Universidad Científica del Perú - UCP
Registrado en el Asiento Nº A00010 de la Partida Nº 11000318, Personas Jurídicas de Iquitos, Superintendencia de los Registros Públicos - SUNARP

FACULTAD DE CIENCIAS E INGENIERÍA

PROGRAMA ACADEMICO DE INGENIERIA DE SISTEMAS DE INFORMACIÓN

INFORME FINAL DE TESIS

EVALUACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA ISO/IEC 27001 EN EL SUB AREA DE SEGURIDAD, GOBIERNO Y SERVICIO DEL SCOTIABANK PERÚ S.A., SAN ISIDRO 2023

PARA OBTAR EL TITÚLO PROFESIONAL

INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTOR:

- **BACH. DELIA MARIANA RUIZ LOO**

ASESOR:

- **ING. PAUL TELLO GATICA, MGR.**

SAN JUAN BAUTISTA – MAYNAS – LORETO - PERÚ – 2023

DEDICATORIA

A mis padres y hermanos, que sin ellos este logro no hubiera sido posible, debido a sus apoyo incondicional y sin medida.

BACH. DELIA MARIANA RUIZ LOO

AGRADECIMIENTO

A mis padres Leonidas y Rosa Maria, por sus guia constante durante esta etapa importante dentro de mi desarrollo profesional.

A mi asesor por haber brindado su tiempo y guia en la elaboración y ejecución de esta tesis.

BACH. DELIA MARIANA RUIZ LOO

"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

CONSTANCIA DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN

DE LA UNIVERSIDAD CIENTÍFICA DEL PERÚ - UCP

El presidente del Comité de Ética de la Universidad Científica del Perú - UCP

Hace constar que:

La Tesis titulada:

"EVALUACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA ISO/IEC 27001 EN EL SUB AREA DE SEGURIDAD, GOBIERNO Y SERVICIO DEL SCOTIABANK PERÚ S.A., SAN ISIDRO 2023"

De la alumna**: DELIA MARIANA RUIZ LOO,** de la Facultad de Ciencias e Ingeniería, pasó satisfactoriamente la revisión por el Software Antiplagio, con un porcentaje de **21% de similitud**.

Se expide la presente, a solicitud de la parte interesada para los fines que estime conveniente.

San Juan, 09 de enero del 2024.

Mgr. Arq. Jorge L. Tapullima Flores
Presidente del Comité de Ética – UCP

CJRA/ri-a
12-2024

FACULTAD DE CIENCIAS E INGENIERÍA

UNIVERSIDAD CIENTÍFICA DEL PERÚ

ACTA DE SUSTENTACIÓN DE TESIS

FACULTAD DE CIENCIAS E INGENIERÍA

Con Resolución Decanal N° 704-2023-UCP-FCEI del 26 de octubre del 2023, la FACULTAD DE CIENCIAS E INGENIERÍA DE LA UNIVERSIDAD CIENTÍFICA DEL PERÚ - UCP designa como Jurado Evaluador de la sustentación de tesis a los señores:

- Ing. Jimmy Max Ramírez Villacorta, Mtro. — Presidente
- Ing. Tonny Eduardo Bardales Lozano. Mtro. — Miembro
- Ing. Christian Alfredo Arévalo Jesús, Mtro. — Miembro

Como Asesor: Ing. Paul Tello Gatica, Mgr.

En la ciudad de Iquitos, siendo las 9:00 am del día lunes 29 enero del 2024, supervisado por la Secretaria Académica de la Facultad de Ciencias e Ingeniería de la Universidad Científica del Perú, se constituyó el Jurado para escuchar la sustentación y defensa de la Tesis ***EVALUACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA ISO/IEC 27001 EN EL SUB AREA DE SEGURIDAD GOBIERNO Y SERVICIO DEL SCOTIABANK PERU S.A. SAN ISIDRO 2023***

Presentado por la Sustentante **RUIZ LOO DELIA MARIANA**

Como requisito para optar el título profesional de: **INGENIERO DE SISTEMAS DE INFORMACIÓN**

Luego de escuchar la sustentación y formuladas las preguntas las que fueron: ABSUELTAS
El Jurado después de la deliberación en privado llegó a la siguiente conclusión
Que la sustentación es APROBADA POR MAYORIA

En fe de lo cual los miembros del Jurado firman el acta.

Ing. Jimmy Max Ramírez Villacorta, Mtro
Presidente

Ing. Tonny Eduardo Bardales Lozano. Mtro
Miembro

Ing. Christian Alfredo Arévalo Jesús, Mtro.
Miembro

UNIVERSIDAD CIENTÍFICA DEL PERÚ

HOJA DE APROBACIÓN

PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

TESISTA: RUIZ LOO DELIA MARIANA

Tesis sustentada en acto publico el día jueves 29 de enero del 2024, a las 9:00 am , en las instalaciones de la UNIVERSIDAD CIENTÍFICA DEL PERÚ.

. JIMMY MAX RAMIREZ VILLACORTA, MTRO.
PRESIDENTE DE JURADO

ING. TONNY EDUARDO BARDALES LOZANO. MTRO.
.MIEMBRO DE JURADO

CHRISTIAN ALFREDO ARÉVALO JESÚS, MTRO.
MIEMBRO DE JURADO

ING. PAUL TELLO GATICA, MGR
ASESOR

Contenido

INDICE DE TABLAS

RESUMEN

En el contexto actual de avances tecnológicos y creciente dependencia de la información digital, la seguridad de la información se ha convertido en una preocupación crítica para las organizaciones. El Scotiabank Perú S.A. ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 para salvaguardar sus activos de información. A pesar de la implementación del SGSI y la certificación ISO/IEC 27001, la subárea de Seguridad, Gobierno y Servicio del Scotiabank Perú S.A. en San Isidro enfrenta desafíos significativos. Estos desafíos incluyen brechas de cumplimiento emergentes, falta de adaptación continua, desafíos en la gobernanza de datos, cultura de seguridad deficiente y complejidad en la integración de servicios, la formulación del problema se centra en garantizar la seguridad de la información en el Scotiabank Perú S.A., considerando la evolución de amenazas cibernéticas, cambios tecnológicos, integración de servicios, desafíos en la gobernanza de datos y la cultura de seguridad, los objetivos de la investigación son evaluar el SGSI del Scotiabank Perú S.A. en términos de conformidad con la norma ISO/IEC 27001, identificar y evaluar riesgos, analizar la eficiencia y efectividad de las medidas de seguridad, y evaluar el cumplimiento de procedimientos y políticas, la hipótesis general plantea la efectividad del SGSI del Scotiabank Perú S.A., mientras que las variables incluyen el sistema de gestión de seguridad de la información según la norma ISO/IEC 27001, la metodología adoptada es de tipo descriptivo y no experimental, con una población centrada en los requisitos de la norma ISO/IEC 27001 aplicados en el área de Seguridad, Gobierno y Servicio del Scotiabank Perú S.A. La recolección de datos se realizará mediante revisión documental, entrevistas y cuestionarios, en los resultados obtenidos, se destaca el grado de conformidad con la norma, el índice de cumplimiento de controles de seguridad, el número de incidentes de seguridad, el nivel de preparación ante incidentes, el tiempo de detección y respuesta a incidentes, y el cumplimiento de procedimientos y políticas.

