de la amenaza y tener respuesta a las posibles amenazas cibernéticas.

Justificación

El problema más grande y extendido en el mundo digital actual son las filtraciones de datos. Organizaciones operativas como el ECU 911 Babahoyo gestionan información sensible y critica, incluidos datos personales y de servicios de emergencia, por lo que es importante prevenir cualquier incidente que pueda comprometer la seguridad de los residentes y la calidad de los servicios. La implementación de estándares compatibles con ISO 27001 no solo ayuda a reducir el riesgo de violaciones de datos, sino que también garantiza el cumplimiento de estándares internacionales de seguridad de datos altamente reconocidos. El incumplimiento puede dar lugar a sanciones legales y daños a la reputación de la empresa.

El Centro Operativo Local ECU 911 en Babahoyo representa un referente de seguridad para la comunidad, por lo cual la existencia de un riesgo en la seguridad de sus datos significaría un peligro en la privacidad de todas las emergencias coordinadas en la ciudad. El correcto uso de la norma ISO 27001 plasmaría una reducción de los peligros informáticos existentes en la actualidad y brindaría a la institución un alto grado de confianza ante la ciudadanía; además aumentaría la eficiencia del Centro Operativo Local ECU 911 Babahoyo ya que se disminuirían los tiempos de respuestas y evitaría el uso de recursos ante incidentes de seguridad.

Hoy en día donde la digitalización y la tecnología está en todos lados, la ciberseguridad se ha convertido en un asunto primordial para gobiernos, organizaciones y ciudadanos en general. La interconexión de sistemas y proliferación de amenazas cibernéticas señalan la importancia de proteger los datos como una medida esencial para salvaguardar su infraestructura, privacidad y seguridad pública.

La función principal de la institución es la coordinación de llamadas de emergencia en las provincias de Los Ríos y Bolívar, por ende, la información que maneja es de carácter sensible y confidencial.

El presente caso de estudio tiene como finalidad proporcionar información actualizada para identificar oportunamente amenazas referentes a la seguridad de la información y de esta manera se garantice el compromiso del Centro Operativo ECU 911 Babahoyo ante las problemáticas cibernéticas.

Objetivos

Objetivo General

Analizar los procedimientos empleados para evitar la filtración de datos en el Centro Operativo Local ECU 911 Babahoyo, a través de la aplicación de controles conforme a los estándares de la Norma ISO 27001.

Objetivos Específicos

• Identificar los protocolos de gestión de datos en el Centro Operativo Local ECU 911 Babahoyo con el fin de comprender en profundidad el manejo de la información en dicho centro.

• Analizar los posibles riesgos de filtración de datos en el Centro Operativo Local ECU 911 Babahoyo para comprender las vulnerabilidades y amenazas potenciales que podrían comprometer la seguridad de los datos en el centro.

• Formular recomendaciones y mejoras en los procedimientos existentes para satisfacer los requisitos establecidos por la Norma ISO 27001 y prevenir la filtración de datos.

Líneas de investigación

Las líneas de investigación de la carrera, que abarcan Sistemas de Información y Comunicación, Emprendimiento e Innovación, y Redes y Tecnologías Inteligentes de Software y Hardware, tienen una clara relación con el caso de estudio sobre el análisis de procedimientos para prevenir la filtración de datos mediante la implementación de controles de la Norma ISO 27001 en el Centro Operativo Local ECU 911 Babahoyo.

Para empezar los sistemas de información y generación de informes desempeñan un papel clave en la comprensión de la gestión de la información y la protección de datos en un entorno como el Centro Operativo Local ECU 911. La adopción de la norma ISO 27001 requiere la implementación de protección de datos durante todo el ciclo de vida de los datos, desde el almacenamiento hasta la entrega. Esto significa que la empresa debe comprender la estructura, integración y gestión de los sistemas de información locales para poder monitorear posibles violaciones de seguridad en el almacenamiento de datos.

A su vez, la innovación es interesante en este sentido, ya que la adopción de la norma ISO 27001 tiene como objeto mejorar la seguridad de la información en la institución.

El uso de la norma significa una nueva herramienta para determinar problemas de seguridad evitando que ocurran y representa una guía para el cumplimiento de estas en la institución y en todo el personal que la conforma. Las líneas investigativas son de vital importancia para determinar la necesidad de estos controles en el Centro Operativo ECU 911 Babahoyo.

La Norma ISO 27001 requiere la implementación de tecnologías actuales y de herramientas que generen una adecuada protección de los datos entre los que se destaca el cifrado de datos y a los sistemas de detección de amenazas que certifiquen la seguridad de la información.

Marco conceptual

Servicio Integrado de Seguridad ECU 911

El presidente en ese entonces el economista Rafael Correa planteó un sistema de gestión de emergencias el cual sería único en respuesta a las preocupaciones que se intensificaban en la población ecuatoriana sobre la seguridad. En el pasado, cada servicio de emergencia tenía un número de teléfono, lo que provocaba tranques en algunas calles, lo que no permitía dar respuestas al momento y coordinadas a las emergencias de los ecuatorianos. (Marcillo Vera, 2020)

Además, se enfrentaba al desafío de llamadas falsas o de broma que saturaban las líneas y retrasaban la atención a emergencias reales. Aunque la adopción de un número único no resolvió completamente este problema, resaltó la necesidad de una política pública que sancionara tales comportamientos. Esto se refleja en el artículo 396 del Código Orgánico Integral Penal (2014), que aborda las infracciones de cuarta clase. (Abujatum, 2019)

Seguridad de la información para empresas

La seguridad de la información comprende un conjunto de medidas diseñadas para proteger tanto los datos como la infraestructura, con el fin de garantizar la confidencialidad, la disponibilidad y la integridad de la información. Sus objetivos se centran en minimizar los daños, así como en prever y prevenir posibles riesgos e impactos. (Cepal, 2024)

Con los avances tecnológicos recientes, se ha vuelto indispensable para todas las organizaciones. Tanto los procesos empresariales actuales como la información que gestionan han migrado del formato físico al electrónico, lo que ha mejorado significativamente su accesibilidad, uso y manipulación desde diversos dispositivos digitales y a través de Internet.

