1. INTRODUCCIÓN

La información es un recurso fundamental para la organización, con un valor importante que debe ser protegido adecuadamente. Esto implica garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y contribuir al cumplimiento de los objetivos de negocio.

Para que esta política sea efectiva, es esencial que forme parte de la cultura organizacional y que todos los trabajadores de la organización se comprometan a difundir, consolidar y cumplir con su contenido.

La organización ha adoptado políticas de seguridad de la información para proteger adecuadamente los activos de información seleccionados. Para ello, se ha utilizado como guía la norma ISO/IEC 27002:2022, que establece controles específicos para la aplicabilidad de controles necesarios después de realizar el análisis de riesgos asociados a los activos de información seleccionados.

2. TERMINOS Y DEFINICIONES OPERATIVAS

Con el fin de asegurar una comprensión clara y precisa de los conceptos presentados en este documento, se proporcionan definiciones de los términos más relevantes y utilizados. Esto permitirá una mejor interpretación y entendimiento del contenido.

2.1 SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se define como la preservación de los siguientes pilares fundamentales:

- **Confidencialidad**: Garantiza que la información sea accesible solo a personas autorizadas.
- **Integridad**: Salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad**: Garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados.

Además, se consideran los siguientes conceptos:

- **Autenticidad**: Asegura la validez de la información en tiempo, forma y distribución, y garantiza el origen de la información.
- **Auditabilidad**: Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- **Protección a la duplicación**: Asegura que una transacción solo se realice una vez, a menos que se especifique lo contrario.
- **No repudio**: Evita que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- **Legalidad**: Cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto la organización.
- **Confiabilidad de la Información**: La información generada es adecuada para sustentar la toma de decisiones y la ejecución de las funciones.

2.2 INFORMACIÓN

La información se define como cualquier comunicación o representación de conocimiento en forma de datos, incluyendo formatos textuales, numéricos, gráficos,

cartográficos, narrativos, audiovisuales y otros, almacenados o transmitidos a través de medios magnéticos, papel, pantallas de computadoras, audiovisuales u otros.

2.3 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Sistema de Gestión de una Organización, con base en un enfoque de riesgos, que tiene como función establecer, implementar, operar y supervisar la seguridad de la información, en un ciclo de mejora continua.

3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

3.1 OBJETIVOS

La presente política tiene como objetivos principales:

- Proteger los recursos de información de la Organización, garantizando la confidencialidad, integridad y disponibilidad de los activos de información, frente a amenazas internas o externas, deliberadas o accidentales.
- Asegurar la implementación y cumplimiento de las medidas de seguridad establecidas en esta política, responsabilidad que recae en la Estructura Organizacional de Gestión de Seguridad de la Información.
- Mantener la política actualizada y vigente, asegurando su eficacia y relevancia en la protección de la información de la Organización.

3.2 ALCANCE

Esta política de seguridad de la información es aplicable en todos los ámbitos de la organización, incluyendo:

- Todos los sistemas y recursos bajo control de la organización.
- La información almacenada, en uso o en tránsito a través de redes de voz o datos.

- El control de la información y los recursos de acceso a la misma.
- Todas las personas que acceden o utilizan los sistemas de información de la organización, incluyendo personal, contratistas y terceros.
- Todos los procesos y actividades relacionadas con el ciclo de vida de la información, desde su creación hasta su eliminación.

Esta política es de aplicación general y obligatoria para toda la organización.

3.3 DECLARACIÓN DE POLÍTICA

Nuestra política se basa en los principios establecidos en la Norma Internacional para la seguridad de la información - ISO/IEC 27001:2022. Nuestro compromiso es desarrollar y mantener un sistema de gestión de seguridad de la información que:

- Proporcione orientación y apoyo para la seguridad de los activos de información.
- Defina responsabilidades para empleados, socios, contratistas y terceros que acceden a recursos de la organización.
- Proporcione un marco para mantener la confidencialidad, integridad y disponibilidad de los recursos de la organización.
- Optimice la gestión de riesgos mediante la prevención y minimización del impacto de incidentes de seguridad.
- Asegure que las infracciones de seguridad sean reportadas, investigadas y abordadas adecuadamente.
- Garantice la revisión periódica de las políticas y procedimientos de seguridad para asegurar la continuidad de las buenas prácticas y la protección frente a nuevas amenazas.

- Comunique periódicamente los requisitos de seguridad de la información a todas las áreas pertinentes.