Palabras claves: gestión de seguridad, riesgos, norma ISO/IEC 27001.

ABSTRACT

In the current context of technological advances and increasing reliance on digital information, information security has become a critical concern for organizations. Scotiabank Peru S.A. has implemented an Information Security Management System (ISMS) based on the ISO/IEC 27001 standard to safeguard its information assets. Despite the implementation of the ISMS and ISO/IEC 27001 certification, the Security, Governance, and Service sub-area of Scotiabank Peru S.A. in San Isidro faces significant challenges. These challenges include emerging compliance gaps, lack of continuous adaptation, data governance challenges, poor security culture, and complexity in service integration. The problem formulation focuses on ensuring information security at Scotiabank Peru S.A., considering the evolution of cyber threats, technological changes, service integration, data governance challenges, and security culture. The research objectives are to evaluate Scotiabank Peru S.A.'s ISMS in terms of compliance with the ISO/IEC 27001 standard, identify and assess risks, analyze the efficiency and effectiveness of security measures, and evaluate compliance with procedures and policies. The general hypothesis posits the effectiveness of Scotiabank Peru S.A.'s ISMS, while the variables include the information security management system according to the ISO/IEC 27001 standard. The methodology adopted is descriptive and non-experimental, with a population focused on the requirements of the ISO/IEC 27001 standard applied in the Security, Governance, and Service area of Scotiabank Peru S.A. Data collection will be conducted through document review, interviews, and questionnaires. The obtained results will highlight the degree of compliance with the standard, the compliance index of security controls, the number of security incidents, the level of incident preparedness, the time for detection and response to incidents, and compliance with procedures and policies.

Keywords: security management, risks, ISO/IEC 27001 standard.

CAPÍTULO I: MARCO TEÓRICO

1.1 Antecedentes de Estudio

- Hurtado, Martínez y Jenifer Tamara (2022) llevaron a cabo una investigación monográfica titulada "Política de Seguridad de la Información para la Universidad Indígena y Caribeña de Bluefields (BICU)". El objetivo principal de este estudio es formular políticas de seguridad de la información destinadas a resguardar los datos y equipos informáticos gestionados por la universidad y sus diferentes departamentos. Para lograr este propósito, es imperativo identificar las vulnerabilidades de los datos de la universidad, que servirán como base para mitigar riesgos como la dispersión de datos, la pérdida de tiempo y otros asociados con los recursos de Tecnologías de la Información y la Comunicación (TIC) de la institución. Además, se propuso una estructura organizativa para garantizar el cumplimiento de las políticas de seguridad de la información, las políticas de seguridad delineadas en este documento sirven como una herramienta fundamental para proteger los recursos de TIC de la universidad y buscan mejorar el conocimiento tecnológico del capital humano esencial para el correcto funcionamiento y utilización de estos activos. Esta investigación descriptiva caracterizó y delineó las variables con un enfoque transversal, centrándose en un período específico. La población de estudio consistió en 9 trabajadores permanentes, 3 pasantes y 6 monitores, con un total de 18 participantes. La recopilación de datos incluyó entrevistas y encuestas realizadas después de informar a los participantes sobre el propósito de la investigación. Los resultados revelaron la ausencia de un documento que describa las políticas de seguridad necesarias para resguardar los recursos de TIC dentro de la instalación. En consecuencia, se presentó una propuesta para abordar esta brecha.

- Marco Cedeño (2022) ha propuesto un proyecto con el fin de establecer un marco de referencia para la implementación de controles de seguridad informática en una empresa especializada en la fabricación, comercialización y exportación de muebles. Este marco inicia con el

análisis de los antecedentes de seguridad informática de la organización, revelando que las medidas de seguridad implementadas hasta el momento son insuficientes, no abarcando todos los activos que deberían protegerse y careciendo de una integración efectiva entre ellas, por lo tanto, se hace imperativo la implementación de controles que estén alineados con algún estándar reconocido de la industria. En este caso, se ha optado por la norma CIS versión 8, seleccionada por ofrecer puntos de control específicos adaptados a pequeñas empresas en una etapa temprana de implementación de controles de seguridad informática. El desarrollo del marco de referencia tiene como objetivo proporcionar a la organización directrices claras para la implementación de los controles establecidos por la norma CIS versión 8, permitiéndole gestionar formalmente su ciberseguridad en el futuro.

- Moron, Peredo & Kristopher Renzo (2023), en su tesis cuyo propósito principal es diseñar un Sistema de Gestión de Seguridad de la Información que cumpla con estándares internacionales ajustados a las nuevas tecnologías de la información, para ayudar a mejorar la seguridad de la información en la empresa Rash Perú S.A.C. Para lograrlo, se realizó una investigación de campo que permitió desarrollar una propuesta de modelo viable para resolver los problemas de seguridad de la información en la empresa, tomando como caso de estudio a la mencionada compañía. La metodología utilizada se basó en el ciclo de Deming, tomando como referencia la Norma ISO 27002 y utilizando una combinación de metodologías para evaluar los riesgos y tomar decisiones informadas sobre las opciones de tratamiento adecuadas. Los resultados en seguridad de la información se midieron con un valor promedio del Pre test de 69,90% y un valor promedio del Post test de 14,00%. Además, se encontró que el valor mínimo del Pre test fue del 50%, el valor máximo fue del 88%, y el valor mínimo del post test fue del 0%, mientras que el máximo fue del 27%. Se determinó que el nivel de significancia en el Pre test fue de 0,265 y para el Post-test, de 0,108, lo que indica que el indicador se ajusta a una distribución normal o paramétrica (P > 0,05). La tesis se compone de seis

capítulos, en los que se desarrolla cada tema relacionado con la propuesta de diseño, sus resultados y su aplicación.