Esto ha impulsado la urgencia de salvaguardar la información y los datos, un reto que impacta no solo a grandes corporaciones y empresas líderes en el mercado, sino también a las pequeñas y medianas empresas (pymes). El presente artículo se centra en examinar la relevancia de proteger los datos contra posibles intrusiones de piratas informáticos o hackers,

y propone principios esenciales para establecer un sistema de seguridad de la información que evidencie ante las partes interesadas la capacidad de la empresa para proteger sus activos de datos. La información se reconoce como un activo intangible crucial para el desarrollo empresarial. (De La Cruz y otros, 2023)

Figura 1

Nota. Triada de la información

Fuente: Google Académico

A menudo, se reportan brechas de seguridad, ataques cibernéticos y robos de datos en todo el mundo, lo que subraya la necesidad urgente de proteger la información en un entorno digital en constante evolución. Aunque muchos creen que solo las grandes empresas o instituciones son blanco de estos ataques, las estadísticas revelan que los ciberataques ocurren constantemente en todo el mundo, y ninguna organización está exenta de riesgo.

Si bien los avances tecnológicos han simplificado muchos aspectos de nuestra vida cotidiana y empresarial, también han generado preocupaciones significativas para los líderes empresariales en todos los niveles. (Komlev, 2022)

Incidentes de

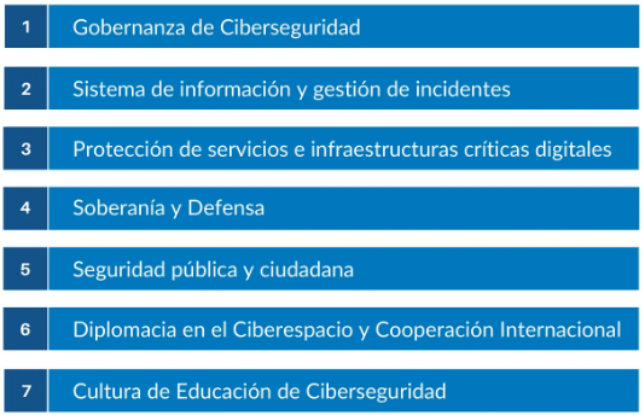
Filtración de datos en empresas ecuatorianas

La información sobre la filtración de datos de ciudadanos ecuatorianos, incluyendo 6,7 millones de niños, se hizo pública en el sitio web ZDNet y fue descubierta por vpnMentor, una firma especializada. Según sus investigaciones, los datos procedían de un servidor de la empresa Novaestrat, una consultora dedicada al análisis de datos, marketing y desarrollo de software. Este incidente ha generado la búsqueda de métodos para eliminar esta información de todos los sitios web donde se publicó sin verificación. Incluso, la empresa Eliminalia, que se especializa en proteger el derecho al olvido en internet, ha puesto a disposición un formulario de asistencia gratuita para borrar los datos, utilizando herramientas de informática forense y extracción de información. (Machuca Vivar y otros, 2022)

Ciberseguridad en Ecuador

Las estadísticas en Ecuador muestran que la mayoría de las violaciones de seguridad se han producido dentro del sistema financiero. Por ejemplo, según el Ministerio Coordinador de Seguridad en 2014, se observó un aumento del 37% en los robos a través de la banca virtual, un 14% en fraudes con tarjetas de crédito y un 46% en ataques a cajeros automáticos. (Toala Indio, 2021)

Figura 2



Nota. Pilares para un Ecuador Digital más seguro

Fuente: Google Académico

Pero los problemas de seguridad no se limitan al sector bancario. La prensa ecuatoriana también ha sido objeto de varios ataques a sus sitios web con dominio ".ec". Además, ha habido ataques atribuidos al grupo Anonymous a los sitios web gubernamentales, ataques al sistema informático electoral y presuntos ataques cibernéticos procedentes de diversos países como Colombia, Estados Unidos, Rusia, China y Francia dirigidos a cuentas o datos personales de ciudadanos ecuatorianos. También se han registrado ataques a cuentas de redes sociales de figuras públicas y a portales web de opinión libre, entre otros incidentes. (Morán Maldonado, 2021)

Incidentes de ciberseguridad en Ecuador

Los avances tecnológicos han incrementado la vulnerabilidad en materia de seguridad informática. A medida que se desarrollan nuevas aplicaciones o sistemas con el fin de facilitar y mejorar actividades empresariales, también surgen otras herramientas con la intención de acceder de forma no autorizada a la información de diversas organizaciones, incluyendo numerosas empresas en Ecuador. (Sanchéz Guerrero, 2022)

Tabla 1

Incidentes de ciberseguridad reportados en Ecuador

Año	Incidente	Descripción
2019	Ataque a Cedatos	El servidor de la empresa de encuestas Cedatos fue hackeado y se filtraron datos personales de millones de ecuatorianos, incluyendo nombres, direcciones y números de teléfono.
2019	Violación de Datos en el Registro Civil	Se reportó una violación de datos en el Registro Civil de Ecuador,

		donde se filtraron registros de millones de ciudadanos, incluyendo información confidencial como nombres, fechas de nacimiento y números de identificación.
2020	Ataque malicioso al Municipio de Quito	Un ataque de ransomware en el Municipio de Quito corrompió el funcionamiento de su sistema informático.
2020	Acontecimiento de Phishing en el Banco Pichincha	Los clientes del Banco Pichincha fueron objeto de un incidente de fraude en el que los clientes recibieron correos electrónicos falsos. Correos electrónicos solicitando información confidencial y bancaria.
2021	Filtración de Datos en Claro Ecuador	Se informó sobre una filtración de datos en la compañía de telecomunicaciones Claro Ecuador, donde se expusieron datos personales y de contacto de miles de clientes.

