1. INTRODUCCIÓN

La protección de la seguridad de los activos de información es un desafío actual que enfrentan muchas organizaciones a nivel mundial. Dado que es difícil crear conciencia y establecer directrices para una gestión adecuada de la información, nuestra organización ha decidido implementar un Sistema de Gestión de Seguridad de la Información (SGSI) para gestionar de manera efectiva la seguridad de nuestros activos de información. Este manual describe las políticas, procedimientos, roles, documentos y herramientas que nuestra organización utiliza para alinear nuestros procesos de negocio con los objetivos de seguridad de la información, con el fin de agregar valor a nuestros accionistas, clientes y colaboradores, y mantener su confianza en la gestión de nuestra infraestructura tecnológica.

2. OBJETIVOS

El propósito de este Manual del Sistema de Gestión de Seguridad de la Información es proporcionar una guía detallada sobre las políticas, directivas y acciones necesarias para implementar un Sistema de Gestión de Seguridad de la Información efectivo. El objetivo principal es reducir al mínimo las vulnerabilidades y amenazas de seguridad de la información que puedan afectar los activos de información de la organización.

3. ANALISIS FODA

Con la finalidad de identificar factores internos y externos que puedan impactar en la implementación del SGSI se realiza el siguiente análisis FODA:

FORTALEZAS (Interno - Positivo)	OPORTUNIDADES (Externo - Positivo)
Conciencia inicial de la importancia de la seguridad de la información en la empresa.	Crecimiento en la demanda de servicios con certificación en seguridad de la información.
Existencia de una infraestructura tecnológica básica para implementar controles de seguridad.	Normativas y regulaciones cada vez más estrictas, incentivando la adopción de estándares como ISO/IEC 27001:2022.
Compromiso de la alta dirección en fortalecer la seguridad de la información.	Mayor interés de clientes y proveedores en empresas que cumplen con estándares de seguridad.
Disponibilidad de talento en TI con conocimientos básicos en ciberseguridad.	Posibilidad de obtener ventajas competitivas en el mercado con la certificación en ISO 27001.
Disposición de algunos procesos de gestión de riesgos previos, aunque no estructurados bajo un SGSI.	Acceso a financiamiento o incentivos para la implementación de normas de seguridad.
DEBILIDADES (Interno - Negativo)	**AMENAZAS (Externo - Negativo)**
Falta de un marco formal para gestionar la seguridad de la información.	Aumento de ciberataques dirigidos a empresas en el sector.
Desconocimiento del personal sobre buenas prácticas en seguridad de la información.	Cambios en normativas gubernamentales que podrían requerir ajustes constantes.
No existe un proceso formal para la gestión de incidentes de seguridad.	Dependencia de terceros en algunos servicios de TI sin garantías de seguridad adecuadas.
Falta de un análisis de riesgos detallado para identificar vulnerabilidades críticas.	Posibles costos de remediación elevados en caso de una brecha de seguridad.
Limitada asignación de recursos para proyectos de ciberseguridad.	Evolución de amenazas cibernéticas con el uso de inteligencia artificial.
No se cuenta con procesos documentados para asegurar la continuidad del negocio ante incidentes de seguridad.	Posible impacto en la reputación de la empresa en caso de un incidente de seguridad significativo.

Este análisis revela que, la implementación del SGSI cuenta con factores positivos como el compromiso de la alta dirección, una infraestructura tecnológica básica y un equipo de TI con conocimientos generales en seguridad. Sin embargo, existen debilidades críticas, como la falta de un marco formal de seguridad, desconocimiento del personal sobre buenas prácticas y la ausencia de un análisis de riesgos detallado.

Las oportunidades externas, como el crecimiento en la demanda de empresas certificadas en seguridad y la existencia de normativas más estrictas, refuerzan la necesidad de implementar un SGSI. No obstante, las amenazas como el incremento de ciberataques y la evolución de las amenazas digitales presentan riesgos significativos.

Este análisis justifica la necesidad de implementar un SGSI basado en la norma ISO/IEC 27001:2022, ya que permite establecer un marco formal de seguridad, reducir vulnerabilidades y mejorar la resiliencia de la empresa ante amenazas cibernéticas.