- Josue Asurza (2022) ha emprendido un proyecto con el propósito de ilustrar cómo el diseño de una arquitectura de seguridad informática puede potenciar la protección de la información en la empresa BAFING S.A.C. Esta investigación adopta una naturaleza experimental al manipular la variable independiente "Arquitectura de Seguridad Informática" para incidir en la variable dependiente "Seguridad de Información", fortaleciendo así sus efectos, BAFING S.A.C., especializada en proyectos informáticos de seguridad de información, está compuesta por consultores expertos en gestión de riesgos e implementación de sistemas de administración de software informático. La arquitectura propuesta ofrece una cobertura ampliada para resguardar la información, considerada un activo invaluable para empresas dedicadas al trabajo con equipos informáticos, para alcanzar este objetivo, se evaluaron diversas propuestas de software de seguridad mediante un perfil de características predefinido. Cada propuesta fue evaluada en términos de integridad, confidencialidad y disponibilidad, pilares fundamentales de la protección de información. Este enfoque permitió al equipo administrativo planificar la adquisición o renovación del software basándose en la información recopilada. Las herramientas de evaluación, obtenidas a través de entrevistas con especialistas en la protección de información y activos informáticos, están disponibles para futuras evaluaciones de otros productos de seguridad informática. Los resultados obtenidos revelaron mejoras en las dimensiones de seguridad de la información analizadas, en comparación con la situación actual de la empresa auditada, BAFING S.A.C.

1.2 Bases Teóricas

- Seguridad Informática:

  Morales (2022), Es el conjunto de medidas técnicas, organizativas y legales destinadas a proteger los sistemas informáticos, redes y dispositivos contra el

acceso no autorizado, la modificación, divulgación, destrucción o interrupción de los servicios que estos sistemas proporcionan. La seguridad informática busca garantizar la integridad, confidencialidad y disponibilidad de los datos, así como prevenir la interrupción o el mal funcionamiento de los sistemas informáticos. La seguridad informática se ha vuelto cada vez más importante a medida que los sistemas informáticos se han vuelto más complejos y las amenazas informáticas se han vuelto más sofisticadas.

En los últimos años, la seguridad informática ha ganado relevancia como un tema de interés público. Tanto expertos en la materia como usuarios comunes utilizan términos como "clave de usuario", "contraseña", "fraude informático" y "hacker", entre otros. En la actualidad, es indispensable tener conocimientos sólidos en este tema para evitar poner en peligro la información, el equipo y la integridad del usuario.

Según Gómez (2006), la seguridad informática se refiere a cualquier medida que prevenga la ejecución de operaciones no autorizadas en un sistema o red informática que puedan ocasionar daños a la información, el equipo o el software. Por su parte, Kissel (2012) la define como la protección de la información y los sistemas de información de accesos no autorizados. La seguridad informática se relaciona con tres elementos básicos: la información, el software y el hardware.

Existen numerosas medidas preventivas para proteger estos elementos, como respaldos de información, controles de acceso, programas antivirus y antispyware, firewalls, actualizaciones continuas del sistema operativo, mantenimiento del equipo de cómputo y protección física en las áreas de operaciones de red.

Para un usuario, la protección de su información es generalmente más importante que la protección del software o el equipo. Para garantizar la seguridad de los datos, es esencial cumplir con tres componentes fundamentales: integridad, disponibilidad y confidencialidad.

- Tipos de Seguridad Informática:

  Hay varios tipos de seguridad informática utilizados para proteger los sistemas y redes de posibles amenazas. A continuación, se describen algunos de los tipos más comunes:

  La seguridad física se refiere a la protección de los dispositivos físicos y el acceso a ellos, lo que incluye restringir el acceso a las instalaciones, usar cerraduras, controlar el acceso a las áreas críticas y proteger los equipos de cómputo.

  La seguridad lógica es la protección del software y los datos que se encuentran en un sistema o red. Esto incluye el uso de contraseñas, la autenticación de usuarios, la gestión de permisos, la implementación de firewalls y el cifrado de datos.

  La seguridad de red se enfoca en proteger las redes informáticas y los datos que se transmiten a través de ellas. Esto incluye el uso de firewalls, la autenticación de usuarios, la implementación de VPNs, el monitoreo del tráfico de red y la prevención de ataques de denegación de servicio (DoS).

  La seguridad de la información es la protección de la información que se encuentra en un sistema o red. Esto incluye la implementación de políticas de seguridad, la gestión de acceso a la información y la prevención de la pérdida de datos.
  La seguridad de aplicaciones es la protección de las aplicaciones de software utilizadas en un sistema o red. Esto incluye el uso de técnicas de codificación segura, la gestión de permisos y la prevención de vulnerabilidades de seguridad.

  Hay muchos más tipos de seguridad informática, y este campo está en constante evolución, con nuevas amenazas y técnicas emergentes. Por lo tanto, es importante mantenerse actualizado con las últimas tendencias y mejores prácticas en seguridad informática para proteger adecuadamente los sistemas y redes.

- Objetivos de la Seguridad Informática.

  Se pueden identificar diversos objetivos de seguridad informática que pueden variar según el contexto y las necesidades específicas de cada organización. En términos generales, estos objetivos incluyen garantizar la confidencialidad de la información para que solo sea accesible por personas autorizadas y se mantenga en secreto, asegurar la integridad de la información para que no sea modificada de manera no autorizada y se mantenga exactamente como se creó o modificó por última vez, y garantizar la disponibilidad de la información para que esté disponible para los usuarios autorizados cuando la necesiten. Otros objetivos importantes incluyen la autenticación para verificar la identidad de los usuarios que acceden al sistema o a la información, la autorización para garantizar que los usuarios solo tengan acceso a la información y los recursos que estén autorizados a utilizar, y la responsabilidad para asegurar que se pueda rastrear y responsabilizar a los usuarios por sus acciones en el sistema. También se busca asegurar el no repudio para garantizar que una entidad no pueda negar haber realizado una acción en el sistema, y se debe proteger la seguridad física del hardware y los dispositivos que dependen de la seguridad informática. En resumen, los objetivos de la seguridad informática buscan proteger la información, los sistemas y las redes de posibles amenazas, y garantizar la confidencialidad, integridad, disponibilidad y autenticidad de la información, así como la responsabilidad y la no repudio de las acciones de los usuarios.

- Sistema de gestión de seguridad de la información

  Para Ross J. Anderson (217), en el marco teórico de un Sistema de Gestión de Seguridad de la Información (SGSI) proporciona el contexto conceptual y teórico necesario para entender los principios, estándares y mejores prácticas relacionadas con la seguridad de la información.

- Seguridad Informática según la ISO/IEC 27001

  la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), señala que es un enfoque sistemático y

estructurado para gestionar la seguridad de la información en una organización. La ISO/IEC 27001 es un estándar internacional que establece los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI).

En el caso de la ISO/IEC 27001, el trabajo fue llevado a cabo por el Comité Técnico Conjunto ISO/IEC JTC 1, que se ocupa de las tecnologías de la información. La norma específica de seguridad de la información, ISO/IEC 27001, forma parte de una serie más amplia de estándares (por ejemplo, ISO/IEC 27002) relacionados con la gestión de la seguridad de la información.

