## I. OBJETIVO

Establecer lineamientos que permitan asegurar la confidencialidad, integridad y disponibilidad de la información (incluye los recursos que la soportan) de CENTRIA (en adelante **LA EMPRESA**), y establecer un marco de referencia para el establecimiento de los objetivos de seguridad de la información.

## II. ALCANCE

Es de aplicación para todo el personal (indistintamente de su nivel jerárquico o modalidad de contratación), partes externas y/o clientes que acceden y manejan información de **LA EMPRESA.**

## III. REFERENCIAS

- Ley N°29733, Protección de datos personales, su reglamento y directivas asociadas.
- Ley N° 31572, Teletrabajo.
- Decreto Supremo N° 002-2023-TR - Decreto Supremo que aprueba el Reglamento de la Ley N° 31572, Ley que regula el Teletrabajo.
- NTP-ISO/IEC 27001:2014 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos.
- NTP-ISO/IEC 27002:2017 Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información.
- Cybersecurity Framework de NIST de los Estados Unidos.
- Reglamento Interno de Trabajo.
- POL-AL-01-02 Política de Protección de Datos Personales.
- POL-SI-01-06 Política de Gestión de Dispositivos Móviles
- POL-SI-01-13 Política de seguridad de la información en las relaciones con los terceros
- POL-SI-01-19 Transferencia de información
- POL-SI-01-20 Política de Uso aceptable de activos de información
- POL-SI-01-02 Política de Clasificación, Etiquetado y Disposición de Información y Datos
- POL-SI-01-03 Política de Controles criptográficos
- POL-SI-01-15 Política de Seguridad en las Instalaciones
- POL-TGE-04-18 Política de Teletrabajo
- POL-SI-01-17 Política de Seguridad para equipos BYOD
- POL-SI-01-21 Política de Gestión de datos durante todo el ciclo de vida del dato
- POL-SI-01-11 Política de Seguridad de Accesos
- POL-SI-01-09 Política de Gestión de Usuarios Privilegiados
- POL-SI-01-10 Política de Gestión de Vulnerabilidades
- POL-SI-01-05 Política de Gestión de Cambios
- POL-TI-01-07 Política de Desarrollo Seguro
- POL-SI-01-16 Política de Seguridad en Servidores
- POL-SI-01-07 Política de Gestión de Incidentes
- POL-SI-01-08 Política de Gestión de Registros de Auditoría
- POL-SI-01-14 Política de Seguridad de la Red
- POL-SI-01-22 Política de Gobierno y Seguridad en la nube
- POL-SI-01-01 Política de Ciberseguridad

## IV. DEFINICIONES

- **Activo Información**

Es todo ente que trata información ya sea en forma física o digital, y que tiene valor para la organización.

- **Activo Informático**

Los activos informáticos son recursos tangibles e intangibles basados en la tecnología que almacenan, procesan y transmiten la información necesaria para que la empresa siga funcionando. Ejemplos: equipos de cómputo, tablets, impresoras, celulares corporativos, servidores, etc.

- **Confidencialidad**

Significa que a los datos y a los sistemas solo accedan personas debidamente autorizadas. Y que la información por su sensibilidad no debe ser compartida ni divulgada a personas no autorizadas.

- **Disponibilidad**

Significa que la información y los sistemas pueden ser utilizados en la forma y tiempo requeridos por una entidad autorizada.

- **Evento de seguridad de la información**

Una ocurrencia que una organización considera que posee implicaciones potenciales a la seguridad de un sistema o su entorno.

- **Gerencia de Área**

Lo comprenden los siguientes roles: Gerente de Talento y Gestión Estratégica, Gerente de Seguridad de la Información, Gerente General y Gerente de Sistemas e Innovación en Tecnología, y Gerente de Contraloría.

- **Gestión de Riesgos**

Consiste en la identificación, análisis y evaluación de riesgos, así como la planificación, implementación y su correspondiente seguimiento de las acciones de tratamiento del riesgo.

- **Incidente Seguridad de la Información**

Uno o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de negocios y amenazar la seguridad de la información.