4. ANALISIS DE STAKEHOLDERS

Con el propósito de gestionar de forma adecuada las expectativas de lo stakeholders se muestra un mapa de clasificándolos según su influencia e interés en la implementación del SGSI. Donde:

Alta influencia, alto interés → Gestión Activa (Involucramiento directo)

Alta influencia, bajo interés → Mantener Satisfechos (Informar estratégicamente)

Baja influencia, alto interés → Mantener Informados (Participación parcial)

Baja influencia, bajo interés → Monitorear (Vigilancia pasiva)

INFLUENCIA / INTERÉS	ALTO INTERÉS	BAJO INTERÉS
ALTA INFLUENCIA	Alta Dirección: Gerentes y Directivos Reguladores: Organismos de cumplimiento y normativas de seguridad de la información, INDECOPI, PCM, SBS	Proveedores estratégicos de TI y ciberseguridad
BAJA INFLUENCIA	Empleados de la empresa Usuarios finales: Internos y externos de los sistemas de información	Proveedores no críticos

Alta Influencia, Alto Interés (Gestión Activa)

- La **Alta Dirección** es clave en la toma de decisiones y asignación de recursos para la implementación del SGSI.
- Los **Reguladores** supervisan el cumplimiento de normativas y estándares de seguridad de la información, por lo que requieren una gestión activa y alineada con sus requisitos.

Alta Influencia, Bajo Interés (Mantener Satisfechos)

- **Proveedores estratégicos de TI y ciberseguridad** pueden influir en la seguridad del SGSI, pero su nivel de involucramiento puede variar. Es crucial garantizar su cumplimiento de estándares.

Baja Influencia, Alto Interés (Mantener Informados)

- **Empleados y usuarios finales** deben estar informados y capacitados, ya que su comportamiento afecta directamente la efectividad del SGSI.
- Se deben implementar campañas de concienciación en seguridad de la **información**.

Baja Influencia, Bajo Interés (Monitorear)

- Proveedores no críticos **pueden ser considerados en la estrategia de seguridad, pero con un nivel de monitoreo menor.**

5. MATRIZ DE REQUISITOS DEL SGSI

Esta matriz permite hacer un seguimiento estructurado de los requisitos del SGSI, asegurando que se. cumpla con los estándares, normativas y buenas prácticas necesarias para fortalecer la seguridad de la información.

ID	CATEGORÍA	REQUISITO	FUENTE	RESPONSABLE	EVIDENCIA DE CUMPLIMIENTO	ESTADO
R1	Normativo	Cumplir con los requisitos de la norma **ISO/IEC 27001:2022**	ISO/IEC 27001:2022	Responsable del SGSI	Manual del SGSI, Declaración de Aplicabilidad, Procedimientos documentados	
R2	Legal	Cumplir con la Ley de Protección de Datos Personales en Perú (Ley N° 29733)	Ley No 29733	Departamento Legal / Responsable del SGSI	Políticas de privacidad, Procedimientos de gestión de datos personales	
R3	Legal	Cumplimiento con regulaciones de la **SBS (Superintendencia de Banca y Seguros)** sobre seguridad de la información	Normativa SBS	Oficial de Seguridad de la Información (CISO)	Informes de cumplimiento, Auditorías internas	
R4	Contractual	Garantizar que los proveedores de TI cumplan con estándares de seguridad de la información	Contratos de servicio	Departamento de Compras / Responsable del SGSI	Acuerdos de Nivel de Servicio (SLA), Cláusulas de seguridad	
R5	Operativo	Implementar controles para asegurar la **confidencialidad, integridad y disponibilidad**	Análisis de Riesgos	Responsable del SGSI / TI	Registros de incidentes, Informes de pruebas de seguridad	

		de la información				
R6	Capacitación	Sensibilizar y capacitar a los empleados en buenas prácticas de seguridad de la información	Programa de Formación	Recursos Humanos / Responsable del SGSI	Registros de capacitaciones, Evaluaciones de conocimiento	
R7	Auditoría	Realizar auditorías internas periódicas para evaluar el cumplimiento del SGSI	Plan de Auditoría	Auditor Interno	Informes de auditoría, Plan de acción correctivo	
R8	Continuidad	Desarrollar y probar un **Plan de Continuidad del Negocio (BCP)**	Análisis de Impacto al Negocio (BIA)	Comité de Continuidad	Documento del BCP, Evidencia de simulacros	

6. ALCANCE DEL MANUAL DE SEGURIDAD DE LA INFORMACIÓN

El presente manual tiene un alcance que abarca los procesos de negocio de la organización, y se basa en los requisitos establecidos por la norma ISO/IEC 27001:2022. Además, el contenido de este manual es aplicable a todos los empleados y colaboradores de la organización, quienes deben seguir las directrices y procedimientos establecidos.