2021	Denegación de Servicio (DDoS) a Instituciones Públicas	Algunos bancos en Ecuador se han visto afectados por ataques DDoS, lo que interrumpió las operaciones en línea y el acceso a las cuentas de los clientes.
2022	Virus informático malicioso en el Hospital de Guayaquil	Uno de los hospitales de Guayaquil sufrió un ataque de ransomware que infectó sistemas informáticos y comprometió el acceso a los datos de los pacientes.

Nota. Con esta tabla se proporciona una descripción general de algunos de los principales problemas de ciberseguridad en Ecuador.

Fuente: Google Académico

Auditorias de seguridad

Una auditoría se define como un procedimiento sistemático, independiente y registrado destinado a recopilar pruebas de auditoría y evaluar de manera imparcial para determinar el nivel de cumplimiento de determinados procesos. La importancia de estas auditorías es innegable, ya que permiten verificar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI). Esta auditoría puede ser llevada a cabo por un miembro interno de la empresa, siempre y cuando esté debidamente calificado para dicha tarea. (Valarezo Lopez & Tenezaca Caizabanda, 2024)

Tabla 2

Plan de auditoría

Etapa de auditoria	Actividades	Responsable	Recursos Necesarios	Tiempo estimado

Planificación	Definir alcance y objetivos de la auditoría, seleccionar sistemas y procesos a auditar, identificar recursos necesarios, programar reuniones con responsables, elaborar cronograma.	Autor Líder	Equipo de auditoría, acceso a la documentación pertinente	1 semana
Preparación	Revisar documentación relacionada, identificar riesgos y controles, preparar cuestionarios de auditoría, asignar roles al equipo de auditoría.	Equipo de Auditoria	Documentación relevante, cuestionarios de auditoría	1 semana
Ejecución	Realizar entrevistas con responsables, revisar evidencia documental, evaluar cumplimiento de controles, identificar hallazgos, comunicar hallazgos preliminares.	Equipo de Auditoría	Equipos de grabación (si es necesario), cuestionarios de auditoría	2 semanas
Reporte	Documentar hallazgos, elaborar informe de auditoría, revisar informe, presentar informe a dirección y responsables.	Auditor Líder	Software de procesamiento de texto, plantillas de informes	2 semanas
Seguimiento	Monitorear acciones correctivas/preventivas, evaluar efectividad, preparar informes de	Auditor Líder	Registro de acciones correctivas, seguimiento de indicadores	En curso

	seguimiento, comunicar resultados.			

Nota. Ejemplo de cómo se podría estructurar un plan de auditoría para una institución como el ECU 911.

Fuente: Google Académico

Experiencias de implementación de ISO 27001

Los profesionales que se embarcan en el proyecto de implementación de ISO 27001 y un Sistema de Gestión de Seguridad de la Información siguen un proceso que comienza con la obtención del respaldo de la Alta Dirección. (More Reaño, 2021)

Para este primer paso, es esencial presentar un plan de trabajo que detalle los recursos requeridos para el proyecto y los objetivos que se pretenden alcanzar. Se trata de un principio básico de análisis de coste-beneficio. La Alta Dirección debe comprender claramente el costo y los beneficios de implementar ISO 27001. En la práctica, el proceso de implementación comienza con la conformidad de las cláusulas 6 (Planificación) y 7 (Soporte y Recursos). Durante estas etapas, se llevan a cabo evaluaciones de riesgos y se definen los controles, seleccionando entre los 114 que sugiere la norma, que serán necesarios implementar. (Escuela europea de excelencia, 2022)

La estimación del tiempo necesario para la implementación variará según el tamaño de la organización y el número de empleados, así como:

Tabla 3

Estimación de tiempo

Número de empleados	***Tiempo estimado***
Hasta 20 empleados	Tres meses, aproximadamente
De 20 a 50 empleados	3 a 5 meses
50 a 200 empleados	Entre 5 y 8 meses

Más de 200 empleados	8 a 20 meses

Nota. Esta tabla muestra el tiempo que tomará la implementación de la norma ISO 27001 en función con los empleados

Fuente: Google Académico

ISO 27001 en los SGSI

La norma ISO 27001, centrada en la seguridad de la información, ayuda a las empresas a cumplir con los requisitos legales establecidos en los contratos de seguridad de la información, los cuales deben estar claramente definidos, documentados y actualizados en cada Sistema de Gestión de Seguridad de la Información. Esta norma estándar se concentra en proteger la confidencialidad, disponibilidad e integridad de todos los activos de información dentro de una organización, siendo el Sistema de Gestión de Seguridad de la Información el concepto principal que la sustenta.

