


	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO			
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 1 de 38	

MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Propósito del cambio:	Implementación del Sistema de Gestión de Seguridad de la Información.	Consecuencia del cambio:	Dar cumplimiento a los requisitos de la ISO 27001:2022.
Diseño del Modelo del Cumplimiento:	4.5, 4.6, 6.1, 8.1	Eficacia operacional del Modelo de Cumplimiento:	Los cambios mejoran los controles para prevenir incumplimientos en materia de Seguridad de la Información y leyes conexas.
Disponibilidad de recursos:	Económico: Ninguno	Humano: Horas hombre	Infraestructura: Equipos de cómputo, oficinas de sede central.
Responsable de hacer seguimiento al cambio:		Gerente Corporativo de Ética, Riesgos y Cumplimiento	

CONTROL DE EMISIÓN Y CAMBIOS					
Rev. N°	Fecha	Descripción	Elaborado por:	Revisado por:	Aprobado por:
0	21/11/2023	Elaboración del Procedimiento	Valeria Carbajal Analista de Riesgos de Seguridad de la Información	Cynthia Solar Jefe de Riesgos Fredy Guerra Rojas Gerente Corporativo de Ética, Riesgos y Cumplimiento	COMITÉ DE SOSTENIBILIDAD
Firmas de la revisión vigente				 	Aprobado en la Sesión Nro. 13-2023 del Comité de Sostenibilidad


	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 2 de 38

TABLA DE CONTENIDO

1. INTRODUCCIÓN.....	4
2. ALCANCE.....	4
3. REFERENCIAS NORMATIVAS.....	4
4. DEFINICIONES.....	5
5. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.....	8
5.1. CONTEXTO DE LA ORGANIZACIÓN.....	8
5.2. COMPRENSIÓN DE LAS NECESIDADES DE LAS PARTES INTERESADAS Y SUS EXPECTATIVAS.....	9
5.3. ALCANCE DEL SISTEMA.....	11
5.4. COMPROMISO DE LA ALTA DIRECCIÓN.....	11
5.5. ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN.....	11
5.5.1. Directorio.....	11
5.5.2. Comité de Sostenibilidad.....	12
5.5.3. Alta dirección.....	13
5.5.4. Oficial de Seguridad de la Información.....	14
5.5.5. Gerencia Corporativa de Ética, Riesgos y Cumplimiento.....	16
5.5.6. Propietarios de la Información.....	17
5.5.7. Responsables de los bancos de datos personales.....	18
5.5.8. Colaboradores.....	20
5.6. POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.....	20
5.7. OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.....	22
5.8. PLANIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.....	23
5.8.1. GESTIÓN DE ACTIVOS DE INFORMACIÓN.....	23
5.8.1.1 Tipos de activo de información.....	23
5.8.1.2 Clasificación de activos de información.....	23
5.8.1.3 Valoración de activos de información.....	23
5.8.2. PROTECCIÓN DE DATOS PERSONALES.....	24
5.8.2.1 Tratamiento de datos personales.....	24
5.8.2.1.1 Principios básicos para el tratamiento de datos personales.....	25
5.8.2.1.2 Ejercicio de derechos ARCO.....	26
5.8.2.2 Transferencia de datos personales.....	27
5.8.3. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.....	27
5.8.3.1 Planificación.....	29
5.8.3.2 Evaluación.....	29
5.8.3.3 Tratamiento.....	29
5.8.3.3.1 Controles.....	29
5.8.3.4 Aceptación.....	30
5.9. RECURSOS.....	30
5.10. COMPETENCIA.....	31
5.10.1. Proceso de contratación.....	31
5.10.2. Difusión y capacitación periódica.....	32
5.10.2.1 Toma de conciencia y formación.....	32
5.10.2.2 Comunicación.....	33
5.10.2.3 Información documentada.....	34
5.11. EVALUACIÓN DEL DESEMPEÑO.....	34
5.11.1. Evaluación y monitoreo continuo del Manual del Sistema de Gestión de Seguridad de la Información.....	34
5.11.2. Fuentes de opinión sobre el desempeño del Modelo de Cumplimiento.....	34
5.11.3. Informes de cumplimiento.....	35
5.11.4. Auditoria.....	35



GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO


Manual del Sistema de Gestión de Seguridad
de la Información

Código: MA-SGSI-01

Rev. 00

Página: 3 de 38

5.11.4.1 Ethical Hacking	36
5.11.5. Revisión por la dirección.....	36
5.12. MEJORA	36
5.12.1. No conformidades y acciones correctivas / Observaciones / Oportunidades de Mejora	36
5.12.2. Mejora Continua del Manual del Sistema de Gestión de Seguridad de la Información ..	37
5.12.2.1 Lecciones aprendidas por monitoreo, seguimiento o eventos de seguridad de la información	37
6. SANCIONES	38
7. CANALES DE DENUNCIA	38

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 4 de 38

1. INTRODUCCIÓN

El presente manual está conformado por los principios y lineamientos de la normativa aplicable en seguridad de la información, la misma que debe ser del conocimiento del personal como parte de sus responsabilidades de trabajo, con respecto al cumplimiento del Sistema de Gestión de Seguridad de la Información y debido a los requerimientos específicos que lo conforman.

COSAPI se compromete en cumplir con las buenas prácticas internacionales en materia de seguridad de la información, así como las leyes de la materia; preservando la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un adecuada Gestión de Riesgos.

Este documento es de obligatorio cumplimiento a todo el personal y/o tercero que nos represente con poder o sin poder ante competidores, socios comerciales, gremios, clientes, proveedores y colaboradores. Además, este documento debe seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, rotación del personal, desarrollo de nuevos productos o servicios, diversificación de productos o servicios, entre otros.

El Directorio de COSAPI S.A, COSAPI Minería y COSAPI Inmobiliaria. ha nombrado a un Oficial de Seguridad de la Información quien depende únicamente de este, el cual tiene como función supervisar la implementación y mantenimiento de este manual de manera corporativa, incluyendo todas las líneas de negocio del grupo económico.


2. ALCANCE

El presente manual es aplicable a todos los integrantes de COSAPI S.A, COSAPI Minería y COSAPI Inmobiliaria, sus subsidiarias y empresas vinculadas, en el ámbito nacional e internacional y en donde tenga sus operaciones (21100-OPV), en adelante COSAPI. Asimismo, alcanza a nuestros socios, proveedores y terceros que interactúen con el Sistema de Gestión de Seguridad de la Información.

Todos los colaboradores y directores de COSAPI deben cumplir con las disposiciones en materia de seguridad de la información contenidas en este Manual, así como las leyes aplicables y comportarse de manera íntegra y transparente, sin importar el puesto, nivel de responsabilidad y su ubicación geográfica. El solo hecho de trabajar para COSAPI lo obliga al conocimiento y cumplimiento de las disposiciones contenidas en este documento, por lo cual se adhiere a lo establecido en el presente Manual y asume el compromiso de capacitarse continuamente en su entendimiento, a efectos de su efectivo cumplimiento.

3. REFERENCIAS NORMATIVAS

- Norma ISO/IEC 27000:2018 – Sistemas de Gestión de Seguridad de la Información – Visión general y vocabulario.
- Norma ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información.
- Norma ISO/IEC 27002:2022 – Seguridad de la Información, ciberseguridad y protección de la privacidad — Controles de Seguridad de la Información.

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO			
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 5 de 38	

- Norma ISO/IEC 27005:2018 – Técnicas de Seguridad para la Gestión de Riesgos de Seguridad de la Información.
- Norma ISO/IEC 37301:2021 – Sistema de Gestión de Compliance.

Perú:


- Ley N° 29733 – Ley de Protección de Datos Personales y su Reglamento.
- Ley N° 30096 – Ley de Delitos Informáticos.
- NTP-ISO/IEC 27001 - Sistemas de Gestión de Seguridad de la Información.
- Decreto Supremo 003-2013-JUS – Reglamento de la Ley de Protección de Datos
- Decreto Legislativo N° 1353 – Decreto Legislativo que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses.
- Resolución Directoral N° 019-2013-JUS/DGPDP – Aprueba la Directiva de Seguridad de la Información, en adelante la Directiva.
- Decreto Supremo N° 019-2017-JUS – Aprueban el Reglamento del Decreto Legislativo N° 1353.
- Personales en Perú.
- Constitución Política del Perú de 1993.
- Código de Ética.
- Reglamento Interno de Trabajo.

Chile:

- Ley N° 19628 – Sobre protección de la vida privada.
- Constitución Política de la República de Chile de 1980.

4. DEFINICIONES

- **Activo de información:** Todo aquello que una organización valora y por lo tanto debe proteger.
- **Alta dirección:** Persona o grupo de personas que dirige y controla una organización al más alto nivel. Está representado por la Gerencia General de COSAPI y/o las Gerencias Generales de las empresas de COSAPI según corresponda.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede resultar en daño de un sistema u organización.
- **Banco de datos personales:** Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.
- **Confidencialidad:** Propiedad de que la información no se pone a disposición ni se revela a personas, entidades o procesos no autorizados.

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 6 de 38

- **Datos personales:** Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.
- **Datos sensibles:** Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.
- **Declaración de aplicabilidad:** Es un documento que permite establecer los controles que debemos implementar para mantener la información segura, disponible y confiable.
- **Derechos ARCO:** Acceso, Rectificación, Cancelación y Oposición. Son el conjunto de derechos que garantiza a las personas el poder de control sobre sus datos personales.
- **Disponibilidad:** Propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada.
- **Evento:** Ocurrencia de un evento o cambio de un conjunto particular de circunstancias.

Nota 1: Un evento puede ser una o más ocurrencias y puede tener varias causas.

Nota 2: Un evento puede consistir en algo que no sucede.


Nota 3: A veces se puede hacer referencia un evento como “incidente” o “accidente”.

- **Flujo transfronterizo de datos personales:** Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de su origen de datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.
- **Información confidencial:** Información a la cual solo tienen acceso personas determinadas que, por su importancia, es imprescindible para el funcionamiento de la empresa.
- **Información de uso interno:** Información que es de accesibilidad para todas las personas dentro de la organización.
- **Información pública:** Información que la organización pone a disposición para todas las personas, incluidos internos y externos, ya sea a través de su página web o medios de comunicación.
- **Integridad:** Propiedad de exactitud y completitud.
- **MC:** Modelo de Cumplimiento.
- **Objetivo:** Resultado a lograr.