7. MATRIZ RACI PARA EL SGSI

Se define la matriz RACI con los roles necesarios para asegurar una implementación efectiva del SGSI:

Actividad / Proceso	Alta Dirección	Responsable SGSI	TI / Seguridad	RRHH	Usuarios / Áreas	Auditor Interno
Definir el alcance del SGSI	A	R	C	I	I	I
Identificación y clasificación de activos de información	A	R	C	I	I	I
Análisis y evaluación de riesgos	A	R	C	I	I	C
Definir la Declaración de Aplicabilidad (SoA)	A	R	C	I	I	C
Desarrollar políticas y procedimientos de seguridad	A	R	C	C	I	I
Implementar controles de seguridad	I	R	A	I	I	I
Gestión de incidentes de seguridad	I	R	A	I	I	C
Capacitación y sensibilización en seguridad	I	R	C	A	I	I
Auditorías internas del SGSI	I	R	C	I	I	A
Revisión del SGSI por la Alta Dirección	A	R	C	I	I	C
Mejora continua del SGSI	A	R	C	I	I	C

8. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

8.1. VISIÓN GENERAL

Debido a la gran dependencia de la organización en sus sistemas de información y la confidencialidad de la información que maneja, tanto propia como de clientes, se ha decidido implementar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2022. Esta decisión estratégica se alinea con las necesidades, objetivos y requisitos de seguridad de la organización, y se apoya en los procesos internos. A continuación, se presentan los lineamientos estratégicos que rigen la organización y respaldan el Sistema de Gestión de Seguridad de la Información.

8.2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información se incluye como anexo del presente proyecto y tiene como objetivo principal establecer las directrices y procedimientos para garantizar la gestión adecuada de la Seguridad de la Información dentro de la organización, en cumplimiento con las disposiciones legales vigentes, y proteger los activos de información y la información propia de cada área de la organización.

8.3. COMPROMISO DE LA DIRECCIÓN

La Alta Dirección de la organización se compromete a garantizar el éxito del Sistema de Gestión de Seguridad de la Información (SGSI), adoptando un enfoque de mejora continua que incluye planificación, implementación, monitoreo y evaluación. Para lograr esto, la Alta Dirección asume los siguientes compromisos:

- Conocer y considerar los controles establecidos en el anexo A de la norma ISO/IEC 27001:2022.

- Comunicar los requisitos de la norma a los gerentes y jefes de área, y asegurarse de que se comuniquen a todos los colaboradores.
- Realizar capacitaciones sobre conciencia de seguridad de la información para todo el personal.
- Asignar recursos necesarios para minimizar los riesgos de seguridad de la información.
- Delegar responsabilidades al Comité de Gestión de Seguridad de la Información (CGSI) y supervisar su desempeño.
- Asignar responsabilidades al Dueño del Riesgo para seguir y evaluar la efectividad de los controles de seguridad.
- Designar un Oficial de Seguridad de la Información para proponer metodologías y procedimientos de seguridad, y apoyar al Dueño del Riesgo en la evaluación de controles.

8.4. PLANIFICACIÓN DEL SGSI

Aunque el presente proyecto se centra en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) para la organización, es importante destacar que existen cuatro fases clave para su implementación y revisión posterior, los que están alineados con el Ciclo Deming de Mejora Continua (PDCA: Plan-Do-Check-Act) y los requisitos de la ISO/IEC 27001:2022.

- Fase 1: Planificación del SGSI.
- Fase 2: Implementación del SGSI.
- Fase 3: Evaluación del SGSI a través de auditorías internas y externas.
- Fase 4: Mejora continua del SGSI mediante la retroalimentación

Se presenta una tabla que permite visualizar la secuencia y relación entre los procesos clave para la implementación y mejora del SGSI.