Figura 3

Nota. Esta figura detalla las fases metodológicas de la norma ISO 27001

Fuente: Google Académico

Consciente de la importancia de las tecnologías de la información y la comunicación (TIC) en el funcionamiento institucional e interinstitucional, la secretaría nacional de administración pública emitió los acuerdos ministeriales No. 804 y No. 837 en julio y agosto

de 2011, respectivamente, estableciendo la comisión para la seguridad informática y de las tecnologías de la información. (Chicaiza Castillo & Torres Chango, 2020)

La seguridad de la información tiene un impacto importante en la privacidad tanto para individuos como para entidades, y este impacto puede variar en función del contexto social en el que se encuentren. La digitalización de las empresas presenta una serie de desafíos, algunos de los cuales pueden ser beneficiosos, pero otros pueden suponer riesgos para la seguridad. (Chavarry Bonilla, 2021)

Nuevo estándar ISO 27001:2022

Acontecimientos externos como los nuevos modelos de negocio, la pandemia y los conflictos geopolíticos han tenido un impacto directo y han iluminado la necesidad de actualizar los controles de seguridad. En este contexto, estos estándares de seguridad son objeto de revisión y actualización periódica. Recientemente, se ha lanzado la nueva versión de ISO 27001 (ISO/IEC 27001:2022), que sigue siendo una de las principales referencias en ciberseguridad a nivel mundial. (Mendoza, 2023)

Tabla 4

Características relevantes del nuevo estándar ISO/IEC 27001:2022

Aspecto	Descripción
Alcance Amplio	La ISO/IEC 27001:2022 amplía su alcance para abarcar una gama más amplia de riesgos y amenazas emergentes en el entorno digital.
Enfoque Proactivo	Se centra en una estrategia proactiva de gestión de riesgos que reconozca la importancia de anticipar y mitigar las amenazas potenciales antes de que se transformen en infracciones.

Adaptabilidad	La norma se adapta a las tendencias tecnológicas y a las tendencias emergentes.
Incorporación de causas externas	El impacto de causas externas, como pandemias y cambios geopolíticos, fomenta la adhesión de estos factores en la gobernabilidad de la seguridad de los datos.
Orientación continua	Infunde a las instituciones a centrarse con en mejorar la protección de la información, renovando periódicamente sus controles de seguridad para mantenerse al día con las amenazas en constante cambio.
Empleo de nuevas tecnologías	Identifica el papel de las tecnologías emergentes como la IA, el internet de las cosas (IoT) y la computación en la nube, proporcionando normas para gestionar los riesgos asociados con su acogida.

Nota. Visión general de los elementos básicos de la nueva versión de ISO/IEC 27001:2022, un enfoque proactivo, flexibilidad y factores externos y nuevas tecnologías.

Fuente: Google Académico

Controles de la norma ISO 27001 para mitigar vulnerabilidades

Tabla 5

Seguridad Física

Control de seguridad física (A.11)	**Descripción**
Acceso físico controlado	Instalación de sistemas de control de acceso, en todas las entradas del centro

Respaldo de energía	Instalación de sistemas de respaldo de energía
Protección contra intrusos	Instalación de sistema de seguridad perimetral
Auditorias de seguridad informática	Realización de auditorías periódicas

Fuente: Norma ISO 27001:2022

Tabla 6

Cifrado de información

Control de cifrado de información (A.5)	**Descripción**
Datos en reposo	Implementación de técnicas de cifrado en datos almacenados en dispositivos de almacenamiento
Dispositivos móviles	Soluciones de cifrado para dispositivos móviles con datos confidenciales
Administración de claves	Revisión regular de los algoritmos de cifrado

Fuente: Norma ISO 27001:2022

Tabla 7

Control de acceso

Control de Acceso (A.9)	**Descripción**
Recomendaciones de Mejora	Implementar la autenticación multifactorial para mejorar la seguridad de las cuentas de usuario
	Establecer políticas claras de gestión de contraseñas que incluyan la rotación periódica de contraseñas y la prohibición del uso de contraseñas débiles

Fuente: Norma ISO 27001:2022

Tabla 8

Seguridad Lógica

Seguridad Lógica (A.12)	Descripción
Recomendaciones de Mejora	Actualizar regularmente el software y los sistemas operativos para corregir vulnerabilidades conocidas
	Implementar sistemas de detección de intrusiones y monitoreo de eventos.

Fuente: Norma ISO 27001:2022

Beneficios y desafíos de la implementación

En la era actual, el fácil acceso a Internet ha simplificado notablemente la comisión de delitos en línea, lo que ha llevado a muchas empresas a reforzar la protección de su información para mitigar los riesgos de pérdida de datos, que podrían desencadenar problemas graves. (Kaspersky, 2024)

Para este caso, surge una norma con su denominación ISO 27001, esta guía ofrece directrices documentadas y mejores prácticas en el ámbito de la seguridad de la información. Este marco normativo garantiza que los datos sean tratados de manera confidencial, íntegra, accesible y legal, con la finalidad de protegerlos contra posibles vulnerabilidades imprevistas.

Puesta en marcha esta guía dentro de la estructura organizacional de una institución promovería la confianza entre los clientes, proveedores y empleados, esta norma está consolidada como un estándar reconocido a nivel internacional.

Adoptar la ISO 27001 permite identificar y controlar los riesgos asociados, lo que facilita la elaboración de un plan para prevenir su ocurrencia y, en caso de que se materialicen, mitigar sus impactos. (Arévalo, 2022)

Marco metodológico

Se optó por una metodología cualitativa, específicamente la realización de entrevistas, porque ofrece la mejor oportunidad para explorar a fondo los aspectos prácticos, las percepciones y las experiencias relacionadas con la implementación de controles de seguridad de la información en un entorno operativo específico como el Centro Operativo ECU 911 Babahoyo. Esto permitirá obtener resultados más significativos para el caso de estudio.

Para abordar el tema del estudio, se fundamentó en varios factores considerados fundamentales para obtener resultados más enriquecedores y comprensivos.

Selección de participantes

Se examinarán los roles y responsabilidades vinculados con la seguridad de la información y la administración de sistemas en el Centro Operativo ECU 911 Babahoyo. Esto englobaría a profesionales directamente involucrados en la aplicación de medidas de seguridad de la información, tales como administradores de sistemas, analistas de seguridad, responsables de tecnologías de la información y directivos con experiencia en ciberseguridad.

Luego de identificar a los participantes potenciales, nos comunicaremos con ellos para explicarles el propósito de la entrevista y solicitar su participación voluntaria. Su ardua experiencia y grande conocimiento son vitales para la investigación, sus contribuciones mejorarán la comprensión de los temas y procedimientos internos centrales.