Nota 1: Un objetivo puede ser estratégico, táctico u operativo.

Nota 2: Los objetivos pueden relacionarse con diferentes disciplinas (como metas financieras, de salud y seguridad y ambientales) y pueden aplicarse a diferentes niveles (como estratégico, de toda la organización, de proyecto, de producto y de proceso).

Nota 3: Un objetivo puede expresarse de otras formas, por ejemplo, como un resultado previsto, un propósito, un criterio operativo, como un objetivo de seguridad de la información o mediante el uso de otras palabras con un significado similar (por ejemplo, fin, meta o destino).

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 7 de 38

Nota 4: En el contexto de los Sistemas de Gestión de Seguridad de la Información, la organización establece los objetivos de seguridad de la información, de acuerdo con la Política de Seguridad de la Información, para lograr resultados específicos.

- **Oficial de Seguridad de la Información:** Es el rol asignado a la Gerencia de Ética, Riesgos y Cumplimiento de COSAPI.
- **Organización:** Persona o grupo de personas que tienen sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos.
- Nota 1: El concepto de organización incluye, pero no se limite a comerciante único, compañía, corporación, firma, empresa, autoridad, asociación, caridad o institución, o parte o combinación de las mismas, ya sea incorporada o no, pública o privada.
- **Órgano de gobierno:** Persona o grupo de personas que son responsables del desempeño y la conformidad de la organización. En COSAPI está representado por el Directorio.
- **Política:** Intenciones y dirección de una organización formalmente expresadas por la alta dirección.
- **Política de Seguridad de la Información:** Es la política de seguridad de la información desarrollada y aprobada por COSAPI.
- **Probabilidad:** Posibilidad de que algo suceda.
- **Propietarios de la Información:** Son los responsables de la información que se genera y utiliza en las operaciones de su gerencia.
- **Representante/s de COSAPI:** Cualquier colaborador, oficial o director de una Empresa COSAPI.
- **Riesgo:** Efecto de la incertidumbre sobre los objetivos.

Nota 1: Un efecto es una desviación de lo esperado, ya sea positivo o negativo.

Nota 2: La incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con, comprensión o conocimiento de un evento, su consecuencia o probabilidad.

Nota 3: El riesgo a menudo se caracteriza por referencia a posibles “eventos” y “consecuencias” o una combinación de estos.


Nota 4: El riesgo a menudo se expresa en términos de una combinación de las consecuencias de un evento (incluidos los cambios en las circunstancias) y la “probabilidad” asociada de ocurrencia.

Nota 5: En el contexto de los Sistemas de Gestión de Seguridad de la Información, los riesgos de seguridad de la información pueden expresarse como efecto de la incertidumbre sobre los objetivos de seguridad de la información.

Nota 6: El riesgo de seguridad de la información está asociado con la posibilidad de que las amenazas exploten las vulnerabilidades de un activo de información y, por lo tanto, causen daño a la organización.

- **Seguridad de la Información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Nota 1: Además, otras propiedades como la autenticidad, la responsabilidad, el no repudio, y confiabilidad también pueden estar involucrados.

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 8 de 38

- **Sistema de Gestión:** Conjunto de elementos interrelacionados o que interactúan de una organización para establecer políticas, objetivos y procesos para lograr esos objetivos.

Nota 1: Un sistema de gestión puede abordar una sola disciplina o varias disciplinas.

Nota 2: Los elementos del sistema incluyen la estructura, roles y responsabilidades, planificación y operación de la organización.


Nota 3: El alcance de un sistema puede incluir la totalidad de la organización, funciones específicas e identificadas de la organización, secciones específicas e identificadas de la organización, o una o más funciones en un grupo de organizaciones.

- **Sistema de Gestión de Seguridad de la Información:** Es el Sistema de Gestión de Seguridad de la Información desarrollado por COSAPI, dirigido a asegurar el cumplimiento de las normas de seguridad de la información.
- **Sistema de Gestión Integral de Riesgos:** Es el Sistema de Gestión Integral de Riesgos desarrollado por COSAPI, el cual ha adoptado las metodologías internacionales del Marco de Gestión de Riesgo Empresarial (COSO ERM 2017) e ISO 31000:2018 – Gestión de Riesgos.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Transferencia de datos personales:** Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.
- **Tratamiento de datos personales:** Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.
- **Titular de datos personales.** Persona natural a quien corresponde los datos personales.
- **Titular del banco de datos personales:** Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.

5. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

5.1. CONTEXTO DE LA ORGANIZACIÓN

La alta dirección de COSAPI determina e informa al Comité de Sostenibilidad las cuestiones internas y externas de conformidad con el requisito 4.1 de la **Norma ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información** y los parámetros señalados en la **Ley N° 29733 – Ley de Protección de Datos Personales**, las cuales son registradas en la **Matriz FODA (MA-SGSI-01-F1)** que son pertinentes para el propósito y dirección estratégica de la organización y que afectan a su capacidad para lograr los resultados previstos del Sistema de Gestión

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 9 de 38

de Seguridad de la Información. Para la elaboración de la Matriz FODA la organización toma en cuenta lo siguiente:

- El modelo de negocio, que incluye la estrategia, la naturaleza, el tamaño, y el nivel de complejidad y sostenibilidad de las actividades y operaciones de la empresa;
- Grado de influencia o poder que la empresa ostenta en el mercado que participa;
- Características y particularidades de la empresa;
- Características del mercado en el que participa;
- La naturaleza y el alcance de las relaciones comerciales con competidores, gremios, socios comerciales, clientes, proveedores y colaboradores;
- El contexto legal y regulatorio;
- La situación económica;
- Los contextos sociales, culturales y ambientales;
- Las estructuras, políticas, procesos, procedimientos y recursos internos, incluyendo la tecnología, y;
- La cultura de seguridad de la información.

El contexto de la organización se revisa con carácter mínimo anual o cuando se de alguna de las siguientes circunstancias:


- Actividades, productos o servicios nuevos o modificados de forma relevante.
- Cambios en la estructura o en la estrategia de la organización.
- Cambios externos significativos, tales como circunstancias económico-financieras, condiciones de mercado, pasivos y relaciones con los clientes.
- Cambios en las obligaciones legales de cumplimiento (modificadoras de legislación vigente).
- Incumplimiento(s) al Sistema de Gestión de Seguridad de la Información.

5.2. COMPRENSIÓN DE LAS NECESIDADES DE LAS PARTES INTERESADAS Y SUS EXPECTATIVAS

La alta dirección de COSAPI conforme a lo señalado en el requisito 4.2 de la **Norma ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información** determina e informa anualmente al Comité de Sostenibilidad lo siguiente:

- a) Las partes interesadas que son pertinentes al Sistema de Gestión de Seguridad de la Información,
- b) Los requisitos pertinentes de estas partes interesadas para el Sistema de Gestión de Seguridad de la Información, y,
- c) Cuáles de estos requisitos se abordarán en el sistema de seguridad de la información.

Para el seguimiento y revisión de las necesidades y expectativas de las partes interesadas pertinente al Sistema de Gestión de Seguridad de la Información, se empleará el **Registro de Necesidades y Expectativas de las Partes Interesadas (PG-SG-01-F7)** del Modelo de Cumplimiento.

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO			
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 10 de 38	


Asimismo, COSAPI realiza un análisis y evaluación de relevancia de sus grupos de interés en el **Registro de Necesidades y Expectativas de las Partes Interesadas (PG-SG-01-F7)**. Para ello, realiza el siguiente análisis: “*(Poder / Influencia sobre COSAPI) x (Interés de la parte interesada para COSAPI) = Relevancia de la Parte Interesada*”.

Para realizar dicho análisis se consideran los siguientes factores Bajo (1), Medio (2) y Alto (3).

MAPA DE CALOR					
NIVEL DEL RIESGO			Poder / Influencia sobre COSAPI		
			Menor	Medio	Grave
			1	2	3
Interés de la parte interesada para COSAPI	Bajo	1	1	2	3
	Medio	2	2	4	6
	Alto	3	3	6	9

SIGNIFICANCIA		
1 al 2	Bajo	Importancia insignificante. No se requiere ninguna acción.
3 al 4	Medio	Importancia significativa. Necesita evaluar acciones para mantener la relación con la parte interesada.
6 al 9	Alto	Importancia relevante. Es necesario realizar acciones para mantener la relación con la parte interesada.

Asimismo, COSAPI realiza una encuesta 01 vez año para recibir la percepción de sus partes interesadas con relación a su Sistema de Gestión de Seguridad de la Información.

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 11 de 38

5.3. ALCANCE DEL SISTEMA

El alcance del Sistema de Gestión de Seguridad de la Información es el siguiente:

“El Sistema de Gestión de Seguridad de la Información es aplicable teniendo en cuenta nuestro contexto, los requisitos y expectativas de nuestras partes interesadas, nuestras obligaciones en materia de seguridad de la información y protección de datos personales, y los principales riesgos de manera corporativa; a todos los procesos de COSAPI S.A., COSAPI Minería y COSAPI Inmobiliaria en sus sedes a nivel nacional e internacional.”

El Sistema de Gestión de Seguridad de la Información de COSAPI, se basa en el marco legal que resulta aplicable a COSAPI que se detalla en **Matriz Normativas Legales (MTZ-AL-01)** y, además, las referencias normativas que se han señalado en el punto 3 (Referencias Normativas) del presente documento. Para determinar el alcance del Sistema, se ha analizado lo siguiente:

1. Las debilidades, fortalezas, amenazas y oportunidades identificadas en el formato **Matriz FODA (MA-SGSI-01-F1)**.
2. Las partes interesadas identificadas en el formato **Registro de Necesidades y Expectativas de las Partes Interesadas (PG-SG-01-F7)**.
3. Los riesgos de seguridad de la información identificados en el formato de **Matriz de Riesgos (MA-SGSI-01-F2)**.


5.4. COMPROMISO DE LA ALTA DIRECCIÓN

El compromiso de la alta dirección es reflejar, lograr y mantener una cultura de cumplimiento a la seguridad de la información y de los Datos Personales, exigiendo el cumplimiento de la **Norma ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información** y de la **Ley N° 29733 – Ley de Protección de Datos Personales** y su Reglamento; normas modificatorias y/o ampliatorias; así como de la legislación en materia de protección de datos personales de los países en donde operamos.