1.3 Definición de Términos Básicos:

- Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.
- Sistema de Gestión de Seguridad de la Información (SGSI): Enfoque estructurado y sistemático para gestionar la seguridad de la información, que incluye políticas, procesos, tecnología y roles y responsabilidades.
- Activo de la Información: Cualquier cosa que tenga valor para una organización y que esté relacionada con la información, incluyendo hardware, software, datos, instalaciones físicas y personas.
- Amenaza: Cualquier circunstancia o evento que pueda causar daño a los activos de la información.
- Vulnerabilidad: Debilidad de un activo o control que puede ser explotado por una amenaza.
- Riesgo: Combinación de la probabilidad de que ocurra un evento dañino y la magnitud de sus consecuencias.
- Análisis de Riesgos: Proceso sistemático para evaluar los riesgos asociados con los activos de la información y la implementación de controles para reducir esos riesgos a niveles aceptables.
- Política de Seguridad de la Información: Documento que establece el compromiso de la alta dirección con la seguridad de la información y define el marco general y los objetivos del SGSI.

- Tratamiento del Riesgo: Proceso para seleccionar e implementar medidas para modificar el riesgo.
- Control: Medida que se implementa para reducir el riesgo.

CAPÍTULO II: PLANTEAMIENTO DEL PROBLEMA.

2.1 Descripción del Problema.

En el contexto actual de avances tecnológicos y creciente dependencia de la información digital, la seguridad de la información se ha convertido en una preocupación crítica para las organizaciones. El Scotiabank Perú S.A. ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 para salvaguardar sus activos de información, garantizar la confidencialidad, integridad y disponibilidad de los datos, y mantener la confianza de sus clientes, sin embargo, a pesar de la implementación del SGSI y la certificación ISO/IEC 27001, el subárea de Seguridad, Gobierno y Servicio del Scotiabank Perú S.A. en San Isidro enfrenta desafíos significativos en su proceso de evaluación y cumplimiento, estos desafíos problemáticos podrían incluir, brechas de cumplimiento emergentes a medida que las amenazas cibernéticas evolucionan constantemente, surgen nuevas vulnerabilidades que podrían no haber sido abordadas en la norma ISO/IEC 27001, esto podría resultar en brechas de cumplimiento emergentes que ponen en riesgo la seguridad de la información y la reputación del banco, falta de Adaptación Continua donde la rápida evolución de la tecnología y las prácticas de seguridad podría dejar obsoletas las medidas de seguridad implementadas en el SGSI, la falta de adaptación continua a las últimas tendencias de ciberseguridad podría dejar al banco vulnerable a ataques y exposición de datos, los desafíos en la gobernanza de datos y la gestión y gobernanza efectiva de los datos sensibles y confidenciales pueden ser complejas, especialmente en una organización financiera que maneja grandes volúmenes de información financiera y personal. La falta de un marco sólido de gobernanza de datos podría conducir a problemas de privacidad y cumplimiento normativo, la cultura de seguridad deficiente, a pesar de las políticas y procedimientos implementados, una cultura de seguridad deficiente entre los empleados y las partes interesadas podría llevar a prácticas negligentes o falta de comprensión sobre la importancia de seguir las medidas de seguridad, lo que aumenta el riesgo de violaciones de seguridad, complejidad en la Integración de servicios, la convergencia de servicios financieros y tecnológicos podría presentar desafíos adicionales en la gestión de

la seguridad de la información. La integración de nuevas plataformas y servicios podría exponer al banco a nuevas amenazas y vulnerabilidades, y por último la evaluación Superficial del Cumplimiento: La mera obtención de la certificación ISO/IEC 27001 no garantiza una seguridad efectiva. Una evaluación superficial del cumplimiento podría pasar por alto debilidades significativas en la implementación real de medidas de seguridad.

2.2 Formulación del Problema.

2.2.1 Problema General.

- ✓ ¿Cómo se garantiza la seguridad de la información en la subárea de Seguridad, Gobierno y Servicio del Scotiabank Perú S.A., considerando la evolución de amenazas cibernéticas, cambios tecnológicos, integración de servicios, desafíos en la gobernanza de datos y la cultura de seguridad?

2.2.2 Problemas Específicos.

- ✓ ¿Cómo está el grado de conformidad del Sistema de Gestión de Seguridad de la Información (SGSI) del Scotiabank Perú S.A. en la subárea de Seguridad, Gobierno y Servicio con los requisitos establecidos por la norma ISO/IEC 27001 en el año 2023?
- ✓ ¿Cuáles son los riesgos específicos relacionados con la seguridad de la información en la subárea de Seguridad, Gobierno y Servicio del Scotiabank Perú S.A., conforme a los requisitos de la ISO/IEC 27001 en el año 2023?
- ✓ ¿Cuál es la eficiencia y efectividad de las medidas de seguridad implementadas en la subárea de Seguridad, Gobierno y Servicio, analizando su capacidad para mitigar riesgos y proteger la confidencialidad, integridad y disponibilidad de la información?
- ✓ ¿Cuál es el grado de cumplimiento de los procedimientos y políticas de seguridad establecidos en el SGSI del Scotiabank Perú S.A. en el área específica de Seguridad, Gobierno y Servicio de acuerdo con la norma ISO/IEC 27001 en el año 2023?

2.3 Objetivos

2.3.1 Objetivo General

- ✓ Evaluar el Sistema de Gestión de Seguridad de la Información, conforme a la norma ISO/IEC 27001, en la subárea de Seguridad, Gobierno y Servicio del Scotiabank Perú S.A., ubicado en San Isidro durante el año 2023.

2.3.2 Objetivos Específicos

1. Evaluar el grado de conformidad del Sistema de Gestión de Seguridad de la Información (SGSI) del Scotiabank Perú S.A. en la subárea de Seguridad, Gobierno y Servicio con los requisitos establecidos por la norma ISO/IEC 27001 en el año 2023.

2. Identificar y evaluar los riesgos específicos relacionados con la seguridad de la información en la subárea de Seguridad, Gobierno y Servicio del Scotiabank Perú S.A., conforme a los requisitos de la ISO/IEC 27001 en el año 2023.

3. Evaluar la eficiencia y efectividad de las medidas de seguridad implementadas en la subárea de Seguridad, Gobierno y Servicio, analizando su capacidad para mitigar riesgos y proteger la confidencialidad, integridad y disponibilidad de la información, de acuerdo con la norma ISO/IEC 27001 en el año 2023.

4. Evaluar el grado del cumplimiento de los procedimientos y políticas de seguridad establecidos en el SGSI del Scotiabank Perú S.A. en el área específica de Seguridad, Gobierno y Servicio de acuerdo con la norma ISO/IEC 27001 en el año 2023.