FASE	ALCANCE
1. PLANIFICACIÓN (PLAN)	Alta Dirección: Lineamientos Definir alcance del SGSI Identificación de activos de información Análisis de riesgos Establecer Declaración Aplicabilidad (SoA) Desarrollo de Políticas y Procedimientos
2. IMPLEMENTACIÓN (DO)	Aplicación de controles de seguridad Gestión de incidentes de seguridad Formación y sensibilización Gestión de accesos Implementación de medidas correctivas
3. EVALUACIÓN Y MONITOREO (CHECK)	Auditorías internas Revisión de cumplimiento Monitoreo de incidentes Evaluación de desempeño del SGSI Revisión por la Alta Dirección
4. MEJORA CONTINUA (ACT)	Gestión de acciones correctivas Actualización del Análisis de Riesgos Revisión y mejora de políticas Revisión de procedimientos

9. VALORIZACIÓN DEL RIESGO POR PARTE DE LA ORGANIZACIÓN

9.1. METODOLOGÍA PARA LA EVALUACIÓN DE LOS RIESGOS

La organización utiliza una metodología propia para evaluar los riesgos de seguridad de la información, basada en la norma ISO 31000. Esta metodología se compone de las siguientes etapas:

- Identificar los activos de información
- Valorar los activos de información
- Analizar y identificar vulnerabilidades y amenazas
- Evaluar y analizar los riesgos
- Crear una matriz de riesgos
- Establecer opciones para tratar los riesgos
- Realizar un seguimiento de los riesgos identificados.

Esta metodología integral permite a la organización gestionar de manera efectiva los riesgos de seguridad de la información.

9.2. CRITERIOS PARA LA EVALUACIÓN DE RIESGOS

La organización considera las siguientes premisas para evaluar los riesgos sobre los activos de información:

- La identificación de riesgos se basará en la experiencia y conocimiento de expertos internos que participan en los procesos relacionados con cada activo de información valorizado.
- Se contará con personal especializado en Seguridad de la Información para obtener una visión integral de los riesgos potenciales que afectan los activos de información.

- Se utilizarán documentos y mejores prácticas del mercado para evaluar los riesgos de seguridad de la información, lo que permitirá crear conciencia sobre los riesgos potenciales y adoptar medidas preventivas.

A continuación, se describe la metodología para valorar los riesgos sobre los activos de información.

Valores de Riesgo				
Escala		Valor	Nivel de Aceptación del Riesgo	
Muy Bajo	1-2	1	Insignificante	Riesgo aceptable para la empresa u organización
Bajo	3-6	2	Insignificante	Riesgo aceptable para la empresa u organización
Medio	7-9	3	Considerable	Riesgo inaceptable para la empresa u organización, se necesita la ejecución de un control de seguridad
Alto	10-16	4	Considerable	Riesgo inaceptable para la empresa u organización, se necesita la ejecución de un control de seguridad
Muy Alto	17-25	5	Importante	Riesgo inaceptable para la empresa u organización, se necesita la ejecución de un control de seguridad

Con base en la evaluación realizada, la organización tomará decisiones sobre el tratamiento de riesgos solo para aquellos que se clasifiquen como "Considerable" o "Importante", según el cuadro de evaluación de riesgos.

9.3. OPCIONES DE TRATAMIENTO DE RIESGOS

La organización ha establecido las siguientes opciones para tratar los riesgos:

- **Mitigación del Riesgo:** Reducir los niveles de riesgo a niveles aceptables mediante la implementación de controles de seguridad que se alineen con los objetivos de negocio.
- **Aceptación del Riesgo:** Aceptar el riesgo cuando no se puedan implementar controles efectivos, siempre y cuando se documenten los criterios utilizados para tomar esta decisión.
- **Transferencia del Riesgo:** Transferir el riesgo a otra parte cuando sea complicado reducir o controlar el riesgo a un nivel aceptable.
- **Eliminación del Riesgo:** Eliminar la fuente del riesgo, ya sea un activo, proceso o área de negocio, para evitar el riesgo asociado.