5.5. ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN

5.5.1. Directorio

Es el órgano de gobierno del Sistema de Gestión de Seguridad de la Información y del Sistema de Cumplimiento de Protección de Datos Personales, el cual a través del Comité de Sostenibilidad tiene la función de determinar, aprobar y fomentar razonablemente el Manual del Sistema de Gestión de Seguridad de la Información y los objetivos de este, así como de su publicación y distribución donde corresponda.


	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO			
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 12 de 38	

- Vigilar permanentemente el cumplimiento de la legislación en protección de datos personales y el Sistema de Gestión de Seguridad de la Información.
- Revisar periódicamente los informes sobre el desarrollo y cumplimiento del Sistema de Gestión de Seguridad de la Información de la corporación que emita el Oficial de Seguridad de la Información.
- Promover y fomentar la cultura de seguridad de la información a toda la organización.
- Garantizar la autonomía, independencia y recursos del Oficial de Seguridad de la Información.
- Asignar los recursos técnicos, humanos y financieros necesarios para la implementación y adecuado funcionamiento del Sistema, mediante la aprobación del presupuesto anual de los proyectos relacionados con la seguridad de la información.
- Aprobar la organización, roles y responsabilidades para el SGSI incluyendo los lineamientos de difusión y capacitación que contribuyan a un mejor conocimiento de los riesgos involucrados.
- Demostrar liderazgo y compromiso respecto al Sistema de Gestión de Seguridad de la Información.

5.5.2. Comité de Sostenibilidad

Es el órgano de seguimiento y supervisión delegado por el Directorio para el Sistema de Gestión de Seguridad de la Información, y tiene las siguientes funciones:

- Garantizar que el Sistema de Gestión de Seguridad de la Información sea implementado y mantenido de acuerdo con la Política de Seguridad de la Información.
- Monitorear los avances del desarrollo del Sistema de Gestión de Seguridad de la Información, así como los inconvenientes que pudieran presentarse.
- Promover y gestionar la implementación de estándares y buenas prácticas de seguridad de la información en la organización.
- Asegurar que las responsabilidades y la autoridad para los roles relevantes a la seguridad de la información estén asignadas y comunicadas.
- Aprobar el manual, políticas y lineamientos para la implementación y mejora continua del Sistema de Gestión de Seguridad de la Información.
- Velar por el cumplimiento de las políticas, lineamientos y procedimientos de seguridad de la información.
- Validar de manera periódica la implementación y monitoreo de los controles de seguridad de la información.
- Asegurar que los objetivos de seguridad de la información cumplan con los requerimientos organizacionales y estén integrados en los procesos relevantes de la organización.
- Revisar los procesos de auditoría interna y externa de manera periódica.
- Aprobar las medidas a adoptar por el incumplimiento e infracciones a las políticas, procedimientos y normas de seguridad de la información.


	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 13 de 38

- Aprobar políticas y lineamientos para la implementación de la Gestión de Riesgos en el Sistema de Gestión de Seguridad de la Información.
- Aprobar los riesgos y oportunidades que deben abordarse en el Sistema de Gestión de Seguridad de la Información.
- Decidir el criterio para la aceptación de riesgos de seguridad de la información.
- Asegurar la ejecución de las acciones que permitan abordar los riesgos y oportunidades identificadas, además de prevenir o reducir los efectos no deseados.
- Aprobar y revisar de manera periódica la implementación y monitoreo de los controles de seguridad de la información.
- Validar que las evaluaciones de riesgos de seguridad de la información produzcan resultados consistentes, válidos y comparables.
- Velar por el cumplimiento de las políticas, lineamientos y procedimientos relacionados a la Gestión de Riesgos dentro del Sistema de Gestión de Seguridad de la Información.
- Asegurar que se establezcan criterios de riesgos de seguridad de la información.
- Garantizar que las opciones apropiadas para el tratamiento de los riesgos de seguridad de la información sean las adecuadas.
- Aprobar los niveles aceptables para los riesgos identificados en el Sistema de Seguridad de la Información.
- Avalar el documento de Declaración de Aplicabilidad.
- Evaluar el desempeño y eficacia de los controles implementados en la Declaración de Aplicabilidad.
- Monitorear y evaluar el proceso de Gestión Integral de Riesgos del Sistema de Gestión de Seguridad de la Información.
- Garantizar la validez de los resultados de la Gestión de Riesgos del Sistema de Gestión de Seguridad de la Información.

5.5.3. Alta dirección

La alta dirección, se encuentra representada en cada caso por el Gerente General de COSAPI, con respecto a la gestión de la seguridad de la información y de los bancos de datos personales, tiene las siguientes funciones y responsabilidades:

- Demostrar liderazgo y compromiso respecto al Sistema de Gestión de Seguridad de la Información.
- Asegurar que la Política de Seguridad de la Información y los objetivos sean establecidos y compatibles con la dirección estratégica de la organización.
- Asegurar la integración de los requisitos del Sistema de Gestión de Seguridad de la Información en los procesos de la organización.
- Asegurar que estén disponibles los recursos necesarios para el funcionamiento del Sistema de Gestión de Seguridad de la Información.
- Difundir la importancia de una efectiva Gestión de Seguridad de la Información en conformidad con los requisitos del Sistema de Gestión de Seguridad de la Información.
- Asegurar que el Sistema de Gestión de Seguridad de la Información logre sus resultados previstos.

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 14 de 38


- Promover la mejora continua del Sistema de Gestión de Seguridad de la Información.
- Dirigir y apoyar a las personas y a los otros roles relevantes para que contribuyan con la efectividad del Sistema de Gestión de Seguridad de la Información.
- Revisar el Sistema de Gestión de Seguridad de la información anualmente o cada que se produzca un cambio significativo para asegurar la conveniencia, adecuación y efectividad continua.
- Difundir de manera periódica y expresa el compromiso de todos los colaboradores de cumplir con los lineamientos de la **Norma ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información** y la **Ley N° 29733 - Ley de Protección de Datos Personales**, así como de las normas que la modifique y/o amplie.
- Revisar el cumplimiento del Sistema de Gestión de Seguridad de la Información de la corporación de manera anual, así como solicitar un informe anual a los gerentes de las distintas áreas respecto al cumplimiento de las medidas adoptadas para el funcionamiento de este, con el objetivo de informar al Comité de Sostenibilidad.
- Monitorear la modificación del Reglamento Interno de Trabajo con el fin de incluir sanciones a los colaboradores en caso de incumplimiento a la normativa de datos personales y al Sistema de Gestión de Seguridad de la Información.
- Participar en las capacitaciones al personal vinculadas al Sistema de Gestión de Seguridad de la Información.
- Difundir a los proveedores y clientes sobre la existencia del Oficial de Seguridad de la Información, así como de los canales de denuncia en donde ellos pueden dirigirse de manera confidencial para informarle sobre cualquier indicio de un riesgo de posible violación a la normativa de datos personales.
- Revisar periódicamente la **Política de Seguridad de la Información (PLT-SGSI-01)**.
- Velar por el cumplimiento de las políticas, lineamientos y procedimientos de seguridad de la información.
- Proponer planes y programas para mantener la conciencia del cumplimiento normativo en materia de seguridad de la información en los procesos relevantes de la organización.
- Comunicar a la organización la importancia de los requisitos vigentes y aplicables a seguridad de la información, en las diferentes reuniones.
- Asegurar de manera periódica la implementación y monitoreo de los controles de seguridad de la información.

5.5.4. Oficial de Seguridad de la Información

Está a cargo del Gerente Corporativo de Ética, Riesgos y Cumplimiento. Teniendo a cargo las siguientes funciones y responsabilidades:

- Asegurar que el Sistema de Gestión de Seguridad de la Información esté conforme a los requisitos de la **Norma ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información**.

- Participar en la creación y revisión de las políticas, lineamientos, procedimientos y planes referidos al Sistema de Gestión de Seguridad de la Información.
- Liderar la presentación de los documentos y/o actualizaciones de los mismos para presentarlos al Comité de Sostenibilidad.
- Liderar, velar, evaluar, coordinar y monitorear el cumplimiento de las políticas, procedimientos y lineamientos de seguridad de la información.
- Evaluar los informes acerca de la efectividad y eficiencia de los controles implementados.
- Participar y coordinar con los propietarios y custodios de la información para la elaboración del inventario y clasificación de activos de información, y ejecución de la Gestión de Riesgos de Seguridad de la Información.
- Liderar la realización de actividades orientadas al análisis y evaluación de riesgos de seguridad de la información, a fin de mantener un conocimiento actualizado de las amenazas y vulnerabilidades de estos.
- En base a los riesgos encontrados para los activos de información, liderar el análisis para presentar al Comité de Sostenibilidad las opciones de tratamiento necesarias para mantener el riesgo en un nivel aceptable para la organización.
- Atender las peticiones de los ciudadanos (todos los colaboradores internos: empleados, obreros y practicantes; postulantes, proveedores, clientes, prospecto comercial, personal de empresas subcontratadas, accionistas, denunciantes), sobre las consultas relacionadas con seguridad de la información.
- Dirigir, coordinar y controlar todas las actividades relacionadas al Sistema de Gestión de Seguridad de la Información.
- Promover y hacer seguimiento de la mejora continua del Sistema de Gestión de Seguridad de la Información.
- Identificar las obligaciones a las que está sujeta la organización en materia de seguridad de la información.
- Realizar y mantener actualizado el mapeo de los riesgos de seguridad de la información.
- Adoptar las medidas que considere necesarias para contrarrestar los riesgos en materia de seguridad de la información que se identifiquen en la organización.
- Encargarse de la supervisión e implementación del Sistema de Gestión de Seguridad de la Información.
- Informar periódicamente a la alta dirección y al Comité de Sostenibilidad sobre los avances del desarrollo del Sistema de Gestión de Seguridad de la Información, así como los inconvenientes o eventos que pudieran presentarse.
- Encargarse mediante los mecanismos internos de la empresa de promover, difundir, capacitar, asesorar y orientar a todo el personal y relacionados acerca del cumplimiento normativo en seguridad de la información, mínimo (1) una vez al año.
- Realizar las evaluaciones, mejoras y monitoreos periódicos pertinentes del Sistema de Seguridad de la Información, mínimo (1) una vez al año.
- Administrar el canal de denuncias considerando la categoría de seguridad de la información.