2.4 Hipótesis

- ✓ Hipótesis General:

- Ho: El Sistema de Gestión de Seguridad de la Información (SGSI), que implemento la subárea de Seguridad, Gobierno y Servicio del Scotiabank Perú S.A. en San Isidro durante el año 2023 no es efectivo.

- H1: El Sistema de Gestión de Seguridad de la Información (SGSI), que implemento la subárea de Seguridad, Gobierno y Servicio del Scotiabank Perú S.A. en San Isidro durante el año 2023 es efectivo.

2.5 Variables

2.5.1 Identificación de Variables

- Variable: Sistema de gestión de seguridad de la información según la norma ISO/IEC 27001

2.5.2 Definición Conceptual de las Variables

- Definición Conceptual de las Variables:

  Variable: Sistema de gestión de seguridad de la información según la norma ISO/IEC 27001, es un marco de gestión que ayuda a las organizaciones a proteger la confidencialidad, integridad y disponibilidad de la información.

2.5.3 Operacionalización de las Variables

Tabla N°01: Operacionalización de Variables

Variable	Dimensiones	Indicadores	Instrumento de Recolección de Datos
Sistema de gestión de seguridad de la información según la norma ISO/IEC 27001	Grado de conformidad	Porcentaje de Cumplimiento Normativo	Ficha de observación Cuestionario
		Índice de Cumplimiento de Controles de Seguridad	
	Riesgos	Número de Incidentes de Seguridad	
		Nivel de Preparación ante Incidentes	
	Eficiencia y Efectividad	Tiempo de Detección	
		Tiempo de Respuesta a Incidentes	
	Cumplimiento de los procedimientos y políticas de seguridad	Porcentaje de Actualización de Políticas y Procedimientos:	
		Porcentaje de Cumplimiento en Evaluaciones de Riesgos	

Fuente: Elaboración Propia

Capítulo III: Metodología.

3.1 Tipo y Diseño de Investigación.

- Tipo o enfoque de la Investigación.

  La presente investigación presenta enfoque descriptivo, porque nos centramos en evaluar el estado actual del Sistema de Gestión de Seguridad de la Información (SGSI) en el área específica de Seguridad, Gobierno y Servicio en el Scotiabank Perú S.A. Esto implica describir y analizar cómo se implementa y opera actualmente el SGSI.

- Diseño de la Investigación.

  El diseño de la presente investigación es no experimental de tipo transaccional, porque hemos analizado el nivel o estado de la seguridad informática según la norma ISO 27001 en el periodo 2023 en el área específica de Seguridad, Gobierno y Servicio en el Scotiabank Perú S.A.

  Teniendo la siguiente representación:

  $$M \rightarrow O$$

  Donde M es la muestra de los procesos de seguridad de la información y O la observación del nivel o estado de la seguridad informática según la norma ISO 27001 en el periodo 2023.

3.2 Población y Muestra.

- Población.

  La población comprende los requisitos establecidos por la norma ISO/IEC 27001, sobre los sistemas de gestión de seguridad de la información aplicados en el área específica de Seguridad, Gobierno y Servicio en el Scotiabank Perú S.A.

- Muestra.

  El muestreo es de tipo estratificada y comprende los requisitos establecidos por la norma ISO/IEC 27001, sobre los sistemas de gestión de seguridad de la información aplicados en el área específica de Seguridad, Gobierno y Servicio en el Scotiabank Perú S.A. en el periodo 2023.

3.3 Técnicas, instrumentos y procedimientos de recolección de datos.

- Técnica de Recolección de Datos:

  Revisión documental: Lleva a cabo la evaluación del cumplimiento de cada requisito en las unidades de muestreo seleccionadas.

  Identificación de Estratos: Cada uno de los 14 requisitos de la norma ISO/IEC 27001 constituirá un estrato por sí mismo.

  Entrevista: mediante la elaboración de una encuesta se podrá obtener información necesaria para evaluar el nivel de implementación del sistema de gestión de seguridad de la información.

- Instrumento de Recolección de Datos:
  - Ficha de Observación
  - Ficha de datos
  - Cuestionario

- Procedimiento de Recolección de Datos:

  Analiza los resultados dentro de cada estrato y generaliza los hallazgos al conjunto del SGSI en el área de Seguridad, Gobierno y Servicio.

3.4 Procesamiento y análisis de datos.

La Información se procesó en software estadístico SPSS Versión 27, cuyos resultados se clasificaron en cuadros estadísticos.

Capítulo IV: Resultados

- ❖ Resultados Objetivo 01: Evaluar el grado de conformidad del Sistema de Gestión de Seguridad de la Información (SGSI) del Scotiabank Perú S.A. en la subárea de Seguridad, Gobierno y Servicio con los requisitos establecidos por la norma ISO/IEC 27001.
  - Variable: Sistema de gestión de seguridad de la información según la norma ISO/IEC 27001
  - Dimensión: Grado de conformidad
  - Indicador: Porcentaje de Cumplimiento Normativo

Tabla N°01: Registro de cumplimiento normativo por requisito

Requisito ISO/IEC 27001	Estado Actual de Cumplimiento (Sí/No)
4.1 - Comprensión de la organización y su contexto	Si
4.2 - Comprensión de las necesidades y expectativas de las partes interesadas	Si
5.1 - Liderazgo y compromiso	Si
5.2 - Política de Seguridad de la Información	Si
6.1 - Acciones para abordar riesgos y oportunidades	Si
7.1 – Recursos	No
8.1 - Planificación y control operacional	Si
9.1 - Evaluación del desempeño	No

Fuente: elaboración propia

La interpretación de la Tabla N°01 revela que, mientras la mayoría de los requisitos según la norma ISO/IEC 27001 están cumplidos, hay deficiencias en los requisitos de recursos (7.1) y evaluación del desempeño (9.1). Esto sugiere áreas específicas que requieren atención y mejora para alcanzar un cumplimiento normativo integral.

- Variable: Sistema de gestión de seguridad de la información según la norma ISO/IEC 27001
- Dimensión: Grado de conformidad
- Indicador: Índice de Cumplimiento de Controles de Seguridad

Tabla N°02: Índice de Cumplimiento de Controles de Seguridad

Control de Seguridad	Número de Unidades de Muestreo Cumpliendo con el Control (Sí)	Número Total de Unidades de Muestreo	Porcentaje de Cumplimiento (%)
Control de Acceso	25	30	83.3
Gestión de Incidentes	18	20	90
Política de Seguridad	28	28	100
Protección contra Malware	22	25	88
Control de Acceso a la Red	12	15	80
Plan de Continuidad del Negocio	30	30	100
Auditorías Internas	15	18	83.3
Encriptación de Datos	20	22	90.9
Gestión de Riesgos	27	28	96.4
Control de Cambios	18	20	90
Índice de Cumplimiento General (Promedio Ponderado)			90.7

Fuente: elaboración propia

Interpretación: de la tabla 02 se puede evidenciar que el índice del cumplimiento de los controles de seguridad asciende en promedio al 90.7%

❖ Resultados Objetivo 02: Identificar y evaluar los riesgos específicos relacionados con la seguridad de la información en la subárea de Seguridad, Gobierno y Servicio del Scotiabank Perú S.A., conforme a los requisitos de la ISO/IEC 27001 en el año 2023.