Diseño de la guía de entrevista

Se realizaría una revisión de la literatura académica y los estándares de seguridad de la información, como la norma ISO 27001, para identificar áreas temáticas relevantes y preguntas específicas que puedan guiar el diseño de la guía de entrevista, diseñando preguntas abiertas que permitan a los participantes compartir sus experiencias, percepciones y opiniones de manera detallada y reflexiva.

Conducción de las entrevistas

Se decidió realizar las entrevistas en un entorno cómodo y privado dentro del Centro Operativo ECU 911 Babahoyo, donde los participantes se sintieran seguros y puedan hablar libremente sobre los temas de seguridad de la información. Durante la entrevista, se utilizarán técnicas de escucha activa para mostrar interés en las respuestas de los participantes y fomentar una comunicación abierta.

Análisis de los datos

• Se iniciaría el proceso de análisis transcribiendo todas las entrevistas realizadas.

• Una vez identificados los temas principales, se interpretarán los resultados en relación con los objetivos del estudio.

• Se tendrá en cuenta la manera de cómo los resultados pueden contribuir a los conocimientos existentes en el dominio de la seguridad de la información y de cómo abordar acciones futuras en este campo.

Resultados

En este caso de estudio se realizó una entrevista con el jefe del Centro Operativo Local ECU 911 Babahoyo, con la finalidad de analizar varios procedimientos en operación y así poder comprender como su información sensible previene fugas de datos. La entrevista mostró los siguientes resultados.

Se remarcan los procedimientos implementados para proteger la información sensible y prevenir la fuga de datos, incluida la implementación de controles de acceso físicos y lógicos, el uso de firewalls, sistemas de detección de intrusiones y el encriptado de datos sensibles. También, la ya existencia de políticas de seguridad de la información y procedimientos de gestión de incidentes, esto es importante porque sirven de gran medida para orientar al personal en la protección de información delicada.

En términos de seguridad de la información y prevención de violaciones de datos, los desafíos están vinculados a la evolución continua de las ciber amenazas, a la formación del personal y a la gestión de los dispositivos móviles utilizados en el terreno identificado. En lo correspondiente a los procedimientos actuales de seguridad de la información, se señalaron áreas de mejora, la autenticación de personas con acceso a datos confidenciales, gestión de contraseñas y la vigilancia de sistemas para detectar todas actividades sospechosas.

En el marco de iniciativas para reforzar la protección de datos, la posibilidad de certificar el centro según la norma ISO 27001 está examinada, lo que implementa la puesta en marcha de controles complementarios, evaluaciones regulares de riesgos y programas de formación sobre la seguridad de la información.

Estos resultados reflejan un análisis completo de los procedimientos actuales de seguridad de la información en el Centro Operativo Local ECU 911 Babahoyo, así como los desafíos e iniciativas encaminadas a reforzar la protección de datos. Esta información obtenida constituye una base sólida para la implementación de mejoras continuas en la seguridad de la

información, garantizando la confidencialidad, integridad y disponibilidad de la información crítica en el centro operativo ECU 911 Babahoyo.

Discusión de resultados

Como indicaban De La Cruz y Méndez con todos estos avances tecnológicos a lo largo de los años se ha vuelto indispensable para cualquier institución salvaguardar su información comprometida, esto es un reto ya que siempre se presentan posibles amenazas, ya sean hackers, piratas informáticos, virus, etc. Todo esto conlleva a mantener un control riguroso en cada una de las acciones y procedimientos que se realizan en la institución.

Para el Centro Operativo ECU 911 Babahoyo es un tema importante salvaguardar sus datos ya que son increíblemente delicados, por ende, llevan controles internos para asegurar su seguridad, claro esto no es del todo seguro ya que siempre hay cualquier tipo de inconveniente cuando se habla de este tema.

Como indica Johana Sánchez cada vez que la tecnología da un paso adelante no simplemente se desarrollan nuevas aplicaciones para facilitar procesos o actividades en instituciones, también surgen programas maliciosos los cuales tendrían intenciones para nada buenas, esto ocurre en todo el mundo no simplemente en nuestro país.

Como se indicaba en la tabla nadie está exento de las manos de estos criminales cibernéticos, no son ataques que ocurrieron hace muchos años más bien todo lo contrario son actuales, esto nos hace darnos cuenta la importancia de una buena gestión de procedimientos en una institución con datos tan vitales. Por eso existen este tipo de guías como la norma ISO 27001 la cual gracias a sus controles ayudan a disminuir o evitar vulnerabilidades actuales o futuras.

Al entrevistar al responsable de la institución a la que me refiero en este estudio de caso, pude comprobar que en ella se mantiene rigurosamente el control de los datos esenciales y críticos, a pesar de las fortalezas anteriormente mencionadas, se han identificado importantes

retos relacionados con la constante evolución de las ciber amenazas, la formación del personal y la gestión de los dispositivos móviles utilizados sobre el terreno. Estos retos son recurrentes en entornos en los que la tecnología avanza rápidamente y las ciber amenazas son cada vez más complejas. La formación del personal y la gestión eficaz de los dispositivos móviles son aspectos críticos que requieren una atención constante para garantizar la protección de los datos.

Esta entrevista me ofreció una visión valiosa de los posibles procedimientos de seguridad de la información que se podrían implementar gracias a los distintos controles que ofrece la norma ISO 27001. La posibilidad de conseguir un certificado más actual conllevaría a que esta institución llevaría a cabo procesos de calidad con una mayor precisión.