	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO			
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 16 de 38	

- Asegurar que el Sistema de Gestión de Seguridad de la Información es conforme con los requisitos del Decreto Supremo N° 003-2013-JUS, Decreto que aprueba el Reglamento de la **Ley N° 29733 – Ley de Protección de Datos Personales**, y la **Norma ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información**.
- Solicitar a cualquier colaborador una copia en medios electrónicos o físicos de todo tipo de documentos, incluyendo, de ser el caso, los programas y equipos necesarios para su lectura, cuando considere que podría existir una vulneración o amenaza en la información de la organización.
- Resolver y atender dudas que pudieran presentarse sobre cómo proceder o si cierta conducta constituye o no a una infracción al Sistema de Seguridad de la Información.
- Resguardar la confidencialidad de toda la información a la que haya tenido acceso en el ejercicio de sus funciones. El incumplimiento de la obligación de reserva generará en el Oficial de Seguridad de la Información las responsabilidades civiles, administrativas y penales previstas en la ley.
- Dar seguimiento y reportar de manera inmediata al Directorio en caso de ocurrencia de eventos, presuntos incumplimientos, incumplimientos probados o frente a la identificación de nuevos riesgos que debe afrontar la organización.
- Supervisar la ejecución de las actividades que se deriven de los informes de las auditorías en relación con la seguridad de la información.
- Proveer el primer nivel de conocimientos respecto a los temas de seguridad de la información a todos los nuevos colaboradores.
- Aprobar planes y programas de concientización y capacitación en materia de seguridad de la información.
- Asesorar a las distintas áreas de la organización en temas relacionados a seguridad de la información.
- Liderar en la planificación y realización de las auditorías en el marco de seguridad de la información.

5.5.5. Gerencia Corporativa de Ética, Riesgos y Cumplimiento

La Gerencia Corporativa de Ética, Riesgos y Cumplimiento tiene las siguientes funciones y responsabilidades:

- Elaborar, gestionar y actualizar, en caso se requiera, la documentación relacionada al Sistema de Gestión Seguridad de la Información.
- Participar y gestionar en los procesos de identificación y clasificación de activos de información.
- Monitorear la efectividad y eficiencia de los controles implementados.
- Participar y gestionar en la ejecución de la Gestión de Riesgos de Seguridad de la Información.
- Tomar conocimiento de los eventos de seguridad que se presenten, con el fin de evaluar la efectividad de los controles implementados.
- Informar al Oficial de Seguridad de la Información ante cualquier evento o exposición a la seguridad que represente un riesgo para la seguridad de la información de la organización.


	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO			
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 17 de 38	

- Ejecutar la realización de actividades orientadas al análisis y evaluación de riesgos de seguridad de la información periódicos sobre los activos de información, a fin de mantener un conocimiento actualizado de las amenazas y vulnerabilidades sobre éstos.
- En base a los riesgos encontrados para los activos de información, proponer opciones de tratamiento necesarias para mantener el riesgo en un nivel aceptable para la organización.
- Promover la difusión y apoyo a la seguridad de la información dentro de la organización.
- Proponer planes y programas de concientización en materia de seguridad de la información y, capacitar en forma constante y continua a los colaboradores.
- Apoyar a las distintas áreas de la organización en temas relacionados a seguridad de la información.
- Apoyar en la revisión gerencial que se realice para el Sistema de Gestión de Seguridad de la Información.
- Realizar el seguimiento de la mejora continua del Sistema de Gestión de Seguridad de la Información.
- Realizar el seguimiento de las acciones correctivas.
- Apoyar en la planificación y realización de las auditorías en materia de seguridad de la información.
- Elaborar los informes de gestión del Sistema de Gestión de Seguridad de la Información, para su revisión por el Oficial de Seguridad de la Información.
- Monitorear cambios significativos en la infraestructura que puedan poner en riesgo los activos de información de la organización.
- Velar por el cumplimiento de los registros de los bancos de datos personales.
- Seguimiento a la información registrada en los bancos de datos personales, así como su almacenamiento, preservación y métodos de destrucción.
- Coordinar con las áreas respectivas acciones para actualizar la información personal de los colaboradores, así como el cambio de funciones o información laboral por rotaciones o cese.

5.5.6. Propietarios de la Información

Los propietarios de la información tienen las siguientes funciones y responsabilidades:

- Participar en los procesos de identificación y clasificación de activos de información.
- Documentar, mantener la clasificación y actualizar la etiqueta a los activos de información identificados.
- Establecer la prioridad de la información y los niveles de servicio.
- Determinar cuando la información ya no sea necesaria, así como ejecutar los procedimientos y métodos de destrucción.
- Participar en la ejecución de la Gestión de Riesgos de Seguridad de la Información.
- Participar en la ejecución de la Gestión de Accesos, definiendo los usuarios y tipos de permisos que deben tener para la visualización o tratamiento de información de acuerdo con sus funciones y competencias.


	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO			
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 18 de 38	

- Revisar periódicamente los niveles de acceso definidos para los usuarios.
- Notificar el cambio de función/ubicación de cualquier colaborador ya sea por reasignación o retiro, con la finalidad de modificar o cancelar sus accesos.
- Sugerir y apoyar en la elaboración de lineamientos y procedimientos relacionados a la seguridad de la información dentro de sus respectivas áreas y procesos.
- Apoyar en la verificación de la aplicación de los controles de seguridad.
- Suscribir y mantener Acuerdos de Confidencialidad con todos los colaboradores, empresas o personal de servicios externos que requieran o puedan tener acceso a la información de la organización.
- Reportar inmediatamente el incumplimiento o infracciones a la políticas, lineamientos o procedimientos del Sistema de Gestión de Seguridad de la Información.
- Apoyar y facilitar las revisiones periódicas para la verificación del cumplimiento de las políticas y procedimientos de seguridad de la información.
- Identificar los riesgos asociados a la seguridad de la información inherente a su gestión, así como solicitar el apoyo a las áreas pertinentes para evaluar dichos riesgos y establecer medidas de mitigación.
- Comunicar requerimientos de control y protección de la información al Oficial de Seguridad de la Información y asegurar que la información y recursos bajo su control estén debidamente protegidos por las medidas de seguridad adecuadas.
- Apoyar en la difusión de las políticas, lineamientos y procedimientos de seguridad de la información a los colaboradores y personal externo, para asegurarse de su conocimiento, comprensión y consecuencias que el incumplimiento pudiera generar, tales como una acción disciplinaria.
- Velar por la integridad, confidencialidad y disponibilidad de la información.
- Adoptar medidas de índole organizativa, legal y técnica, necesarias que garanticen la seguridad de la información y eviten su alteración, pérdida, tratamiento o acceso no autorizado, teniendo en cuenta el estado de la tecnología, la naturaleza de la información almacenada y los riesgos a los que están expuestos ya sea que provengan de la acción humana o del medio físico o natural.

5.5.7. Responsables de los bancos de datos personales


Los responsables de los bancos de datos personales son:

- Jefe de Atracción y Desarrollo del Talento
- Jefe de Administración del Talento
- Coordinador Salud Ocupacional
- Gerente de Procura
- Jefe de Imagen y Comunicaciones
- Jefe de Administración de Proyectos
- Gerente de Asesoría Legal
- Gerente de Ética, Riesgos y Cumplimiento
- Gerente de Inmobiliaria

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO			
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 19 de 38	

Los responsables tienen las siguientes funciones y responsabilidades:

- Decidir sobre la finalidad, contenido y uso del tratamiento del banco de datos.
- Declarar y actualizar los bancos de datos personales ante el Ministerio de Justicia.
- Adoptar medidas de índole organizativa, legal y técnica, necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, teniendo en cuenta el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a los que estén expuestos ya sea que provengan de la acción humana o del medio físico o natural.
- Velar por la integridad, confidencialidad y disponibilidad de la información.
- Apoyar en la difusión de las políticas y procedimiento de seguridad de la información a los trabajadores y colaboradores externos, para asegurarse que las conozcan y comprendan que el incumplimiento de las mismas podría resultar en una acción disciplinaria.
- Comunicar requerimientos de control y protección de la información al Oficial de Seguridad de la Información y asegurar que la información y recursos bajo su control estén debidamente protegidos por las medidas de seguridad adecuadas.
- Identificar los riesgos asociados a la seguridad de la información inherente a su gestión, así como solicitar el apoyo de las áreas pertinentes para evaluar dichos riesgos y establecer medidas de mitigación.
- Apoyar y facilitar las revisiones periódicas para la verificación del cumplimiento de las políticas y procedimientos de seguridad de la información.
- Determinar los criterios y niveles de acceso a la información de la cual son responsables y notificar el cambio de función/ubicación de cualquier trabajador sea por reasignación o retiro, con la finalidad de modificar o cancelar sus accesos.
- Autorizar y revisar periódicamente la asignación de accesos sobre la información.
- Determinar cuando la información ya no es necesaria, los tiempos y métodos de destrucción.
- Establecer la prioridad de la información y los niveles mínimos de servicio cuando requiere recuperar información en casos de desastres.
- Reportar inmediatamente el incumplimiento o infracciones a las políticas y normas de seguridad.
- Velar porque en la contratación de servicios tercerizados y/o la contratación de personal se contemplen cláusulas que obliguen al proveedor / trabajador a que sus servicios no afecten la confidencialidad, integridad y disponibilidad de la información.
- Revisar y autorizar la transferencia de datos personales hacia terceros.
- Mantener actualizado el inventario de activos de la información que se encuentran bajo su responsabilidad.
- Mantener acuerdos de confidencialidad con todos los colaboradores externos que requieran o puedan tener acceso a la información de carácter personal.

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 20 de 38

5.5.8. Colaboradores


Todos los colaboradores tienen las siguientes funciones y responsabilidades:

- Velar por la integridad, confidencialidad y disponibilidad de los datos personales y de la información de la organización.
- Participar en las capacitaciones sobre el Sistema de Gestión de Seguridad de la Información.
- Conocer, comprender y cumplir las políticas, lineamientos y procedimientos del Sistema de Gestión de Seguridad de la Información.
- Notificar eventos y riesgos relacionados a la información personal e información de la organización.
- Proteger la información que utiliza en su trabajo diario.
- Utilizar la información, sistemas y todos los recursos de la organización únicamente para los propósitos autorizados e inherentes a la función asignada.
- Mantener la confidencialidad e integridad de la información que ha sido compartida o a la que ha tenido acceso para realizar sus funciones asignadas.
- Mantener la confidencialidad e integridad de la información que circula al interior de la organización.
- Mantener la confidencialidad de sus datos de acceso de los distintos Sistemas de Información de la organización.
- Almacenar la información en los repositorios de archivos autorizados por la organización, asegurando que solo las personas autorizadas puedan acceder a ella.
- Reportar incumplimientos que puedan afectar al Sistema de Gestión de Seguridad de la Información.