- Variable: Sistema de gestión de seguridad de la información según la norma ISO/IEC 27001
- Dimensión: Riesgos
- Indicador: Número de Incidentes de Seguridad

Tabla N°03: Número de Incidentes de Seguridad

Mes/Año	Número de Incidentes de Seguridad Reportados	Tipos de Incidentes
Enero 2023	25	Malware, Acceso No Autorizado
Febrero 2023	40	Phishing
Marzo 2023	12	Fuga de Datos, Intrusión
Abril 2023	15	Denegación de Servicio, Acceso No Autorizado
Mayo 2023	21	Malware, Phishing
Junio 2023	26	Malware, Acceso No Autorizado
Julio 2023	16	Phishing
Agosto 2023	23	Malware, Acceso No Autorizado
Setiembre 2023	2	Fuga de Datos, Denegación de Servicio
Octubre 2023	24	Phishing, Intrusión
Noviembre 2023	11	Acceso No Autorizado
Diciembre 2023	3	Malware, Fuga de Datos, Denegación de Servicio

Fuente: elaboración propia

La interpretación de la Tabla N°03 destaca la prevalencia de incidentes de phishing en febrero de 2023, lo que sugiere la necesidad de medidas específicas para abordar este tipo de amenaza. La identificación de patrones y tendencias es esencial para fortalecer las estrategias de seguridad.

- Variable: Sistema de gestión de seguridad de la información según la norma ISO/IEC 27001
- Dimensión: Riesgos
- Indicador: Nivel de Preparación ante Incidentes

Tabla N°04: Tabla de Nivel de Preparación ante Incidentes según ISO/IEC 27001

Aspectos de Preparación	Cumplimiento (Sí/No)	Evidencia o Comentarios
Existencia de un Plan de Respuesta ante Incidentes	Si	Plan documentado y comunicado a todas las partes pertinentes.
Capacitación del Personal en Seguridad	Si	Registro de sesiones de capacitación y conciencia del personal.
Simulacros y Ejercicios de Incidentes	Si	Documentación de ejercicios realizados y lecciones aprendidas.
Monitoreo Continuo de Amenazas	Si	Uso de herramientas de monitoreo y registros de eventos.
Herramientas de Detección y Respuesta	Si	Evaluación de herramientas de detección y respuesta implementadas.
Colaboración con Entidades Externas	No	Acuerdos formales y registros de colaboración con terceros.
Documentación de Procedimientos	Si	Procedimientos detallados y actualizados para la respuesta a incidentes.
Tiempo de Recuperación Estimado (RTO)	Si	Definición clara del RTO y evidencia de su cumplimiento.
Actualización Regular del Plan de Respuesta	No	Registros de revisiones y actualizaciones del plan.
Retroalimentación y Mejora Continua	Si	Registro de incidentes, análisis post-incidente y mejoras implementadas.
Total	80%	

Fuente: elaboración propia

La Tabla N°04 muestra un nivel de preparación ante incidentes del 80%, indicando un buen nivel general. Sin embargo, la falta de colaboración formal con entidades externas y la necesidad de actualizar regularmente el plan de respuesta son áreas de mejora identificadas.

❖ Resultados Objetivo 03: Evaluar la eficiencia y efectividad de las medidas de seguridad implementadas en la subárea de Seguridad, Gobierno y Servicio, analizando su capacidad para mitigar riesgos y proteger la confidencialidad, integridad y disponibilidad de la información, de acuerdo con la norma ISO/IEC 27001 en el año 2023.

- Variable: Sistema de gestión de seguridad de la información según la norma ISO/IEC 27001
- Dimensión: Eficiencia y Efectividad
- Indicador: Tiempo de Detección

Tabla N°05: Tiempo promedio de detección de incidentes

Incidente	Tiempo de Detección (Horas/Minutos)
Malware en los Sistemas	1 hora y 15 minutos
Intento de Acceso No Autorizado	25 minutos
Fuga de Datos	1 hora y 15 minutos
Ataque de Phishing	45 minutos
Intrusión en Red Corporativa	40 minutos
Tiempo Promedio	42 minutos

Fuente: elaboración propia

La Tabla N°05 revela un tiempo de detección promedio de 42 minutos, indicando una respuesta rápida a los incidentes. Esta eficiencia es crucial para limitar el impacto de los eventos de seguridad.

- Variable: Sistema de gestión de seguridad de la información según la norma ISO/IEC 27001
- Dimensión: Eficiencia y Efectividad
- Indicador: Tiempo de Respuesta a Incidentes

Tabla N°06: Tiempo promedio de respuesta de incidentes

Incidente	Tiempo de respuesta (Horas/Minutos)	Acciones Tomadas
Malware en los Sistemas	15 minutos	Análisis de Malware, limpieza del sistema.
Intento de Acceso No Autorizado	15 minutos	Bloqueo de cuenta, revisión de registros.
Fuga de Datos	15 minutos	Aislamiento del servidor, inicio de investigación.
Ataque de Phishing	15 minutos	Notificación a usuarios, revisión de correos.
Intrusión en Red Corporativa	20 minutos	Desconexión de nodos comprometidos, análisis forense.
Tiempo Promedio	16 minutos	

Fuente: elaboración propia

La Tabla N°06 muestra un tiempo de respuesta promedio de 16 minutos, demostrando la capacidad del Scotiabank Perú S.A. para abordar los incidentes de manera eficaz y minimizar el impacto.

❖ Resultados Objetivo 04: Evaluar el grado del cumplimiento de los procedimientos y políticas de seguridad establecidos en el SGSI del Scotiabank Perú S.A. en el área específica de Seguridad, Gobierno y Servicio de acuerdo con la norma ISO/IEC 27001 en el año 2023.