De las posibles áreas de mejora reconocidas, como el manejo de autenticación de usuarios y gestión de contraseñas, podrían aplicarse medidas complementarias, tales como el uso de herramientas y autenticación multifactorial de gestión de contraseñas seguras. La continua supervisión de los sistemas y la realización periódica de evaluaciones de riesgos son hábitos y practicas recomendadas para detectar, mitigar y proteger los datos de posibles vulnerabilidades estas tecnologías de la información.

Conclusiones

El análisis de los procedimientos utilizados en el Centro de Operaciones Local ECU 911 Babahoyo pone de relieve la importancia vital de abordar las cuestiones de seguridad de la información en un entorno en el que la gestión de datos es esencial para la eficacia de las operaciones.

Conocemos que el Centro de Operación local ECU 911 Babahoyo enfrenta un sinnúmero de desafíos difíciles de seguridad en la información, desde posibles contravenciones de seguridad física hasta sofisticados utillajes que amenazan a diario a los establecimientos. Aunque, también es confortador ver un compromiso con las mejoras continuas de la seguridad de la información, como señalan las iniciativas actuales y futuras para reforzar la protección de datos en dicha institución.

Un encuentro con el jefe del área de tecnología brinda información meritoria sobre los retos y esfuerzos actuales relacionados con la seguridad de los datos. Es importante reconocer lo difícil de mantener la seguridad de los datos en un entorno operativo dinámico y de alto riesgo como el Centro Operativo Local ECU 911 Babahoyo.

Esta guía internacional indica normas claras y prácticas para la gestión de la seguridad de la información, admitiendo a la institución adoptar un enfoque lógico y organizado para la defensa de la información.

En vista que la tecnología y tácticas de ataque siguen transformándose, el Centro Operativo Local ECU 911 Babahoyo debe estar constantemente alerta, adaptándose a las amenazas nuevas y emergentes. En definitiva, la seguridad en este campo es un esfuerzo de equipo continuo que requiere el compromiso y la participación de todos los que conforman la institución.

Por ende, este caso de estudio proporciona una comprensión global de los retos y oportunidades para la prevención de fuga de datos en el Centro Operativo Local ECU 911

Babahoyo. Aunque siguen existiendo retos importantes, la determinación y la ambición de reforzar la protección de datos y mejorar continuamente los procedimientos de seguridad de la información son evidentes. Aplicando estas recomendaciones y manteniendo un enfoque proactivo de la seguridad de la información, el centro puede avanzar hacia un entorno más seguro y fiable para el tratamiento de datos de misión crítica.

Recomendaciones

Las recomendaciones dirigidas al jefe del área de tecnología del Centro Operativo Local ECU 911 demuestran los hallazgos del estudio realizado de manera organizada; las mismas que se brindan para que la institución adapte una política de seguridad de datos, garantizando de esta manera la confidencialidad de su información.

• Realizar una revisión exhaustiva de los procedimientos de manejo de datos existentes para identificar áreas de mejora y asegurar su alineación con las mejores prácticas de seguridad de la información. Esto incluye la documentación clara de los procesos y la identificación de responsabilidades claras para el manejo y protección de los datos.

• Acarrear a cabo un proceso formal de evaluación de riesgos para identificar y anticipar amenazas potenciales a la seguridad de la información. Esto contendría la práctica de evaluaciones habituales de las vulnerabilidades, y la aplicación de medidas de reducción adecuadas para así abordar los peligrosos fallos reconocidos.

• Impulsar un ambiente de seguridad de la información dentro del Centro Operativo Local ECU 911 Babahoyo, que promueva la responsabilidad y concienciación en todos los niveles de la institución. Esto puede llegar a concretarse mediante programas regulares de capacitación, campañas de promoción y sensibilización de prácticas de seguridad en el lugar de trabajo de las personas que allí laboran.

• Buscar la certificación en la Norma ISO 27001 la cual indicaría cuales son los controles más indicados para salvaguardar la información de forma eficaz, así validando y demostrando el compromiso del Centro Operativo Local ECU 911 Babahoyo con las mejores prácticas de seguridad de la información.

Demandará la aplicación de controles añadidos y auditorías asiduas para garantizar el cumplimiento incesante de las pautas de seguridad.

De esta forma, se instaurará un programa perpetuo de gestión de riesgos que alertará y evaluará constantemente las amenazas salientes y vulnerabilidades permisibles. Lo cual permitiría al Centro Operativo Local ECU 911 Babahoyo acomodarse ágilmente a los cambios en el panorama de la seguridad de la información, tomando medidas proactivas para proteger su información íntima.

Referencias

Abujatum, J. (16 de agosto de 2019). *Biblioteca Nacional de Chile.* Servicio Integrado de Seguridad ECU 911: https://www.bcn.cl/asesoriasparlamentarias/detalle_documento.html?id=75021

Arévalo, M. C. (16 de Octubre de 2022). *Pirani*. Ventajas de implementar la norma ISO 27001: https://www.piranirisk.com/es/blog/las-ventajas-de-implementar-la-iso-27001

Cepal. (5 de enero de 2024). https://biblioguias.cepal.org/gestion-de-datos-de-investigacion

Chavarry Bonilla, S. N. (Abril de 2021). *Repositorio Universidad Cesar Vallejo*. https://repositorio.ucv.edu.pe/handle/20.500.12692/791331&isAllowed=y

Chicaiza Castillo, D. V., & Torres Chango, C. D. (enero de 2020). *Repositorio Universidad Técnica de Ambato.* https://repositorio.uta.edu.ec/jspui/handle/123456789/30690

De La Cruz, G., Mendez, A., & Mendez, R. (30 de marzo de 2023). *redalyc*. https://doi.org/https://www.redalyc.org/journal/6738/673874721015/

Escuela europea de excelencia. (22 de Septiembre de 2022). https://www.escuelaeuropeaexcelencia.com/2022/09/implementar-iso-27001-tiempo-esfuerzo-y-roles-necesarios/