5.6. POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

COSAPI se compromete con el cumplimiento de los 3 principios que rigen su Sistema de Gestión de Seguridad de la Información.



	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO			
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 21 de 38	

Dichos principios forman parte de la Política de Seguridad de la Información. Este documento plasma la declaración de COSAPI a sus partes interesadas de su compromiso con la protección de la información de la organización, cumplimiento de la legislación y las buenas prácticas en materia de seguridad de la información.

"En COSAPI sabemos que la fuente de poder más importante es la información que maneja cada uno de nuestros colaboradores. Por ello, nos comprometemos a garantizar que la información precisa esté disponible en el momento adecuado para las personas autorizadas."


Por ello, todos los principios que conforman este Sistema son de obligatorio cumplimiento para todos los colaboradores, directores, accionistas, y demás personas naturales y jurídicas que actúen de forma autorizada en nombre o por cuenta de COSAPI.

COSAPI tiene una **TOLERANCIA CERO** a la comisión de prácticas no seguras, abuso de poder, así como toda acción que vulnere la seguridad de la información de la organización; pudiendo sancionar con acciones como la desvinculación, cese de la relación comercial e inicio de acciones legales en caso corresponda.

Asimismo, la Política de Seguridad de la Información declara la independencia, recursos, autoridad, competencias, y facultad de reporte a los directores con los que cuenta el Oficial de Seguridad de la Información.

El órgano de gobierno y la alta dirección de COSAPI establecen, implementan y mantienen una política para el Sistema de Seguridad de la Información que:

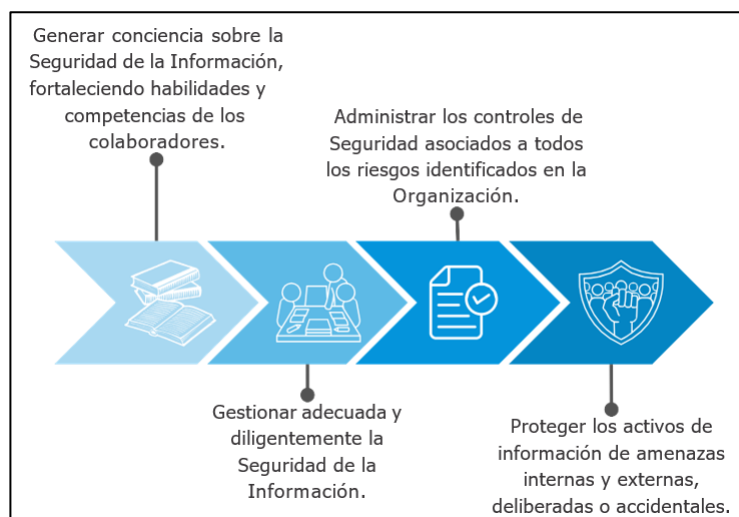
- Requiera y fomente la cultura de cumplimiento de la **Ley N° 29733 – Ley de Protección de Datos Personales** y normas modificatorias y/o ampliatorias.
- Está alineada con los valores, objetivos y estrategia de la organización.
- Asegure que la Gerencia de Ética, Riesgos y Cumplimiento cuenta con los recursos y la independencia para supervisar la implementación y mantenimiento de esta política de manera corporativa.
- Sancione disciplinariamente el incumplimiento del Sistema de Gestión de Seguridad de la Información, sus políticas y procedimientos, de acuerdo con lo establecido en el Código de Ética y Reglamento Interno de Trabajo, aquellas conductas que conlleven al incumplimiento de esta política.
- Genere un entorno de transparencia manteniendo un canal de denuncias confiable que permite a los colaboradores y socios de negocio comunicar el incumplimiento de esta política y a la normativa en materia de seguridad de la información aplicable a COSAPI.
- Proporcione un marco de referencia para el establecimiento, revisión y logro de los objetivos.
- Incluya el compromiso de cumplir los requisitos del Sistema de Gestión de Seguridad de la Información.
- Proporcione orientación, en un lenguaje fácilmente comprensible, para que todo el personal pueda entender los principios y su intención.

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 22 de 38

- No restrinja el derecho de denunciar bajo condicional de obligaciones contractuales, como acuerdos de no divulgación o cláusulas como la confidencialidad comercial y confidencialidad del empleado, entre otros.
- Incluya el compromiso de mejora continua del Sistema de Gestión de Seguridad de la Información.

5.7. OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN


El Comité de Sostenibilidad determina y aprueba los objetivos del Sistema de Gestión de Seguridad de la Información en el documento **Política de Seguridad de la Información (PLT-SGSI-01)** de acuerdo con las funciones y niveles pertinentes. Estos objetivos son medibles y alcanzables; y serán comunicados y actualizados, según corresponda.



Además, estos objetivos serán replicados en las siguientes acciones:

- Proteger la información de la organización
- Mitigar los riesgos de seguridad a niveles aceptables
- Gestionar de manera eficaz los eventos de seguridad de la información
- Fomentar la cultura de seguridad de la información
- Crear una mejor imagen en el mercado
- Reducir el impacto ocasionado por potenciales eventos no deseados de seguridad de la información

Para el logro y el seguimiento de los objetivos del Sistema de Gestión de Seguridad de la Información, se empleará el **Procedimiento de Seguimiento a los Objetivos del Modelo de Cumplimiento (PG-MC-01)**, el cual, incluye dicho sistema.

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 23 de 38

5.8. PLANIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Para la planificación del Sistema de Gestión de Seguridad de la Información, se ha considerado el contexto, alcance, compromiso de la alta dirección y las expectativas de las partes interesadas de nuestra organización.

5.8.1. GESTIÓN DE ACTIVOS DE INFORMACIÓN

COSAPI con el objetivo de mantener una adecuada Gestión de Activos de Información, identifica 6 etapas dentro de su proceso: Identificación, Clasificación, Revisión, Modificación y actualización, Aprobación y Etiquetado. Asimismo, se ha desarrollado el **Procedimiento de Gestión de Activos de Información (PG-SGSI-01)** para detallar de manera más específica sobre los pasos a seguir.

5.8.1.1 Tipos de activo de información

COSAPI tipifica sus activos de información en tipos, los cuales son:

- Información
- Equipos tecnológicos
- Hardware
- Software
- Componentes de red
- Personal (colaboradores y directores)
- Ubicación física
- Otros

5.8.1.2 Clasificación de activos de información


COSAPI clasifica sus activos de información de tres maneras en función de la sensibilidad:

- Confidencial
- Uso interno
- Pública

5.8.1.3 Valoración de activos de información

COSAPI en función a los criterios para definir la confidencialidad, integridad y disponibilidad, brinda una valorización al activo, teniendo en cuenta lo siguiente:

Valor	Clasificación	Definición
1	Muy baja	Cuando la falla o pérdida de confidencialidad, disponibilidad e integridad del activo puede generar un impacto no significativo para COSAPI.
2	Baja	Cuando la falla o pérdida de confidencialidad, disponibilidad e integridad del activo puede generar un impacto bajo para COSAPI.

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 24 de 38

3	Media	Cuando la falla o pérdida de confidencialidad, disponibilidad e integridad del activo puede generar un impacto medio o parcial para COSAPI.
4	Alta	Cuando la falla o pérdida de confidencialidad, disponibilidad e integridad del activo puede generar un impacto grave para COSAPI.
5	Muy alta	Cuando la falla o pérdida de confidencialidad, disponibilidad e integridad del activo puede generar un impacto irreversible para COSAPI.

5.8.2. PROTECCIÓN DE DATOS PERSONALES

El Sistema de Gestión de Seguridad de la Información cuenta con requerimientos específicos sobre la gestión de bancos de datos personales de la organización como parte de sus responsabilidades de trabajo. Por ello, COSAPI implementa una **Política de Protección de Datos Personales (PLT-SGSI-02)**, la cual brinda lineamientos comprometiéndose a proteger la seguridad y confidencialidad de la información de todos los bancos de datos inscritos con los que tiene vínculo, para garantizar el derecho al honor y a la intimidad, o sea utilizado para cometer actos ilícitos.

Los bancos de datos personales son inscritos en el Registro Nacional de Protección de Datos Personales que es administrado por la Autoridad Nacional de Protección de Datos Personales. Estos bancos están registrados en la **Matriz de bancos de datos personales (PLT-SGSI-02-F1)**.


5.8.2.1 Tratamiento de datos personales

COSAPI realiza el tratamiento de los datos personales de sus colaboradores, directores, accionistas, clientes y proveedores para una finalidad determinada, explícita y lícita, asegurándose que previamente el titular haya brindado su consentimiento. En el caso del tratamiento de datos personales sensibles, COSAPI asegura que el consentimiento se realice por algún mecanismo que garantice la voluntad inequívoca del titular.

Asimismo, COSAPI adopta las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos recopilados, los cuales se almacenan en los bancos de datos personales.

- Técnicas, por ejemplo: Generar copias de seguridad de los datos personales.
- Organizativas, por ejemplo: Identificar al personal autorizado para acceder a las bases de datos.
- Legales, por ejemplo: Elaborar directrices internas que oriente el tratamiento de datos personales en la entidad.

Las medidas de seguridad mencionadas son para garantizar confidencialidad de los datos personales, guardando reserva respecto de

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 25 de 38

los datos y sus antecedentes, que recae en el titular del banco de datos, en el encargado y en toda aquella persona que intervenga en el tratamiento; aún después de finalizada las relaciones con el titular del banco de datos personales.

En caso de que COSAPI identifique casos específicos en los cuales no se requiera el consentimiento del titular para el tratamiento de sus datos, éstos serán tratados según lo informa **la Ley N° 29733 - Ley de Protección de Datos Personales** en el artículo N° 14.

COSAPI asegura y verifica que los datos almacenados no serán utilizados para otras finalidades incompatibles con las previamente autorizadas por el titular.