- **Integridad**

Significa exactitud de la información y de los sistemas contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.

- **Sistema de Gestión de Seguridad de la Información**

Conocido también por sus siglas SGSI, es un conjunto de políticas, procedimientos y lineamientos junto a los recursos y actividades asociados que son gestionados colectivamente

por una organización, en la búsqueda de proteger la confidencialidad, integridad y disponibilidad de sus activos de información.

- **Tratamiento de Información**

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 la información.

## V. ROLES Y RESPONSABILIDADES

- **COLABORADOR:**

Cumplir con los lineamientos especificados en el presente documento.

- **Comité Ejecutivo de SI:**

Revisar y aprobar las políticas de seguridad de la información y asegurar que sea compatible con los objetivos estratégicos de LA EMPRESA.
Promover el cumplimiento de las políticas de seguridad de la información en LA EMPRESA.

- **GERENTE DE SEGURIDAD DE LA INFORMACION:**

Garantizar la definición, actualización y difusión de los lineamientos establecidos en el presente documento, así como asegurar y promover su cumplimiento.

- **Proveedor:**

Cumplir con los lineamientos especificados en el presente documento que le resulten aplicables.

## VI. POLÍTICAS

### 1. Enunciado de la Política General de Seguridad de la Información

**LA EMPRESA** considera a la información como un activo valioso para el cumplimiento de sus funciones, alcance de su propósito ***(Aceleramos las oportunidades del presente para asegurar un futuro mejor)*** y de sus objetivos. Por tanto, resulta necesario gestionar la seguridad de la información a través de medidas que aseguren su confidencialidad, integridad y disponibilidad, por ello se compromete a:

- Cumplir con los requisitos aplicables en seguridad de la información.
- Promover la adopción de una cultura en seguridad de la información que prevenga la ocurrencia o mitigue el impacto de situaciones que atenten contra la confidencialidad, integridad y disponibilidad de la información.
- Mejorar continuamente nuestro SGSI, evaluando permanentemente su desempeño.

### 2. Políticas Específicas de Seguridad de la Información

La Política General de Seguridad de la Información se soporta en una serie de políticas específicas que proporcionan lineamientos sobre tópicos específicos, las cuales buscan complementar la presente política.

## 3. Lineamientos de la Política General de Seguridad de la Información

**3.1.** **LA EMPRESA** se compromete a definir roles y responsabilidades para abordar las actividades de seguridad de la información.

**3.2.** **LA EMPRESA** debe establecer y mantener contactos con autoridades y grupos de interés relacionados al rubro de seguridad de la información.

**3.3.** La información de **LA EMPRESA** debe ser clasificada, etiquetada y gestionada en función de su valor, nivel de sensibilidad, requisitos legales y criticidad para **LA EMPRESA, según lo establecido en POL-SI-01-02 Política de Clasificación, Etiquetado y Disposición de Información y Datos.**

**3.4.** **LA EMPRESA** debe definir lineamientos para controlar el acceso físico (**POL-SI-01-15 Política de Seguridad en las Instalaciones**) y lógico (**POL-SI-01-11 Política de Seguridad de Accesos**) a la información corporativa y a los activos asociados en función a las necesidades del negocio y la seguridad de la información.
En ese sentido, establece requisitos de seguridad más exhaustivos para usuarios privilegiados en **POL-SI-01-09 Política de Gestión de Usuarios Privilegiados.**

**3.5.** Todo Colaborador de **LA EMPRESA** que realice teletrabajo deberá cumplir con los lineamientos descritos en **POL-TGE-04-18 Política de Teletrabajo.**