Kaspersky. (2024). *¿Qué es la privacidad de los datos?* https://latam.kaspersky.com/resource-center/threats/internet-and-individual-privacy-protection

Komlev, A. (07 de Abril de 2022). *Linkedin*. https://es.linkedin.com/pulse/seguridad-de-la-informaci%C3%B3n-para-empresas-lo-simple-complejo-komlev

Machuca Vivar, S. A., Vinueza Ochoa, N. V., Sampedro Guamán, C. R., & Molina, S. (2 de Abril de 2022). Habeas data y protección de datos personales en la gestión de las bases de datos. *Revista Universidad y Sociedad*, págs. 244-251. http://scielo.sld.cu/scielo.php?pid=S2218-36202022000200244&script=sci_arttext&tlng=pt

Marcillo Vera, G. A. (2020). *Gestión administrativa y satisfacción laboral percibidas por personal de atención prehospitalaria en politraumatismo de ECU 911 en Babahoyo, Ecuador, 2020*. https://hdl.handle.net/20.500.12692/49061

Mendoza, M. (4 de febrero de 2023). *welivesecurity*. ISO 27001:2022: ¿qué cambios introdujo el nuevo estándar de seguridad?: https://www.welivesecurity.com/la-es/2023/02/09/iso-270012022-cambios-nuevo-estandar-seguridad/

Morán Maldonado, N. M. (2021). *Repositorio Institucional de la Universidad Politécnica Salesiana.* http://dspace.ups.edu.ec/handle/123456789/20243

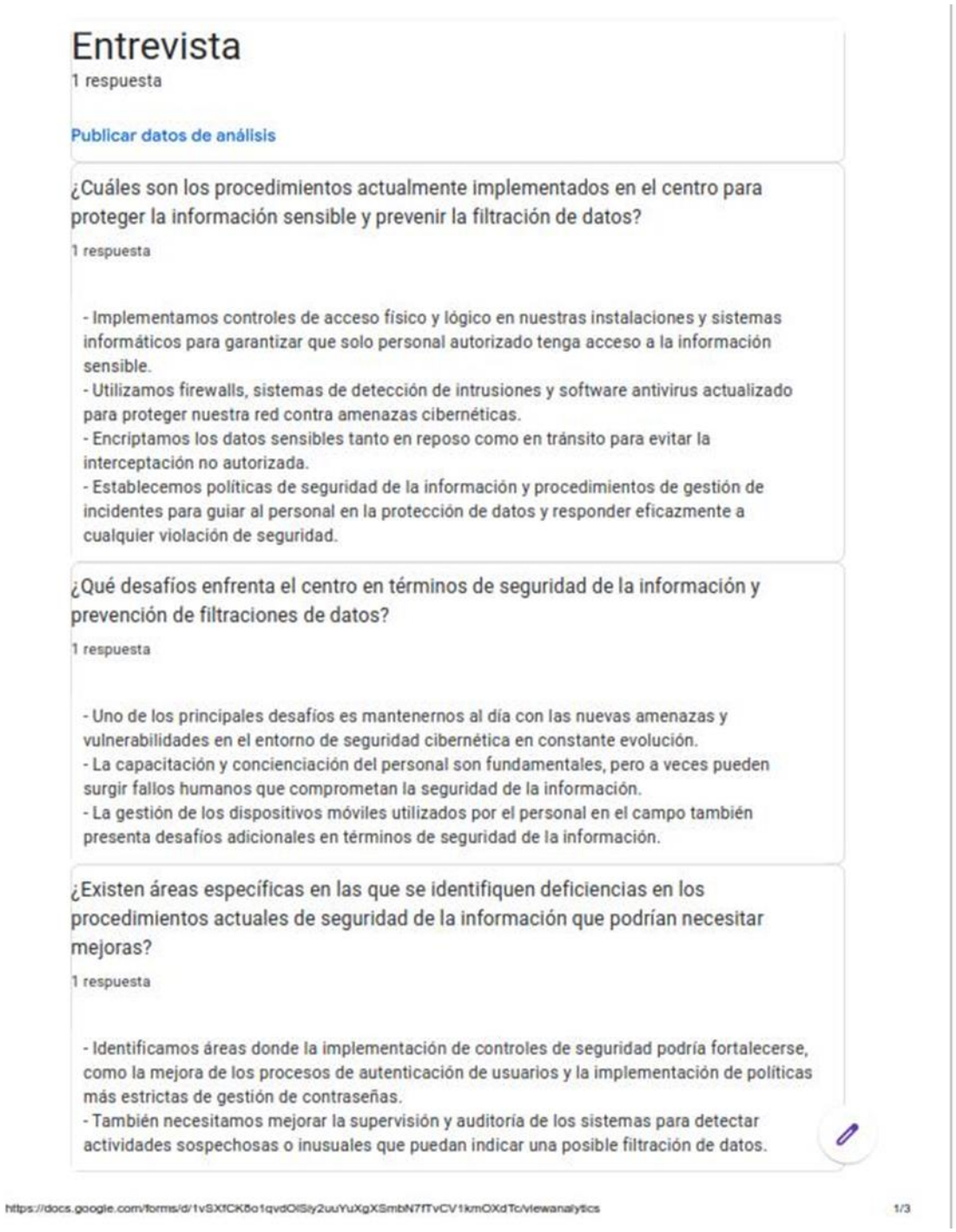
More Reaño, R. (28 de Septiembre de 2021). *Implementación de auditoría informática con la ISO 27001 en la Municipalidad Distrital de Suyo-Piura*. https://repositorio.uladech.edu.pe/handle/20.500.13032/23722

Sanchéz Guerrero, J. D. (diciembre de 2022). *Repositorio Institucional Universidad de Guayaquil*. Estudio del estado actual de la seguridad informática en las Pymes de Guayaquil - Ecuador: http://repositorio.ug.edu.ec/handle/redug/67061

Toala Indio, Y. I. (2021). *Delitos informáticos frecuentes en el Ecuador*. http://dspace.ups.edu.ec/handle/123456789/20942

Valarezo Lopez, J., & Tenezaca Caizabanda, M. (febrero de 2024). *Repositorio Universidad Técnica de Ambato.* Auditoria informática para el análisis de la seguridad en los recursos informáticos utilizando Normas ISO 27001 en Megakons S.A.: https://repositorio.uta.edu.ec/jspui/handle/123456789/40779

Anexos



Entrevista

1 respuesta

Publicar datos de análisis

¿Cuáles son los procedimientos actualmente implementados en el centro para proteger la información sensible y prevenir la filtración de datos?