4. CUMPLIMIENTO

La organización se compromete a cumplir con todas las leyes y regulaciones peruanas relacionadas con el procesamiento y almacenamiento de información, incluyendo:

- La Ley de Protección de Datos Personales y su Reglamento.
- Requerimientos de legislación y normativa específica de clientes.
- Requerimientos contractuales establecidos en acuerdos comerciales.

Además, la organización cumplirá con los requisitos contractuales, normas y principios necesarios para mantener sus funciones de negocios, incluyendo:

- Protección de los derechos de propiedad intelectual.
- Protección de registros propios de la organización.
- Verificación de cumplimiento y procedimientos de auditoría.
- Prevención del uso indebido de instalaciones y acciones de remediación.
- Cumplimiento de códigos de conexión a redes y servicios de terceros.

La organización mantiene un listado actualizado de normatividad relevante para garantizar el cumplimiento de los requerimientos legales y contractuales.

4.1 REPORTE DE INCIDENCIA

Se alentará a los usuarios a informar cualquier infracción a la Política de Seguridad de la Información a través de una función específica en el Sistema de Gestión de Tickets. Esto incluye incidentes relacionados con:

- Uso indebido de equipos de tecnología de la información.

- Manejo incorrecto de datos, pérdida, abuso o cualquier otro incidente que pueda comprometer la seguridad.
- Infracciones a las políticas de la organización.

El Sistema de Gestión de Tickets incluye un procedimiento de gestión de incidencias para realizar acciones correctivas y de mejora, permitiendo una respuesta eficaz y oportuna ante incidentes de seguridad.

4.2 GESTIÓN DE INCIDENCIA

Cuando se presente una infracción, la persona que reporte el incidente deberá introducir los detalles del mismo a través del Sistema de Gestión de Tickets. Una vez registrado el reporte, se realizará un seguimiento según el procedimiento de gestión de incidentes de seguridad.

El Oficial de Seguridad de la Información (OSI) liderará la gestión del incidente, trabajando en conjunto con los líderes de área y las partes involucradas, para tomar medidas correctivas apropiadas y analizar la solución de los incidentes de seguridad.

5. ORGANIZACIÓN DE LA SEGURIDAD

La organización cuenta con una Estructura Organizacional del Sistema de Gestión de Seguridad de la Información (SGSI), diseñada para alcanzar los siguientes objetivos:

- Establecer un marco gerencial para administrar la seguridad de la información dentro de la organización.
- Definir roles y responsabilidades en materia de seguridad de la información.
- Fomentar la colaboración y consulta con organizaciones especializadas en seguridad de la información.

- Implementar medidas de seguridad y controles efectivos para proteger los activos de información, tanto interna como externamente.

5.1 SEGURIDAD DE LA INFORMACIÓN

Además, como se mencionó anteriormente, la organización de la seguridad se fundamenta en una Estructura Organizacional del Sistema de Gestión de Seguridad de la Información (SGSI), cuyos detalles se presentan a continuación:

5.1.1 COMITÉ DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (CGSI)

El CGSI es el ente máximo responsable de la seguridad de la información dentro de la organización. Sus funciones principales son:

- Revisar y proponer la Política de Gestión de Seguridad de la Información para su aprobación por la máxima autoridad.
- Gestionar la implementación, verificación y evaluación del Sistema de Gestión de Seguridad de la Información (SGSI).
- Difundir la importancia del SGSI dentro de la organización.
- Asignar roles y responsabilidades en materia de seguridad de la información a cada área.
- Promover un ambiente seguro y comprometido con la seguridad de la información.

El CGSI estará integrado por:

- El Gerente General
- El Gerente de Consultoría TI

- El Gerente Comercial
- El Gerente Administrativo y Financiero
- El Gerente de Recursos Humanos

5.1.2 COMITÉ DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (CGSI)

El GISI es responsable de garantizar que las actividades de Seguridad de la Información se ejecuten de acuerdo con la Política de Gestión de Seguridad de la Información. Sus funciones incluyen:

- Aprobar metodologías y procesos que fomenten la confianza y concientización en materia de Seguridad de la Información.
- Proporcionar un canal para que el personal de la organización pueda expresar sus dudas e inquietudes sobre Seguridad de la Información.
- Garantizar la implementación efectiva de la Política de SGSI.

En la organización, el GISI estará integrado específicamente por:

- Jefe de Servicios de Soporte Técnico
- Jefes de Proyectos
- Líderes de Equipos Técnicos

5.1.3 OFICIAL DE SEGURIDAD DE LA INFORMACIÓN (OSI)

El Oficial de Seguridad de la Información es responsable de:

- Proponer metodologías, procedimientos, herramientas y procesos para garantizar la seguridad de la información.
- Administrar incidentes y vulnerabilidades de los activos de información para identificar controles a implementar.