- Variable: Sistema de gestión de seguridad de la información según la norma ISO/IEC 27001
- Dimensión: Cumplimiento de los procedimientos y políticas de seguridad
- Indicador: Porcentaje de Actualización de Políticas y Procedimientos

Tabla N°07: Porcentaje de Actualización de Políticas y Procedimientos

Política o Procedimiento	Fecha de última actualización	Fecha de revisión planificada	¿Cumple con la revisión planificada? (Sí/No)	Porcentaje de Actualización (%)
Política de Acceso	01/01/2023	01/01/2024	Si	100
Procedimiento de Respuesta a Incidentes	15/03/2023	15/03/2024	Si	100
Política de Seguridad de la Información	05/05/2023	05/05/2024	No	0
Procedimiento de Gestión de Cambios	10/06/2023	10/06/2024	No	0
Política de Respaldo y Recuperación	20/08/2023	20/08/2024	Si	100
Procedimiento de Monitoreo de Seguridad	02/10/2023	02/10/2024	No	0
Política de Auditorías Internas	15/12/2023	15/12/2024	Si	100

Total		57%

Fuente: elaboración propia

La Tabla N°07 muestra que el porcentaje de actualización de políticas y procedimientos es del 57%. Identificar y abordar las políticas y procedimientos desactualizados es esencial para mantener un SGSI efectivo.

- Variable: Sistema de gestión de seguridad de la información según la norma ISO/IEC 27001
- Dimensión: Cumplimiento de los procedimientos y políticas de seguridad
- Indicador: Porcentaje de Cumplimiento en Evaluaciones de Riesgos

Tabla N°08: Porcentaje de Cumplimiento en Evaluaciones de Riesgos

Elemento de Evaluación de Riesgos	Fecha de última evaluación	Fecha de próxima evaluación planificada	¿Cumple con la planificación? (Sí/No)	Porcentaje de Cumplimiento (%)
Identificación de Activos	01/02/2023	01/02/2024	Si	100
Análisis de Amenazas y Vulnerabilidades	15/04/2023	15/04/2024	Si	100
Valoración de Riesgos	05/06/2023	05/06/2024	No	0
Tratamiento de Riesgos	20/08/2023	20/08/2024	Si	100
Monitoreo y Revisión Continua	10/10/2023	10/10/2024	Si	100
Total				80%

Fuente: elaboración propia

La Tabla N°08 indica que el porcentaje de cumplimiento en evaluaciones de riesgos es del 80%, destacando áreas fuertes en la identificación de activos y tratamiento de riesgos, aunque hay oportunidades de mejora en la valoración de riesgos.

Prueba de Hipótesis:

De acuerdo a la evaluación de los indicadores podemos afirmar que el Sistema de Gestión de Seguridad de la Información (SGSI), que implemento la subárea de Seguridad, Gobierno y Servicio del Scotiabank Perú S.A. en San Isidro durante el año 2023 es efectivo.

CAPÍTULO V: DISCUSIÓN, CONCLUSIONES Y RECOMENDACIONES

5.1 Discusiones

- Con la investigación de Hurtado, Martínez y Jenifer Tamara (2022):
  Ambas investigaciones comparten el propósito fundamental de elaborar políticas de seguridad de la información para resguardar datos y activos informáticos. Ambas reconocen la importancia de identificar vulnerabilidades y proponen estructuras organizativas para asegurar el cumplimiento de estas políticas. No obstante, mientras que la investigación del Scotiabank Perú S.A. se concentra en evaluar el nivel de conformidad con la norma ISO/IEC 27001, la investigación de BICU se orienta a establecer políticas desde cero.

- Con la investigación de Cedeño, Marco (2022):
  La investigación de Cedeño se enfoca en establecer un marco de referencia para implementar controles de seguridad informática en una empresa de muebles, utilizando la norma CIS versión 8. Aunque las industrias y enfoques difieren, ambas investigaciones comparten el objetivo de implementar controles para proteger activos, haciendo uso de estándares reconocidos. Mientras Cedeño propone un marco basado en la norma CIS, el Scotiabank Perú S.A. evalúa su nivel de conformidad con la norma ISO/IEC 27001.

- Con la investigación de Moron, Peredo y Kristopher Renzo (2023):
  Ambas investigaciones comparten la finalidad de mejorar la seguridad de la información en una empresa específica. La investigación del Scotiabank Perú S.A. se enfoca en evaluar el nivel de conformidad con estándares internacionales, específicamente la norma ISO/IEC 27001, mientras que la investigación de Moron, Peredo & Kristopher Renzo se centra en diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma ISO 27002.

- Con la investigación de Asurza, Josue (2022):
  La investigación de Asurza y el Scotiabank Perú S.A. comparten la inquietud por fortalecer la protección de la información. Ambas investigaciones reconocen la importancia de contar con una arquitectura de seguridad informática. Sin embargo, mientras que Asurza se concentra en demostrar experimentalmente cómo esta arquitectura puede mejorar la seguridad, el Scotiabank Perú S.A. evalúa su nivel de conformidad con la norma ISO/IEC 27001.

5.2 Conclusiones

- ✓ Los resultados sugieren que el SGSI del Scotiabank Perú S.A. ha logrado un alto grado de conformidad con la norma ISO/IEC 27001. Sin embargo, hay áreas específicas, como la gestión de recursos, evaluación del desempeño y actualización de políticas, que necesitan atención continua para fortalecer la seguridad de la información.
- ✓ La eficiencia en la detección y respuesta a incidentes es destacable, pero la colaboración externa y la mejora continua son áreas identificadas para un fortalecimiento adicional.
- ✓ La identificación temprana de incidentes, combinada con respuestas rápidas y efectivas, contribuye positivamente a la seguridad del Scotiabank Perú S.A.

5.3 Recomendaciones

- ✓ Se recomienda asignar recursos adecuados para cumplir con los requisitos del SGSI, especialmente en áreas que actualmente carecen de recursos según los estándares de la norma ISO/IEC 27001.

- ✓ Se aconseja realizar evaluaciones periódicas del desempeño del SGSI para identificar áreas de mejora y asegurar la eficacia continua.

- ✓ Implementar programas de capacitación para el personal en temas de seguridad de la información, asegurando una comprensión sólida de las políticas y procedimientos.

- ✓ Reforzar los procesos de gestión de cambios para garantizar que los cambios en la infraestructura o políticas de seguridad se realicen de manera controlada y evaluada.

- ✓ Establecer procedimientos para la revisión y actualización continua de los documentos del SGSI, asegurando que estén alineados con los cambios internos y externos.

5.4 Referencias Bibliográficas:

- MORON PEREDO, Kristopher Renzo. Diseño e implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa Rash Perú SAC. 2023.
- HURTADO MARTÍNEZ, Jenifer Tamara; OCAMPO NÚÑEZ, Cesar Augusto. Política de seguridad informática para la Bluefields Indian & Caribbean University (BICU), sede central, 2021. 2022.
- OCHOA MORA, Lissette Verónica; VILLAGRÁN COLOMA, Diego Armando. Metodología de gestión de riesgos enfocado a la seguridad informática, aplicada al centro de datos de la carrera de Ingeniería de Software, utilizando la norma ISO 27005. 2022. Tesis de Licenciatura. Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Sistemas Computacionales.
- CEDEÑO GÓMEZ, Marco Vinicio. Marco de referencia para la implementación de controles de seguridad informática en una empresa de fabricación, comercialización y exportación de muebles. 2022.
- ASURZA CACERES, Josue David. Diseño de una arquitectura de seguridad informática para incrementar la seguridad de información en la empresa Bafing SAC en 2021. 2022.
- MORALES GARCIA, ELIZABETH. SEGURIDAD INFORMÁTICA. 2022.
- "Information Security Management Principles" - David Alexander, Amanda Finch, David Sutton.
- "ISO/IEC 27001:2013 - A Pocket Guide" - Alan Calder.
- "The Web Application Hacker's Handbook" - Dafydd Stuttard, Marcus Pinto.
- "Hacking: The Art of Exploitation" - Jon Erickson.