**3.6.** **LA EMPRESA** debe definir procedimientos seguros para la contratación de su personal en donde considerará controles de comprobación de antecedentes de los postulantes que permita la Ley y otros para los cuales de considerarlo pertinente requerirá el consentimiento expreso del titular de acuerdo con la normativa vigente.
Así también establece compromisos contractuales con sus **Colaboradores**, en donde se incluye cláusula de confidencialidad, de protección de datos personales entre otros; además brinda autorización expresa y fidedigna de forma excepcional a sus correos electrónico ante un peligro o duda razonable que ponga en contingencia a **LA EMPRESA.**
Así también todo cese o rotación de empleo debe ser controlado de forma segura por procedimientos establecidos por la **Gerencia de Talento y Gestión Estratégica.**

**3.7.** Todo Colaborador de **LA EMPRESA** se encuentra obligado a cumplir con los cursos de concientización y capacitación en seguridad de la información que le fueran asignados. **LA EMPRESA** es responsable de incluir como parte de su proceso de inducción de todo nuevo **Colaborador** contenidos referentes a seguridad de la información.

**3.8.** Todo **Colaborador** de **LA EMPRESA** debe notificar de forma oportuna cualquier evento o incidente de seguridad de la información a través de la **Mesa de Servicios.** Esto incluye los casos de pérdida o robo de activos informáticos que tratan información corporativa, en donde una notificación oportuna permite el bloqueo y borrado de información para proteger la información.
**LA EMPRESA** debe establecer los procesos para una gestión adecuada de eventos e incidentes de seguridad de la información para dar cumplimiento a **la POL-SI-01-07 Política de Gestión de Incidentes.**
En ese sentido **LA EMPRESA** establece los requisitos de seguridad asociados a la protección de los activos de información ante amenazas cibernéticas en la **POL-SI-01-01 Política de Ciberseguridad.**

**3.9.** Todo incumplimiento a la **Política General de Seguridad de la Información** y/o a las políticas de tópicos específicos se considerará una falta que será sancionada según el **Reglamento Interno de Trabajo** de conformidad con su gravedad.

**3.10.** **LA EMPRESA** define lineamientos para el uso aceptable de activos de información **(POL-SI-01-20 Política de uso aceptable de activos de información)** para garantizar la confidencialidad, integridad y disponibilidad de la información tanto física y digital.
En ese sentido, también define lineamientos que regulan la transferencia de información corporativa entre áreas interna de **LA EMPRESA,** con proveedores, clientes y otros agentes externos **(POL-SI-01-19 Política de Transferencia de información).**

Además, establece requisitos de seguridad para los servidores que administra en **POL-SI-01-16 Política de Seguridad en Servidores.**

Dado que la mayor parte de activos de información se encuentran en la nube, **LA EMPRESA** establece los requisitos de seguridad en la **POL-SI-01-22 Política de Gobierno y Seguridad en la nube.**

**3.11.** **LA EMPRESA** incorpora requisitos de seguridad de la información en la gestión del ciclo de vida de sus proyectos de cualquier índole, y asegura la gestión de riesgos de seguridad de información de éstos para garantizar que no solo sean funcionales sino también seguros.

**3.12.** De forma anual o cuando ocurren cambios significativos en los procesos, organización y/o tecnología; **LA EMPRESA** ejecuta la gestión de riesgos de seguridad de la información en los procesos de negocio, garantizando un mantenimiento adecuado del **Inventario de Activos de Información.** Así también, aborda los riesgos y oportunidades del SGSI como parte de las actividades que le permiten la mejora continua.

**3.13.** **La Gerencia de Sistemas e Innovación en Tecnología** de **LA EMPRESA** define procedimientos seguros para la devolución y reasignación de activos informáticos corporativos.

**3.14.** **LA EMPRESA** establece requisitos de seguridad que regulan la relación con sus proveedores durante todo su ciclo de vida. Estos requisitos son de obligatorio cumplimiento para proveedores que tratan información corporativa, los mismos se encuentran en la **POL-SI-01-13 Política de seguridad de la información en las relaciones con los terceros,** la cual está disponible desde la página web de **LA EMPRESA.**

**3.15.** Consideramos que la continuidad de negocio y de TI es vital para garantizar el propósito de **LA EMPRESA** y de nuestros clientes, por ello se es responsable de mantener una gestión adecuada de la continuidad de nuestros procesos de negocio críticos, así como de nuestros servicios de TI críticos, a efectos de garantizar su recuperación dentro de los umbrales esperados.