5.8.2.1.1 Principios básicos para el tratamiento de datos personales

COSAPI se rige al cumplimiento de los 8 principios básicos para el tratamiento de datos personales, los cuales se detallan en la **Ley N° 29733 – Ley de Protección de Datos Personales**.

a) Principio de legalidad

Los datos personales deben ser legítimos conforme a la legislación aplicable, además, la recopilación de los datos personales debe realizarse de manera lícitas por medios confiables.

b) Principio de consentimiento

Todo tratamiento de datos personales debe contar con el consentimiento del titular.

c) Principio de finalidad


Los datos personales deben ser recopilados para una finalidad específica. Además, el tratamiento de datos personales no se debe extender a otra finalidad que no sea la establecida y aprobada por el titular.

d) Principio de proporcionalidad

El tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad por la cual fueron recopilados.

e) Principio de calidad

Los datos personales deben ser veraces y exactos, y, de ser necesario, actualizados, necesarios, pertinentes y adecuados respecto a la final con la cual fue recopilado. Asimismo, los datos personales deben conservarse de forma tal que garantice su seguridad por el tiempo necesario para cumplir con la finalidad de su tratamiento.

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 26 de 38

f) Principio de seguridad

Las medidas de seguridad implementadas deben ser apropiadas y acordes con el tratamiento que se vaya a realizar y con la categoría a la cual corresponden los de datos personales.

g) Principio de disposición de recurso

Todo titular de los datos personales debe contar con las vías necesarias para ejercer sus derechos.

h) Principio de nivel de protección adecuado


En caso de realizarse flujo transfronterizo, se debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar.

5.8.2.1.2 Ejercicio de derechos ARCO

Todos los colaboradores internos (empleados, obreros y practicantes) postulantes, proveedores, clientes, prospecto comercial, personal de empresas subcontratadas, accionistas y denunciantes tienen derecho.

- **Derecho de acceso:** Averiguar si sus datos están siendo usados, solicitar la información sobre el origen de dichos datos y, además, con quién los han compartido y todos los detalles de su uso.
- **Derecho de rectificación:** Actualizar o completar los datos personales faltantes cuando estos sean erróneos, inexactos o incompletos; para esto se deberá precisar qué datos se desea modificar o agregar en la solicitud y adjuntar un documento que lo valide.
- **Derecho de cancelación:** Solicitar la eliminación de sus datos personales siempre y cuando ya no cumplan una finalidad, cuando se haya revocado el consentimiento o haya transcurrido el plazo para su tratamiento.
- **Derecho de oposición:** Oponerse al tratamiento de sus datos personales almacenados en el banco de datos, en caso se estén usando los datos personales para otros motivos; para esto se deberá generar una solicitud para restringir su uso.

La aplicación de los derechos ARCO, permite obtener información sobre sus propios datos y el tratamiento que se le otorga, se desarrollan en el **Procedimiento para atención de solicitudes de ejercicio de derechos ARCO (PG-SGSI-04)**.

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 27 de 38

5.8.2.2 Transferencia de datos personales

La transferencia de datos personales implica la comunicación de datos personales dentro o fuera del territorio nacional, realizada a una persona distinta al titular de los datos personales, al encargado del banco de datos personales o al encargado del tratamiento de datos personales. En el caso de la transferencia fuera del territorio nacional, llamada también flujo transfronterizo, se realizará únicamente si COSAPI autoriza y garantiza la suficiente protección para el tratamiento que se vaya a aplicar.

COSAPI resguarda la privacidad de sus colaboradores, directores, accionistas, clientes y proveedores, por ello, asegura la no transferencia de información a terceros sin una previa autorización del titular. Sin embargo, según lo establece el artículo N° 14 de la **Ley N° 29733 - Ley de Protección de Datos Personales**, estos datos personales podrían ser transferidos sin consentimiento alguno a entidades administrativas, autoridades judiciales y/o policiales, en caso corresponda.


El **Procedimiento para la transferencia de datos personales (PG-SGSI-05)**, establece los lineamientos a seguir para solicitar de manera formal la transferencia de datos personales.

Por otro lado, COSAPI puede valerse de proveedores de servicios que considere conveniente para la realización de ciertas actividades definidas, en consecuencia, respecto a los datos personales almacenados, estos proveedores tendrán la condición de encargados de tratamiento de acuerdo con las disposiciones de la **Ley N° 29733 - Ley de Protección de Datos Personales** y su Reglamento.

5.8.3. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El Sistema de Gestión Integral de Riesgos establece el Proceso de Gestión Integral de Riesgos, el cual se ejecutará en el Sistema de Gestión de Seguridad de la Información, puesto que permitirá adoptar las medidas necesarias para tratar los riesgos de prácticas que atenten contra la seguridad de la información y delitos relacionados que pudieran derivarse. Por tal motivo, cuando la Gerencia de Ética, Riesgos y Cumplimiento planifica el Manual del Sistema de Gestión de Seguridad de la Información, se identifica y aborda los riesgos y oportunidades con el fin de asegurar que se logre sus objetivos, hacer seguimiento de la eficacia y lograr la mejora continua del sistema para prevenir o reducir efectos no deseados relacionados con la política y objetivos.

El Oficial de Seguridad de la Información siguiendo la Gestión Integral de Riesgos, elabora y define las acciones para abordar estos riesgos de prácticas que atenten contra la seguridad de la información y delitos relacionados, y las oportunidades de mejora, así como la integración de dichas acciones en los procesos del Manual del Sistema de Gestión de

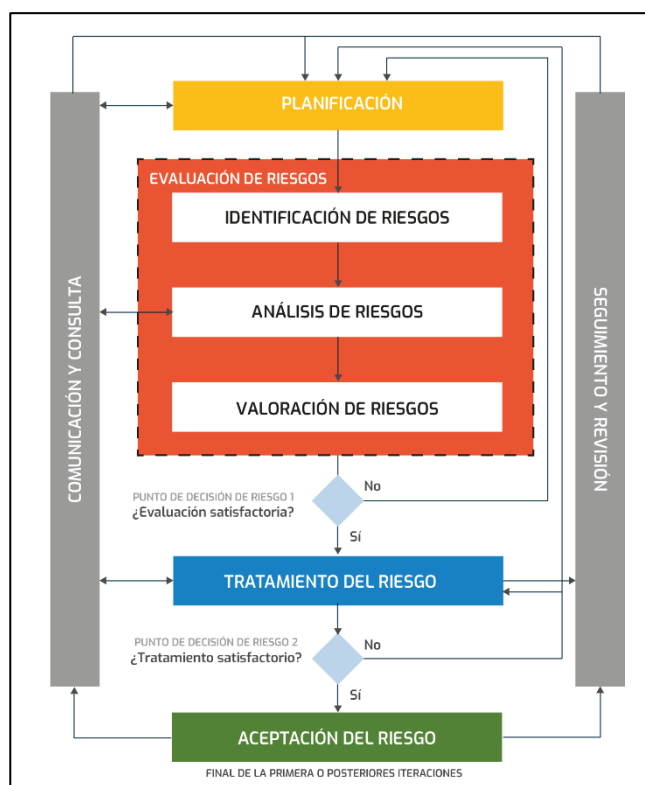
	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 28 de 38


Seguridad de la Información. Asimismo, planifica la evaluación de la eficacia de cada una, informando oportunamente al Comité de Sostenibilidad y al Directorio.

Para determinar, evaluar y establecer acciones para abordar los riesgos y oportunidades se empleará el formato **Matriz de Riesgos de Seguridad de la Información (MA-SGSI-01-F2)**; todos los procesos involucrados en la Gestión Integral de Riesgos se detallan en el **Manual de Gestión de Integral de Riesgos (MA-SIGR-01)**.

La base para aplicar y mantener el Sistema de Gestión de Seguridad de la Información de manera eficaz y eficiente es indispensable que, posterior a la identificación de activos, amenazas y vulnerabilidades; se establezca una metodología de evaluación del riesgo. Por ello, el área de Ética, Riesgos y Cumplimiento ha establecido un Sistema de Gestión Integral de Riesgos, el cual ha adoptado las metodologías internacionales del **Marco de Gestión de Riesgo Empresarial (COSO ERM 2017)**, la **Norma ISO 31000:2018 – Gestión de Riesgos** y la **Norma ISO 27005:2018 – Técnicas de Seguridad para la Gestión de Riesgos de Seguridad de la Información** para establecer el proceso de Gestión Integral de Riesgos de acuerdo con sus objetivos estratégicos o de negocio, de procesos y proyectos a fin de prevenir la materialización de los riesgos y fortalecer la eficiencia, efectividad, creación y protección del valor dentro de la organización.

El proceso de Gestión Integral de Riesgos detalla 4 actividades: Planificación, Evaluación, Tratamiento y Aceptación los cuales se encuentran en constante mejora continua.



	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO			
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 29 de 38	

5.8.3.1 Planificación

Es el proceso por el cual se identifica el alcance, contexto y criterios a considerar dentro del Sistema.

5.8.3.2 Evaluación

Es el proceso global que involucra identificación del riesgo, análisis del riesgo y valoración del riesgo.

La evaluación cuantifica o describe cualitativamente el riesgo y permite priorizar los riesgos según su gravedad percibida u otros criterios establecidos.

5.8.3.3 Tratamiento

El tratamiento del riesgo implica un proceso iterativo de:

- Formular y seleccionar opciones para el tratamiento del riesgo.
- Planificar e implementar el tratamiento del riesgo.
- Evaluar la eficacia del tratamiento del riesgo.
- Decidir si el riesgo residual es aceptable.
- Si no es aceptable, efectuar una iteración adicional del tratamiento.