1 respuesta

- Implementamos controles de acceso físico y lógico en nuestras instalaciones y sistemas informáticos para garantizar que solo personal autorizado tenga acceso a la información sensible.
- Utilizamos firewalls, sistemas de detección de intrusiones y software antivirus actualizado para proteger nuestra red contra amenazas cibernéticas.
- Encriptamos los datos sensibles tanto en reposo como en tránsito para evitar la interceptación no autorizada.
- Establecemos políticas de seguridad de la información y procedimientos de gestión de incidentes para guiar al personal en la protección de datos y responder eficazmente a cualquier violación de seguridad.

¿Qué desafíos enfrenta el centro en términos de seguridad de la información y prevención de filtraciones de datos?

1 respuesta

- Uno de los principales desafíos es mantenernos al día con las nuevas amenazas y vulnerabilidades en el entorno de seguridad cibernética en constante evolución.
- La capacitación y concienciación del personal son fundamentales, pero a veces pueden surgir fallos humanos que comprometan la seguridad de la información.
- La gestión de los dispositivos móviles utilizados por el personal en el campo también presenta desafíos adicionales en términos de seguridad de la información.

¿Existen áreas específicas en las que se identifiquen deficiencias en los procedimientos actuales de seguridad de la información que podrían necesitar mejoras?

1 respuesta

- Identificamos áreas donde la implementación de controles de seguridad podría fortalecerse, como la mejora de los procesos de autenticación de usuarios y la implementación de políticas más estrictas de gestión de contraseñas.
- También necesitamos mejorar la supervisión y auditoría de los sistemas para detectar actividades sospechosas o inusuales que puedan indicar una posible filtración de datos.

https://docs.google.com/forms/d/1vSXfCK8o1qvdOlSiy2uuYuXgXSmbN7fTvCV1kmOXdTc/viewanalytics 1/3

Anexo 1

¿Qué iniciativas se están considerando o implementando para fortalecer aún más la protección de datos en el centro?

1 respuesta

- Estamos considerando la certificación ISO 27001 como un marco de referencia para establecer un sistema de gestión de seguridad de la información robusto y basado en estándares internacionales.
- Esto implicaría realizar evaluaciones de riesgos regulares, implementar controles de seguridad adicionales según las mejores prácticas de la norma ISO 27001, y someternos a auditorías internas y externas para verificar el cumplimiento de los estándares de seguridad.
- Además, planeamos aumentar la inversión en tecnologías de seguridad avanzadas y mejorar los programas de capacitación en seguridad de la información para todo el personal.

Anexo 2

REPÚBLICA
DEL ECUADOR

Memorando Nro. SIS-COL5B-2024-0060-M

Babahoyo, 22 de febrero de 2024

PARA: Mac Eduardo Enrique Galeas Guijarro

ASUNTO: AUTORIZACION DE ESTUDIO DE CASO "ANALISIS DE PROCEDIMIENTOS PARA PREVENIR LA FILTRACIÓN DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE CONTROLES DE LA NORMA ISO 27001 EN EL CENTRO OPERATIVO LOCAL ECU 911 BABAHOYO".

De mi consideración:

Reciba un cordial y atento saludo señor Decano de la Facultad de Administración, Finanzas e Informática, en atención al Oficio N. D-FAFI-UTB-0179-2024 de fecha 16 de Febrero del presente año, y en conformidad al Convenio de Cooperación Interinstitucional entre el Servicio integrado de Seguridad ECU 911 y La Universidad Técnica de Babahoyo y; en virtud de la delegación de competencias, atribuciones y facultades otorgadas a los Jefes de Centros Operativos determinadas en la RESOLUCIÓN Nro. SISECU911-DG-2023-003 de fecha 23 de Enero del 2023 otorgadas por el señor Director General del Servicio Integrado de Seguridad ECU 911, se otorga el permiso institucional correspondiente para que el señor Ariel Oswaldo Pendolema Espinosa con cédula de ciudadanía N. 120631478-1 estudiante de la Carrera de Ingeniería en Sistemas de Información de la Facultad de Administración, Finanzas e Informática realice en las instalaciones del Centro Operativo Local ECU 911 Babahoyo el Estudio de Caso con su tema: "ANALISIS DE PROCEDIMIENTOS PARA PREVENIR LA FILTRACIÓN DE DATOS MEDIANTE LA IMPLEMENTACIÓN DE CONTROLES DE LA NORMA ISO 27001 EN EL CENTRO OPERATIVO LOCAL ECU 911 BABAHOYO", para lo cual se deberá alinear a los preceptos de confidencialidad determinadas por la institución.

Con sentimientos de distinguida consideración.

Atentamente,

Documento firmado electrónicamente

Ing. Diego Armando Soria Cordova (E)
JEFE DE CENTRO OPERATIVO LOCAL, ENCARGADO

Copia:
Srta. Ing. Dora Patricia Gomez Alvarado
Analista de Recursos Humanos Local

Anexo 3