- Elaborar y actualizar el Plan de Seguridad de la Información.
- Realizar un monitoreo constante de incidentes relacionados con la seguridad de la información y establecer parámetros de mejora.

En la organización, el Oficial de Seguridad de la Información fue seleccionado mediante un riguroso proceso de evaluación que consideró su conocimiento y experiencia en la implementación de la norma ISO/IEC 27001:2022. El Jefe de Servicios de Soporte Técnico de la organización ocupará este cargo.

5.1.4 DUEÑO DEL RIESGO

Según la norma ISO/IEC 27001:2022, el Dueño del Riesgo es la persona responsable de gestionar los riesgos asociados a los activos de información valorizados. Su función es:

- Gestionar las actividades y recursos necesarios para mitigar las amenazas y vulnerabilidades en los activos de información.
- Asegurarse de que los controles aplicables se están implementando correctamente.
- Monitorear cambios significativos en los riesgos que afectan los activos de información identificados.

En la organización, el Gerente de Consultoría TI asumirá el rol de Dueño del Riesgo.

5.1.5 PROPIETARIOS DE ACTIVOS DE LA INFORMACIÓN

Son los responsables de:

- Clasificar los activos de información según su sensibilidad y criticidad.

- Documentar y mantener actualizada la clasificación de activos de información.
- Definir quiénes tienen acceso a los activos de información bajo su custodia.

En la organización, los Propietarios de Activos de Información serán los Gerentes que representen cada área que disponga de activos de información seleccionados.

Por ejemplo:

- El Gerente de Operaciones será el propietario de los contratos de mantenimiento y servicios de soporte de los clientes.
- Otros Gerentes serán propietarios de activos de información específicos de sus áreas.

5.1.6 CUSTODIO DE LOS ACTIVOS DE INFORMACIÓN

Actúan como intermediarios entre el propietario de la Información y el usuario de los activos de información, garantizando el uso adecuado y seguro de la información.

Son responsables de:

- Administrar y proteger los activos de información.
- Monitorear el cumplimiento de controles de seguridad en los activos bajo su administración.

En la organización, los Custodios de Activos de Información serán:

- El Jefe de Servicios de Soporte Técnico.
- Los Jefes de Proyectos.
- Los Líderes de Equipos Técnicos.

5.1.7 USUARIOS DE ACTIVOS DE INFORMACIÓN

Son las personas que utilizan los activos de información para realizar sus tareas y responsabilidades laborales.

En la organización, se considera usuario de activos de información a cualquier persona que:

- Tenga asignado un activo (bien, proceso, servicio, etc.) a través de un documento formal y explícito.
- Haya aceptado y acordado la responsabilidad de manejar dicho activo.

6. PREVENCIÓN DE RIESGOS Y APLICACIÓN DE CONTROLES

Los responsables de la información deben identificar, evaluar y mitigar los riesgos de seguridad de la información de manera efectiva y eficiente. Para ello, deben:

- Utilizar la metodología de gestión de riesgos establecida.
- Cumplir con todos los estatutos y procedimientos relacionados.
- Considerar los niveles de valoración de riesgos y los controles necesarios para prevenir la materialización de amenazas sobre los activos de información.

7. MANTENER LA SEGURIDAD DE LA INFORMACIÓN EN NIVELES ÓPTIMOS

Es fundamental evaluar constantemente el desempeño y la efectividad del SGSI para asegurarse de que:

- Se ajuste a los niveles de exigencia de la organización.
- Persiga los objetivos organizacionales establecidos.

Para lograr esto, la organización debe considerar el contenido del Anexo A de la norma ISO/IEC 27001:2022, también conocido como el Código de Buenas Prácticas o Norma ISO/IEC 27002:2022. Esto permitirá asegurar la mejora continua del SGSI.

8. INCUMPLIMIENTO

El incumplimiento de esta política tendrá consecuencias disciplinarias, que se aplicarán según la gravedad y características de la infracción.

Se consideran infracciones a esta política:

- Eventos que causen pérdidas o daños a los activos de la organización.
- Eventos que violen procedimientos y políticas de seguridad.

Los empleados que incumplan esta política estarán sujetos a medidas disciplinarias, que pueden incluir:

- Despido.
- Acciones disciplinarias que la organización considere convenientes.

9. APROBACIÓN

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