5.8.3.3.1 Controles


Con el objetivo de proteger la información personal de sus trabajadores y la información de la organización, disminuyendo los riesgos que puedan atentar frente a ello; COSAPI vela por el cumplimiento de los estándares detallados en la **Norma ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información**. Ante ello, implementa los controles detallados en el documento **Declaración de Aplicabilidad (PLT-SGSI-01-F1)**, el cual los divide en los siguientes grupos:

a) Controles organizacionales

Los controles organizacionales se definen como conjunto de políticas, procedimientos o lineamientos auditables que son establecidos y atendidos por las gerencias correspondientes dentro de la organización. Estos controles tienen como objetivo cumplir con ayudar a gestionar la seguridad de la información de la organización, así como asegurar la confidencialidad, integridad y disponibilidad de la información.

b) Controles de personas

Los controles de personas se definen como conjunto de políticas, procedimientos o lineamientos auditables que son establecidos y atendidos por la Gerencia de Capital Humano. Estos controles tienen como objetivo gestionar al personal desde su ingreso hasta el término laboral; capacitándolo, detallando

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 30 de 38

sus responsabilidades durante el vínculo laboral y velando que la información tanto personal como compartida por la organización esté asegurada durante todo el proceso.

c) Controles físicos

Los controles físicos se definen como conjunto de políticas, procedimientos o lineamientos auditables que son establecidos y atendidos por la Gerencia de Administración y Finanzas, específicamente el área de Servicios Generales. Estos controles tienen como objetivo prevenir o detener el acceso al personal o terceros no autorizados a estructuras o espacios que almacenen información confidencial de la organización.

d) Controles tecnológicos

Los controles tecnológicos se definen como conjunto de políticas, procedimientos o lineamientos auditables que son establecidos y atendidos por la Gerencia de Tecnología de la Información. Estos controles garantizan cumplir con la confidencialidad, integridad y disponibilidad de la información en los sistemas o servicios tecnológicos.

5.8.3.4 Aceptación

Es el proceso mediante el cual se decide la aceptación de los riesgos y responsabilidades. Esta decisión será tomada y registrada formalmente.

La finalidad del Sistema de Gestión Integral de Riesgos es establecer la metodología de gestión de riesgos, mediante la planificación, evaluación, tratamiento y aceptación del riesgo, además de su control dentro de la organización. La metodología, responsabilidades y el proceso de Gestión Integral de Riesgos del Sistema se encuentra detallada en el documento **Manual del Sistema de Gestión Integral de Riesgos (MA-SGIR-01)**.

5.9. RECURSOS


a) Recursos e Infraestructura

La organización determina y proporciona los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.

b) Recursos físicos

La alta dirección de COSAPI proporciona la infraestructura necesaria para lograr que el Sistema de Gestión de Seguridad de la Información funcione con eficacia. La infraestructura incluye, cuando es aplicable:

- Edificios, espacio de trabajo y servicios asociados: En Sede Central es responsabilidad del Jefe de Servicios Generales, y en los proyectos del Administrador de obra,

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 31 de 38

- Equipos de Cómputo: La responsabilidad es de la Gerencia de Tecnología de la Información, quien brinda los recursos informáticos de la empresa (hardware y software de computadoras y teléfonos).

c) Recursos humanos

El Oficial de Seguridad de la Información en coordinación con el Gerente de Capital Humano proporciona las personas necesarias para la implementación eficaz de su Sistema de Gestión de Seguridad de la Información.

Todos los integrantes del área de Ética, Riesgos y Cumplimiento deben cumplir con el perfil descrito en el documento **Perfil de Puesto del Personal Empleado (MA-GC-01-F1)**.

d) Recursos financieros

Respecto a los recursos financieros, el área de Ética, Riesgos y Cumplimiento mantiene un presupuesto anual identificado para los gastos de las actividades relacionadas con el Modelo de Cumplimiento. Ello es corroborado e identificado en la contabilidad y en la verificación del destino efectivo de los gastos realizados.


5.10. COMPETENCIA

El Comité de Sostenibilidad en coordinación con la Gerencia de Capital Humano, determinan las competencias necesarias de las personas que forman parte de la Gerencia de Ética, Riesgos y Cumplimiento, logrando así asegurar que estás personas sean competentes, basándose en una educación, formación o experiencia apropiadas. Esta información se encuentra definida en el **Perfil de Puesto del Personal Empleado (MA-GC-01-F1)**.

5.10.1. Proceso de contratación

En relación con todo nuestro personal, los controles determinados por el Comité de Sostenibilidad que son ejecutados por la Gerencia de Capital Humano aseguran:

- Las condiciones de empleo, en las cuales se exigen al personal a cumplir con el Manual del Sistema de Gestión de Seguridad de la Información, y, a su vez, da a la organización el derecho de aplicar medidas disciplinarias al personal en caso de incumplimiento según lo establecido en el Reglamento Interno de Trabajo y el Código de Ética.
- En un periodo de tiempo razonable desde su incorporación al empleo, el personal recibirá una copia o se le dará acceso a la Política de Seguridad de la Información, Política de Protección de Datos Personales y a información relacionada con esa política, en caso aplique.
- Se tomen las acciones disciplinarias adecuadas contra el personal que infrinja las obligaciones, las políticas, los procesos y los procedimientos del Sistema de Gestión de Seguridad de la Información de COSAPI.
- Que el personal reciba y comprenda el Manual del Sistema de Gestión de Seguridad de la Información según lo establecido en el presente documento y el **Procedimiento de Reclutamiento y Selección de Personal (PG-ATE-**

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 32 de 38

01), Procedimiento de Atracción del Talento Obrero y Obrero Especializado (PG-ATO-01).

- Que el personal no sufrirá represalias, discriminación o medidas disciplinarias (como, por ejemplo, amenazas, aislamiento, degradación, impedimentos para su promoción, el traslado, despido, intimidación, victimización u otras formas de acoso) por:
 - Negarse a participar y/o rechazar, cualquier actividad respecto de la cual han juzgado razonablemente que existe más que un riesgo de comisión de prácticas que atenten contra la seguridad de la información u otros delitos relacionados y que dicho riesgo no ha sido mitigado por la organización; o
 - Plantear inquietudes, denunciar o informar hechos de buena fe, o sobre la base de una creencia razonable, de intento real o sospecha de realización efectiva de comisión de prácticas que atenten contra la seguridad de la información u otros delitos relacionados, o violación de la Política de Seguridad de la Información o del Manual del Sistema de Gestión de la Seguridad de la Información (excepto cuando el individuo participó en la comisión de la falta).


Asimismo, para el personal que participa de los procesos considerados expuestos a riesgos con probabilidad de ocurrencia y/o impacto medio y alto, la Gerencia de Capital Humano, ha establecido los siguientes controles:

- La debida diligencia a los candidatos antes de su contratación, y al personal antes de que sean transferidos o promovidos por la organización, con el fin de determinar, en la medida de lo razonable, que es apropiado emplearlos o reubicarlos y que cumplirán con los requisitos del Manual del Sistema de Gestión de Seguridad de la Información. Este procedimiento de debida diligencia se encuentra establecido en el **Procedimiento de Debida Diligencia PLAFT y Anticorrupción (PG-SPLAFT-01)**.
- No se fomentará la comisión de prácticas que atenten contra el Sistema de Gestión de Seguridad de la Información ni delitos relacionados que puedan perjudicar y/o alterar la realización de los objetivos detallados en el Manual del Sistema de Gestión de Seguridad de la Información, los cuales se revisan anualmente.

5.10.2. Difusión y capacitación periódica

5.10.2.1 Toma de conciencia y formación

El área de Ética, Riesgos y Cumplimiento facilita la toma de conciencia (sensibilización) y la formación en cumplimiento normativo para los trabajadores, Directores y Socios de Negocio resaltando el enfoque de mantener segura la información personal y de la organización, siguiendo los estándares recomendados por la **Norma ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información** y cumpliendo las normativas y leyes relacionadas. Estas acciones se realizan en coordinación con el área de Imagen y Comunicaciones, y con el área de Capital Humano.

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO			
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 33 de 38	

Se reconoce que el propósito de la formación es ayudar a asegurar que el personal pertinente entienda, según corresponda a su rol en la organización, los riesgos que atentan o afectan a la seguridad de la información y cualquier incumplimiento relacionado al Manual de Gestión de Seguridad de la Información, la Política de Gestión de Denuncias, cualquier acción preventiva, y de reporte necesario que requieran realizar en relación con cualquier riesgo de seguridad de la información.

El Plan de Capacitación determina el nombre, público objetivo y la frecuencia de las capacitaciones. Este plan se revisa y actualiza anualmente de acuerdo con las necesidades del grupo económico y la evaluación del Oficial de Seguridad de la Información. El plan se detalla en el documento **Plan Anual de Difusiones y Capacitaciones (PL-MC-01)** del Modelo de Cumplimiento de COSAPI.


El área de Ética, Riesgos y Cumplimiento facilita la toma de conciencia, considerado en el Plan de Capacitaciones, a sus socios de negocios que suponen riesgos que puedan atentar contra el Sistema de Gestión de Seguridad de la Información con probabilidad y/o impacto MEDIO, ALTO o MUY ALTO.

5.10.2.2 Comunicación

El área de Ética, Riesgos y Cumplimiento determina las comunicaciones internas y externas pertinentes al Manual del Sistema de Gestión de Seguridad de la Información. Para estos efectos, ha establecido un **Plan Anual de Difusiones y Capacitaciones (PL-MC-01)** del Modelo de Cumplimiento, el cual se llevará a cabo a través de los canales de comunicación establecidos por la organización (intranet, foro, correo electrónico, boletines, charlas, capacitaciones, reuniones de obra, comunicación directa, entre otros). Asimismo, los documentos relacionados al manual del Sistema de Gestión de Seguridad de la Información se ponen a disposición de todo el personal de la organización y socios de negocio en la:

- **Página web:** <https://www.cosapi.com.pe>
- **Repositorio web público:** [Sistema de Gestión de Compliance](#) en Conecta COSAPI
- **Intranet:** <https://intranet.cosapi.com.pe/intranet/>

Además, es comunicada directamente tanto al personal interno como a los socios de negocios que suponen más que un riesgo BAJO de prácticas que atenten contra el Sistema de Gestión de Seguridad de la Información y riesgos relacionados, y es publicada a través de los canales de comunicación internos y externos de la organización.

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 34 de 38

5.10.2.3 Información documentada

La gestión y control de información documentada del Sistema de Gestión de Seguridad de la Información se desarrolla en el **Procedimiento para la Elaboración y Control de la Información Documentada de los Sistemas de Gestión (PC-SG-01)** del Modelo de Cumplimiento.

5.11. EVALUACIÓN DEL DESEMPEÑO

5.11.1. Evaluación y monitoreo continuo del Manual del Sistema de Gestión de Seguridad de la Información

La gerencia de Ética, Riesgos y Cumplimiento aplica métodos apropiados para el seguimiento, y cuando sea aplicable, mide los procesos del Manual del Sistema de Gestión de Seguridad de la Información. Los métodos de seguimiento, medición, análisis y evaluación necesarios demuestran la capacidad de los procesos para alcanzar los resultados planificados. Los lineamientos para realizar el seguimiento y medición del Sistema de Gestión de Seguridad de la Información se recogen en el **Procedimiento de Seguimiento a los Objetivos del Modelo de Cumplimiento (PG-MC-01)**.