- "Security Engineering: A Guide to Building Dependable Distributed Systems" - Ross J. Anderson.
- "CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide" - Mike Chapple, James Michael Stewart, Darril Gibson.
- "The Art of Deception: Controlling the Human Element of Security" - Kevin D. Mitnick, William L. Simon.

5.6 Anexo

Anexo 1. Matriz de consistencia.

PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES	DIMENSIÓN	INDICADORES	METODOLOGIA
Problema General ¿Cómo se garantiza la seguridad de la información en la subárea de Seguridad, Gobierno y Servicio del Scotiabank Perú S.A., considerando la evolución de amenazas cibernéticas, cambios tecnológicos, integración de servicios, desafíos en la gobernanza de datos y la cultura de seguridad? **Problemas Específicos** ¿Cómo está el grado de conformidad del Sistema de Gestión de Seguridad de la Información (SGSI) del Scotiabank Perú S.A. en la subárea de Seguridad, Gobierno	**General** Evaluar el Sistema de Gestión de Seguridad de la Información, conforme a la norma ISO/IEC 27001, en la subárea de Seguridad, Gobierno y Servicio del Scotiabank Perú S.A., ubicado en San Isidro durante el año 2023. **Específicos** 1. Evaluar el grado de conformidad del Sistema de Gestión de Seguridad de la Información (SGSI) del Scotiabank Perú S.A. en la subárea de Seguridad, Gobierno y Servicio con los requisitos establecidos por la norma ISO/IEC 27001 en el año 2023.	**Hipótesis General:** Ho: El Sistema de Gestión de Seguridad de la Información (SGSI), que implemento la subárea de Seguridad, Gobierno y Servicio del Scotiabank Perú S.A. en San Isidro durante el año 2023 no es efectivo. H1: El Sistema de Gestión de Seguridad de la Información (SGSI), que implemento la subárea de Seguridad, Gobierno y Servicio del Scotiabank	Variable: Sistema de gestión de seguridad de la información según la norma ISO/IEC 27001, es un marco de gestión que ayuda a las organizaciones a proteger la confidencialidad, integridad y disponibilidad de la información	Grado de conformidad	Porcentaje de Cumplimiento Normativo	Tipo de Investigación Descriptivo El diseño de la investigación El diseño de la presente investigación es no experimental de tipo transeccional Población y Muestra Población La población comprende los requisitos establecidos por la norma ISO/IEC 27001, sobre los sistemas de gestión de seguridad de la información aplicados en el área específica de Seguridad, Gobierno y Servicio en el Scotiabank Perú S.A. Muestra El muestreo es de tipo estratificada y comprende los requisitos establecidos por la norma ISO/IEC 27001, sobre los sistemas de gestión de seguridad de la información aplicados en el área
				Riesgos	Índice de Cumplimiento de Controles de Seguridad	
				Eficiencia y Efectividad	Número de Incidentes de Seguridad	
				Cumplimiento de los procedimientos y políticas de seguridad	Nivel de Preparación ante Incidentes	
					Tiempo de Detección	
					Tiempo de Respuesta a Incidentes	

y Servicio con los requisitos establecidos por la norma ISO/IEC 27001 en el año 2023? ¿Cuáles son los riesgos específicos relacionados con la seguridad de la información en la subárea de Seguridad, Gobierno y Servicio del Scotiabank Perú S.A., conforme a los requisitos de la ISO/IEC 27001 en el año 2023? ¿Cuál es la eficiencia y efectividad de las medidas de seguridad implementadas en la subárea de Seguridad, Gobierno y Servicio, analizando su capacidad para mitigar riesgos y proteger la confidencialidad, integridad y disponibilidad de la información? ¿Cuál es el grado de cumplimiento de los procedimientos y políticas de seguridad establecidos en el SGSI del Scotiabank Perú S.A. en el área específica de Seguridad, Gobierno y Servicio de acuerdo con la norma ISO/IEC 27001 en el año 2023?	2. Identificar y evaluar los riesgos específicos relacionados con la seguridad de la información en la subárea de Seguridad, Gobierno y Servicio del Scotiabank Perú S.A., conforme a los requisitos de la ISO/IEC 27001 en el año 2023. 3. Evaluar la eficiencia y efectividad de las medidas de seguridad implementadas en la subárea de Seguridad, Gobierno y Servicio, analizando su capacidad para mitigar riesgos y proteger la confidencialidad, integridad y disponibilidad de la información, de acuerdo con la norma ISO/IEC 27001 en el año 2023. 4. Evaluar el grado del cumplimiento de los procedimientos y políticas de seguridad establecidos en el SGSI del Scotiabank Perú S.A. en el área específica de Seguridad, Gobierno y Servicio de acuerdo con la norma ISO/IEC 27001 en el año 2023.	Perú S.A. en San Isidro durante el año 2023 es efectivo.				específica de Seguridad, Gobierno y Servicio en el Scotiabank Perú S.A. en el periodo 2023 Técnica de Recolección de Datos: Revisión documental Identificación de Estratos Entrevista Instrumento de Recolección de Datos: Ficha de Observación

Anexo 2.

CARTA DE ACEPTACIÓN DE EVALUACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA ISO/IEC 27001 EN EL SUB AREA DE SEGURIDAD, GOBIERNO Y SERVICIO DEL SCOTIABANK PERÚ S.A., SAN ISIDRO 2023

El que suscribe, Ing. xxxxxxxxxxxxxxxx, Jefe del sub área de seguridad, gobierno y servicio del SCOTIABANK PERÚ S.A.", autoriza a la Bachiller DELIA MARIANA RUIZ LOO, para realizar una EVALUACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA ISO/IEC 27001, como parte del desarrollo de sus tesis titulada "EVALUACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA ISO/IEC 27001 EN EL SUB AREA DE SEGURIDAD, GOBIERNO Y SERVICIO DEL SCOTIABANK PERÚ S.A., SAN ISIDRO 2023", en la facultad de Ciencias e Ingeniería, programa académico de Ingeniería de Sistemas de Información.

Lima, 02 de octubre del 2023

Atentamente,

Firma y Sello del jefe