En ese sentido, deberá realizar copias de respaldo de la información del negocio de forma periódica, a fin de minimizar la pérdida de información crítica ante alguna incidencia.

**3.16.** No se debe publicar NADA que pueda poner en peligro la privacidad de **LA EMPRESA o** de su personal, a través de redes sociales o algún otro medio.

**3.17.** Se deben proteger los derechos de propiedad intelectual, los cuales abarcan derechos de copia (*"copyright"*), derechos de diseño, marcas registradas, patentes, licencias de código fuente, etc. de sistemas, recursos y desarrollos de **LA EMPRESA.**

**3.18.** Los datos personales que trate **LA EMPRESA** deben estar debidamente protegidos en todos los ambientes dónde residan, a fin de reducir los riesgos asociados a accesos indebidos, mal uso o divulgación no autorizada, etc.

En ese sentido **LA EMPRESA** dispone de la **POL-SI-01-21 Política de Gestión de datos durante todo el ciclo de vida del dato**, que regula el mapeo del ciclo de vida del dato.

**3.19.** **LA EMPRESA** debe mantener un registro actualizado de los requisitos legales, reglamentarios y contractuales propios del negocio y de seguridad de la información.

**3.20.** **LA EMPRESA** dispone de mecanismos que le permiten revisar de forma independiente el cumplimiento de los requisitos de seguridad de la información, los cuales son realizados a intervalos planificados o siempre que se produzcan cambios significativos.

**3.21.** Todos los documentos internos de **LA EMPRESA** son puestos a disposición de los **Colaboradores** a través del sistema de gestión documental.

**3.22.** **LA EMPRESA** cuenta con procesos para garantizar el mantenimiento de los activos informáticos que resulten aplicables.

**3.23.** Se debe realizar, por lo menos una (01) vez al año, un análisis sobre la red y los sistemas de **LA EMPRESA**, que permitan identificar vulnerabilidades a ataques

externos o internos. Los lineamientos respecto a esta materia son establecidos en la **POL-SI-01-10 Política de Gestión de Vulnerabilidades.**

**3.24.** Se debe contar con un proceso de control de cambios en los sistemas, aplicaciones y recursos de **LA EMPRESA**, el cual incluya un análisis de impacto y riesgo del cambio, y una especificación de los controles de seguridad necesarios.
De igual manera, toda iniciativa o proyecto que contemple la implementación o adquisición de un servicio, sistema o software debe contar con la participación de la **Gerencia de Seguridad de la Información** desde la concepción del requerimiento hasta su salida en vivo, a fin de cumplir con los requisitos mínimos de seguridad necesarios.
Se define la **POL-SI-01-05 Política de Gestión de Cambios** donde se establecen los requisitos de seguridad en esta materia.

**3.25.** **LA EMPRESA** prohíbe el uso de medios de almacenamiento removibles como USB, disco duro externo, DVD, Blu-ray, entre otros afines; para lo cual ha establecido el bloqueo de toda funcionalidad para transferencia de información en los equipos de cómputos. Sin embargo, las excepciones deberán ser debidamente justificadas y autorizadas por la **Gerencia de Área respectiva**.

**3.26.** **LA EMPRESA** debe establecer controles para prevenir la fuga de información corporativa sensible hacia agentes no autorizados (tales como filtrado de las webs, cifrado de disco duro de equipos de cómputo, cifrado de información digital, entre otras).
Los lineamientos en torno a los controles de cifrado son definidos en **POL-SI-01-03 Política de Controles criptográficos**. Por otro lado también, deberá disponer de controles contra programas maliciosos.

**3.27.** Todo **Colaborador** debe tener restringido el perfil de administrador local en su equipo de cómputo para evitar la instalación de software o sistemas no autorizados en el equipo y que no estén acorde a sus funciones y/o responsabilidades. Excepcionalmente, se asignará sólo a los usuarios que cuenten con el debido sustento asociado estrictamente a sus funciones, así como la autorización de su **Gerencia de Área respectiva**.

**3.28.** **LA EMPRESA** define requisitos de seguridad en el ciclo de vida del desarrollo de software corporativo, a efectos de garantizar su funcionalidad y la seguridad de la información que traten a través de **POL-TI-01-07 Política de Desarrollo Seguro**.

**3.29.** Se define controles para asegurar las redes y dispositivos de red de **LA EMPRESA**, a fin de proteger la información corporativa que se trasmita por estos medios. Los requisitos de seguridad son definidos en **POL-SI-01-14 Política de Seguridad de la Red**.

**3.30.** **LA EMPRESA** debe realizar una supervisión periódica y realizar los ajustes respectivos para garantizar la adecuada gestión de capacidades.

**3.31.** Todos los colaboradores de **LA EMPRESA** deben proteger la información del negocio, por ende, deberán cumplir con lo siguiente:

a. No dejar documentos físicos ni medios digitales removibles a la vista o que sean de fácil acceso por terceras personas.
b. Bloquear la sesión cuando no se esté usando la computadora, tanto en casa como en lugares públicos (“Windows + L” o “Ctrl + Atl + Supr”)
c. No registrar las contraseñas o información de accesos en lugares que sean accesibles por personas no autorizadas. (Ejemplo: notas adhesivas, blocks, etc.)
d. No abrir archivos, enlaces ni páginas sospechosas que se reciban por correo electrónico.
e. Usar soluciones de cifrado para la información corporativa y correos sensibles.
f. No usar correos personales para compartir información corporativa.
g. Trabajar la información en repositorios que cuenten con backup: OneDrive, Sharepoint y MS Teams.

**3.32.** Todo equipo de cómputo corporativo de **LA EMPRESA** debe contar con las soluciones de seguridad definidas en la **POL-SI-01-06 Política de Gestión de**

**Dispositivos Móviles**. Solo para casos excepcionales (casos de contratación fuera de Perú), el Colaborador podrá utilizar sus equipos personales para fines laborales, y deberá ceñirse a los lineamientos descritos en **POL-SI-01-17 Política de Seguridad para equipos BYOD.**

**3.33.** **LA EMPRESA** debe mantener la gestión de la configuración de los activos informáticos que administra para garantizar el correcto funcionamiento de estos.

**3.34.** **LA EMPRESA** reconoce la importancia de una adecuada gestión de los registros de auditoría, razón por la cual establece lineamientos para su protección en **POL-SI-01-08 Política de Gestión de Registros de Auditoría.**

## VII. ANEXOS

- Manual del Sistema de Gestion de Seguridad de la Informacion
- Estrategia de Continuidad del Servicio ONBASE
- Estrategia de Continuidad del Servicio SAP HANA

## VIII. CONTROL DE CAMBIOS

## IX. APROBACIÓN

| | Nombre | Cargo | Fecha |
|---|---|---|---|
| 1. Dueño | VERONICA VANESSA ORDOÑEZ | COORDINADOR DE GOBIERNO Y RIESGOS DE SEGURIDAD | 20/02/2024 |
| 2. Editor | LUIS RIVERA | ANALISTA DE GOBIERNO Y RIESGOS DE SEGURIDAD | 22/02/2024 |
| 3. Revisor | ANGELLO GIURIA | ANALISTA DE PROCESOS | 27/02/2024 |
| 4. Aprobador | PEDRO TRINIDAD LOZADA | GERENTE GENERAL | 27/02/2024 |
| 4. Aprobador | RICARDO ROJAS | GERENTE DE SISTEMAS E INNOV. EN TECNOLOG | 18/03/2024 |
| 4. Aprobador | MARIA FERNANDA GIAMBERINI | GERENTE DE TALENTO Y GESTIÓN ESTRATÉGICA | 12/03/2024 |
| 4. Aprobador | JUAN CARLOS MENDOZA | GERENTE DE SEGURIDAD DE LA INFORMACION | 29/02/2024 |