El Manual del Sistema de Gestión de Seguridad de la Información de COSAPI y los documentos que lo componen son evaluados mediante indicadores en el que se define a que se realizará seguimiento y medición, los responsables y frecuencia del seguimiento, así como la información documentada de estas evaluaciones.

Estos indicadores evalúan el logro de los objetivos del Sistema de Gestión de Seguridad de la Información y la eficacia y eficiencia del Manual del Sistema de Gestión de Seguridad de la Información, y están registrados en el **Registro de Seguimiento y Medición de Objetivos del MC y Sistemas (PG-MC-01-F1)**. El seguimiento de los indicadores está a cargo del Gerente Corporativo de Ética, Riesgos y Cumplimiento y se realizará semestralmente.

El Gerente Corporativo de Ética, Riesgos y Cumplimiento revisa aquellos indicadores que no alcancen los resultados planificados, lleva a cabo correcciones y acciones correctivas, según sea conveniente para asegurarse de la conformidad de los procesos.

5.11.2. Fuentes de opinión sobre el desempeño del Modelo de Cumplimiento

La gerencia Ética, Riesgos y Cumplimiento realizará encuestas de manera semestral a las partes interesadas de COSAPI a fin de obtener la percepción del desempeño del Modelo de Cumplimiento por parte de ellos. Todo hallazgo negativo que se identifiquen en las encuestas deberá generar un informe de No Conformidad a fin de evaluar la causa raíz del incumplimiento y asegurarse que se tomen las acciones adecuadas para subsanar el incumplimiento.

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO		
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 35 de 38

5.11.3. Informes de cumplimiento

El Seguimiento a los Objetivos del Manual del Sistema de Gestión de Seguridad de la Información es informado a la alta dirección y órgano de gobierno, a través del Comité de Sostenibilidad, en las reuniones de seguimiento a intervalos planificados de conformidad con lo señalado en el **Procedimiento de Seguimiento a los Objetivos del Modelo de Cumplimiento (PG-MC-01)**.

5.11.4. Auditoría

La organización lleva a cabo auditorías a intervalos planificados, para proporcionar información acerca el Manual del Sistema de Gestión de Seguridad de la Información, si se implementa y mantiene eficazmente y es conforme con:

- Los requisitos propios de la organización para el Manual del Sistema de Gestión de Seguridad de la Información;
- Los requisitos de la **Norma ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información**;
- Los requisitos de la normativa local e internacional vigente.

El área de Auditoría Interna elabora un programa de **Programa General de Auditoría Interna (PG-AI-01-F8)** tomando en consideración el estado y la importancia de los procesos y de las áreas a auditar, así como los resultados de auditorías previas. Se definen los criterios de auditoría, el alcance de la misma, su frecuencia y metodología. Esta documentación se encuentra especificada en el **Procedimiento para la Planificación y Ejecución de Auditorías Internas (PG-AI-01)**.

La selección de los auditores y la realización de las auditorías aseguran la objetividad e imparcialidad del proceso de auditoría. Los auditores no auditan su propio trabajo.


Se establece un procedimiento documentado para definir las responsabilidades y los requisitos para planificar y realizar las auditorías, establecer los registros e informar los resultados.

La dirección responsable del área que está siendo auditada se asegura de que se realicen las correcciones y se tomen las acciones correctivas necesarias sin demoras injustificadas para eliminar las no conformidades detectadas y sus causas, según lo señala el **Plan de Acción de Auditorías (PG-SG-03-F2)**. Las actividades de seguimiento incluyen la verificación de las acciones tomadas y el informe de los resultados de la verificación.

El Gerente de Auditoría Interna informa los resultados de las auditorías al órgano de gobierno, a través del Comité de Auditoría según corresponda.

Estas auditorías son razonables, proporcionales, y basadas en el riesgo; las cuales se ejecutan revisando los procedimientos, controles y sistemas para:

- Comisión o sospecha del delito de corrupción u otros delitos relacionados;

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO			
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 36 de 38	

- Falta por parte de los socios de negocios de cumplir con los requisitos anticorrupción aplicables de la organización; y debilidades u oportunidades de mejora en el Manual del Sistema de Gestión de Seguridad de la Información.

5.11.4.1 Ethical Hacking

Con el objetivo de realizar evaluaciones de seguridad para conocer sus vulnerabilidades existentes en sus sistemas que almacenan información, COSAPI ejecutará como mínimo un (01) Ethical Hacking de manera bianual. Posterior a ello, con apoyo del informe generado por los especialistas, se ejecutará planes de acción de mejora continua en el Sistema de Gestión de Seguridad de la Información.

5.11.5. Revisión por la dirección


La Gerencia General es responsable de revisar como mínimo 01 vez al año el funcionamiento del Modelo de Cumplimiento conforme se señala en el **Procedimiento de Seguimiento a los Objetivos del Modelo de Cumplimiento (PG-MC-01)**.

5.12. MEJORA

5.12.1. No conformidades y acciones correctivas / Observaciones / Oportunidades de Mejora

Conscientes de que, pese a todos los controles establecidos, es posible que aparezcan no conformidades / observaciones asociadas al Manual del Sistema de Gestión de Seguridad de la Información, por tal motivo, la Gerencia de Ética, Riesgos y Cumplimiento ha desarrollado el **Procedimiento de No Conformidades y Acciones Correctivas (PG-SG-04)**, en el que se definen las acciones que se adoptan para:

- Reaccionar inmediatamente ante la no conformidad / observación, y según sea aplicable:
 - Tomar acciones para controlarla y corregirla,
 - Hacer frente a las consecuencias;
- Evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante:
 - La revisión de la no conformidad,
 - La determinación de las causas de la no conformidad, y
 - La determinación de si existen no conformidades similares, o que podrían ocurrir;
- Implementar cualquier acción necesaria;
- Revisar la eficacia de cualquier acción correctiva tomada;
- Si fuera necesario, hacer cambios al Manual del Sistema de Gestión de Seguridad de la Información.

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO			
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 37 de 38	

5.12.2. Mejora Continua del Manual del Sistema de Gestión de Seguridad de la Información


La Gerencia de Ética, Riesgos y Cumplimiento busca la mejora continua para la idoneidad, adecuación y eficacia del Manual del Sistema de Gestión de Seguridad de la Información.

Para ello, atendemos al Proceso de Auditorías, Gestión de No Conformidades y Acciones Correctivas. Este proceso de mejora incluye la adopción de acciones correctivas y/o cambios al modelo ante la ocurrencia de eventos, violaciones al mismo, cambios en la estructura de la organización, en el desarrollo de sus actividades o ante factores internos o externos que impliquen cambios en el perfil de riesgos identificados que sirvió para la elaboración del modelo de prevención desarrollado en el **Procedimiento para la Planificación y Ejecución de Auditorías (PC-SG-03)**.

5.12.2.1 Lecciones aprendidas por monitoreo, seguimiento o eventos de seguridad de la información

En relación con la gestión general de los eventos de seguridad de la información, la Gerencia de Ética, Riesgos y Cumplimiento, con el objetivo de ser más eficientes y consumir únicamente los recursos imprescindibles dentro de los parámetros de funcionamiento establecidos y asumidos por la organización, detalla lo siguiente:

- Cada vez que el personal involucrado en el Sistema de Gestión de Seguridad de la Información identifique una oportunidad de mejora o cambio, será responsable de comunicarla al Oficial de Seguridad de la Información, Jefe de Gestión de Riesgos, Analista de Riesgos de Seguridad de la Información o al responsable del proceso en el cual se ha identificado la oportunidad de mejora o cambio.
- El responsable de cada proceso en conjunto con el Oficial de Seguridad de la Información, Jefe de Gestión de Riesgos y el Analista de Riesgos de Seguridad de la Información deben identificar y evaluar las acciones de mejora a implementar posterior al análisis de un evento detectado. En caso la evaluación determine un resultado positivo, la implementación deberá ser aprobada por el Comité de Sostenibilidad; caso contrario se deberá solicitar un nuevo análisis que identifique acciones más viables de implementar.
- El responsable de cada proceso en conjunto con el Oficial de Seguridad de la Información, Jefe de Gestión de Riesgos y el Analista de Riesgos de Seguridad de la Información son los responsables de crear un plan de acción para la implementación de Oportunidades de Mejora y Cambios.
- El Oficial de Seguridad de la Información con apoyo del Jefe de Gestión de Riesgos y el Analista de Riesgos de Seguridad de la Información realizará seguimiento y monitoreará los planes de acción con el fin de comprobar su cumplimiento y eficacia de estos.

	GERENCIA DE ÉTICA, RIESGOS Y CUMPLIMIENTO			
Manual del Sistema de Gestión de Seguridad de la Información	Código: MA-SGSI-01	Rev. 00	Página: 38 de 38	

- El responsable de cada proceso ejecutará el plan de acción que corresponda a su gestión o se le haya derivado.

6. SANCIONES

La aplicación de sanciones por incumplimiento a este documento y/o al Sistema de Gestión de Seguridad de la Información se desarrolla en **el Código de Ética (COD-EyC-01)** y **Reglamento Interno de Trabajo (RIT 2023)**, sin perjuicio de la aplicación de sanciones de la **Ley N° 30096 – Ley de Delitos Informáticos** y la **Ley N° 29733 – Ley de Protección de Datos Personales**, en caso corresponda.

7. CANALES DE DENUNCIA

Todo incumplimiento al presente documento, así como a todos los documentos del Sistema de Gestión de Seguridad de la Información e identificación de riesgos que atenten contra la Seguridad de la Información se reportarán a través de nuestro canal ético COSAPI TE ESCUCHA, el cual emplea distintos canales de comunicación para plantear consultas o informar sobre algún incumplimiento relacionado con cualquier aspecto relativo al Sistema de Gestión de Seguridad de la Información a través de: <https://www.cosapiteescucha.com/> y cumplimiento@cosapi.com.pe. El tratamiento y consultas de denuncias se desarrollan en el **Procedimiento de tratamiento de denuncias y consultas (PG-SGD-01)**.