9.4. PLAN DE TRATAMIENTO DE RIESGOS

Después de realizar el Análisis de Riesgos sobre los activos de información, el Comité de Gestión de Seguridad de la Información (CGSI), el Oficial de Seguridad de la Información y el área responsable del activo de información en riesgo se reunirán para desarrollar un plan de tratamiento de riesgos para aquellos riesgos clasificados como "Considerables" o "Importantes". El Plan de Tratamiento de Riesgos seguirá un formato específico, que se describe a continuación.

IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS							
Código Activo	Nombre del Activo	Descripción del Activo	Tipo de Activo	Clasificación			Valor del Activo
				C	I	D	

ANÁLISIS Y EVALUACIÓN DE RIESGOS					
Vulnerabilidad	Amenaza	Descripción del Riesgo	Probabilidad	Impacto	Severidad

TRATAMIENTO DE RIESGOS			
Estrategia Respuesta	**Control ISO 27001: 2022**	**Descripción de la Estrategia**	**Responsable**

SEGUIMIENTO	
Estado	**Actividades Realizadas**

10. DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad (SOA) es un documento que resume las decisiones de la organización sobre el tratamiento de los riesgos de seguridad de la información. Además, en este documento se justifica la aplicación o no aplicación de cada control de seguridad en la organización. La Declaración de Aplicabilidad del Sistema de Gestión de Seguridad de la Información de la organización se incluye como anexo en el presente proyecto.

11. REQUISITOS DE DOCUMENTACIÓN

La organización asigna al Comité de Gestión de Seguridad de la Información y al Oficial de Seguridad de la Información la responsabilidad de gestionar la documentación del Sistema de Gestión de Seguridad de la Información, mediante las siguientes acciones:

- Revisar, aprobar y actualizar los documentos del sistema antes de su publicación.
- Asegurar que los documentos sean claros, fáciles de entender y cumplan con los objetivos de seguridad de la información.
- Garantizar la disponibilidad y distribución de los documentos a personal autorizado, según sus privilegios de acceso.
- Controlar y gestionar documentos obsoletos, actualizando o eliminando aquellos que ya no sean necesarios.

12. POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Las políticas que integran el Sistema de Gestión de Seguridad de la Información son de cumplimiento obligatorio para todos los empleados y colaboradores de la organización. Estas políticas tienen como objetivo establecer las acciones necesarias para proteger la información de los activos de información que son fundamentales para los procesos de negocio de la organización. A continuación, se presentan las políticas que componen este sistema:

- Política de Seguridad de la Información
- Política de Control de Acceso
- Política de Uso Aceptable de los Sistema de Información, Internet y Correo Electrónico
- Política de Puesto de Trabajo despejado y Bloqueo de Pantalla
- Política de Teletrabajo
- Política de Gestión de Incidentes de Seguridad de la Información
- Política y Procedimientos de Intercambio de Información

13. SEGUIMIENTO Y REVISIÓN DEL SGSI

Aunque el objetivo principal del presente proyecto es implementar un Sistema de Gestión de Seguridad de la Información (SGSI), la organización realizará auditorías internas y externas después de su implementación. Esto con el fin de evaluar el desempeño y cumplimiento del SGSI, asegurando que se ajuste a los estándares y requisitos establecidos.

14. MANTENER LA SEGURIDAD DE LA INFORMACIÓN EN NIVELES ÓPTIMOS

Es fundamental evaluar continuamente el rendimiento y la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) para asegurarse de que se ajuste a las necesidades y objetivos de la organización. Para ello, es importante considerar los requisitos de la norma ISO/IEC 27001:2022 y el Código de Buenas Prácticas establecido en la norma ISO/IEC

27002:2022, con el fin de garantizar que el SGSI cumpla con los estándares internacionales y apoye los objetivos organizacionales.

15. INCUMPLIMIENTO

El incumplimiento de las disposiciones establecidas en el presente Manual de Seguridad de la Información dará lugar a la aplicación de sanciones proporcionales a la gravedad y naturaleza de la infracción. Además, cualquier empleado que sea encontrado culpable de violar alguna de las políticas o procedimientos establecidos en este manual estará sujeto a medidas disciplinarias, que pueden incluir el despido o otras acciones que la organización considere adecuadas.

16. APROBACIÓN

Elaborado por	Verificado por	Aprobado por
Nombre **Oficial de Seguridad de la Información** Fecha:	Nombre **Gerente Administrativo** Fecha:	Nombre **Gerente General** Fecha: