I. OBJETIVO

Establecer los principios, bases, lineamientos y normas que permitan ejercer los controles necesarios para una adecuada gestión de los activos de **CENTRIA** (en adelante **LA EMPRESA**) a los que tienen acceso los terceros.

II. ALCANCE

El presente documento "Política de seguridad de la información en las relaciones con los terceros" se aplicará en los siguientes puntos:

- Acceso de los terceros a los aplicativos de **LA EMPRESA**
- Acceso de los terceros a los datos de **LA EMPRESA**
- Acceso de los terceros a las instalaciones 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.
- POL-SI-01-12 Política General de Seguridad de la Información.
- POL-AL-01-02 Política de Protección de Datos Personales.
- POL-SI-01-15 Política de Seguridad en las Instalaciones.
- DOC-SI-01-30 Metodología de gestión de riesgos y oportunidades del SGSI, de riesgos de seguridad de la información de procesos y proyectos

IV. DEFINICIONES

- **Tercero**

Cualquier persona, natural o jurídica, externa a CENTRIA que no mantiene de manera directa una relación contractual con CENTRIA.

V. ROLES Y RESPONSABILIDADES

- **COLABORADOR:**

- Informar a los terceros que tenga a cargo las responsabilidades de seguridad de la información que le resulten aplicables.

- Asegurar la confidencialidad, integridad y disponibilidad de la información de **LA EMPRESA.**

- **GERENTE DE SEGURIDAD DE LA INFORMACION:**
- Velar por el cumplimiento de los lineamientos de seguridad de la información en las relaciones con los terceros establecidos por **LA EMPRESA.**

- **Tercero:**
- Cumplir con los lineamientos de seguridad de la información que le resulten aplicables.

VI. POLÍTICAS

PREVIO A LA RELACIÓN CON UN TERCERO

Antes de contratar a un tercero se debe tener en consideración los siguientes lineamientos de acuerdo con cada acápite:

Abordar la seguridad dentro de los acuerdos con terceros

- Los acuerdos con los terceros deben ser establecidos y documentados para garantizar que no existan malentendidos entre **LA EMPRESA** y terceros respecto a las obligaciones de ambas partes para cumplir con los requisitos relevantes de seguridad de la información.
- Se debe establecer y acordar todos los requisitos de seguridad de la información alineados al principio de mínimo conocimiento con cada tercero que pueda tener acceso a procesar, almacenar, comunicar o suministrar activos de información de **LA EMPRESA**.
- La información que sea proporcionada y/o accedida por un tercero debe estar identificada y descrita en los acuerdos, en conjunto con los métodos con los que se proporcionará y/o accederá el tercero a la información.
- La información compartida con terceros debe estar clasificada de acuerdo con el esquema de clasificación de **LA EMPRESA** (confidencial, reservada, interna o pública).
- Los requisitos legales y regulatorios deben ser incluidos en los contratos, como la protección de datos, los derechos de propiedad intelectual y los derechos de autor de programas de software, documentación u otra información generada o proporcionada por **LA EMPRESA**.
- Se debe exigir que, en todos los contratos o acuerdos con terceros, que implique un intercambio, uso o procesamiento de información de **LA EMPRESA**, cuenten con acuerdos de confidencialidad y/o acuerdos de protección de datos sobre el manejo de la información.
- Se debe definir las reglas de uso aceptable de la información, incluido el uso inaceptable, de ser necesario.
- En los acuerdos se debe definir reglas para la comunicación de cualquier evento entre **LA EMPRESA** y terceros, dando manejo adecuado a los incidentes de Seguridad de la Información.
- El tercero debe proporcionar capacitación y supervisión continua (mínimo anualmente) sobre privacidad y protección de la información para todo su personal, siempre que acceda a la información de **LA EMPRESA**. Es posible que **LA EMPRESA** pida proporcionar alguna capacitación adicional que considere razonablemente necesaria para que el tercero lo realice.

- Para los asuntos de seguridad de la información se debe determinar una persona de contacto, así como el número telefónico y/o correo electrónico al cual habrá que dirigir las solicitudes. Las personas de contacto son los responsables de negocio de **LA EMPRESA** que adquirieron servicios de terceros.
- Se debe determinar derechos de auditoría de las prácticas de seguridad y privacidad de la información del tercero y/ o el subcontratista.
- Se debe asegurar que el tercero brinde reportes sobre la efectividad de los controles de manera periódica, asimismo debe establecerse un acuerdo sobre la corrección oportuna de las cuestiones relevantes planteadas en el reporte según corresponda.
- En los contratos o acuerdos con los terceros se debe incluir una causal de terminación del acuerdo o contrato de servicios, por el incumplimiento de las políticas de seguridad de la información.
- Se debe determinar en los acuerdos la obligación de no divulgar la información y de mantener el acuerdo aun después de terminar la relación contractual.
- En los acuerdos se deben incluir las obligaciones de los terceros una vez terminada la relación contractual.
- Todo análisis y evaluación de riesgos de las relaciones con terceros se basan en los lineamientos de **DOC-SI-01-30 Metodología de gestión de riesgos y oportunidades del SGSI, de riesgos de seguridad de la información de procesos y proyectos.**

Cadena de suministro de tecnología de información y comunicación

- Los acuerdos con terceros deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos, con el fin de asegurar la seguridad de los productos de tecnología de información y de la comunicación para que funcionen de manera adecuada.

DURANTE LA RELACIÓN CON UN TERCERO

Posterior a la contratación de un tercero se debe tener en consideración los siguientes lineamientos de acuerdo con cada acápite:

Generalidades

- El equipo de Seguridad de la Información debe informar sobre los lineamientos de seguridad en la relación con un tercero al personal de **LA EMPRESA** que interactúa con el personal de los terceros, respecto a las reglas apropiadas de compromiso y comportamiento basado en el tipo de tercero y en el nivel de acceso de los terceros a los sistemas e información de **LA EMPRESA**.
- El tercero deberá acceder a las instalaciones de **LA EMPRESA**, cumpliendo los lineamientos de **POL-SI-01-15 Política de Seguridad en las Instalaciones.**

Monitoreo y revisión de servicios de los terceros

- El monitoreo y la revisión de los terceros de servicios deben garantizar el cumplimiento de los términos y condiciones de seguridad de la información, de los acuerdos y que los incidentes y problemas de seguridad de la información estén gestionados correctamente.
- Las evaluaciones de riesgos deben llevarse a cabo y revisarse cuando la relación con el tercero cambia significativamente, incluidas las renovaciones de contratos**.**
- Los niveles de desempeño de los servicios brindados por el tercero deben ser monitoreados para verificar la adhesión a los acuerdos.
- Se deben revisar los reportes del servicio entregados por los terceros y agendar reuniones regulares de progreso según los requisitos de los acuerdos

- Considerar la realización de auditorías o solicitar evidencia de la ejecución de auditorías independientes relacionadas al riesgo tecnológico, control interno, o auditorías de certificación de seguridad de la información para asegurar que los terceros que prestan servicios cuenten con buenas prácticas en seguridad de la información. Adicionalmente, **LA EMPRESA** también podrá realizar visitas programadas y supervisadas a las instalaciones de los terceros que presten servicios de resguardo de activos de información, con el objeto de verificar en campo las condiciones de seguridad implementadas.
- El tercero debe proporcionar información sobre incidentes de seguridad de la información que afecten a **LA EMPRESA** por los canales adecuados alineados a los acuerdos que se especifiquen en el contrato del tercero. Asimismo, deberá resolverlos y gestionarlos.
- Exigir que el tercero mantenga la suficiente capacidad de servicio junto con los planes realizables diseñados para garantizar que los niveles de continuidad de servicio brindados se mantendrán después de fallas importantes en el servicio o desastres.

Gestión de cambios a los servicios de terceros

- Los responsables del negocio que cuenten con un servicio brindado por un tercero, con el apoyo del área de Seguridad de la Información, deben administrar los cambios a la provisión de servicios por parte de los terceros, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos, evaluar la necesidad de modificar o ampliar los acuerdos de prestación de servicios para cubrir las nuevas necesidades de seguridad si así se estima oportuno, y monitorear la aparición de nuevos riesgos.

TERMINO DE LA RELACIÓN CON UN TERCERO

- Al término de contrato con un tercero, se debe remover los accesos a la información y recursos de **LA EMPRESA** y garantizar que se devuelva o destruya (según aplique) la información y recursos de propiedad de **LA EMPRESA.**

VII. ANEXOS

- Metodología de gestión de riesgos y oportunidades del SGSI, de riesgos de seguridad de la información de procesos y proyectos

VIII. CONTROL DE CAMBIOS

IX. APROBACIÓN

	Nombre	Cargo	Fecha
1. Dueño	VERONICA VANESSA ORDOÑEZ	COORDINADOR DE GOBIERNO Y RIESGOS DE SEGURIDAD	07/03/2024
2. Editor	LIVIA JACKELYNE CORTEZ	ANALISTA SENIOR DE GOBIERNO Y RIESGOS DE SEGURIDAD	11/03/2024
2. Editor	ALESSANDRA PEREZ	ANALISTA DE GOBIERNO Y RIESGOS DE SEGURIDAD	11/03/2024
3. Revisor	ANGELLO GIURIA	ANALISTA DE PROCESOS	11/03/2024
3. Revisor	VERONICA VANESSA ORDOÑEZ	COORDINADOR DE GOBIERNO Y RIESGOS DE SEGURIDAD	12/03/2024
4. Aprobador	JUAN CARLOS MENDOZA	GERENTE DE SEGURIDAD DE LA INFORMACION	13/03/2024
4. Aprobador	MARIA FERNANDA GIAMBERINI	GERENTE DE TALENTO Y GESTIÓN ESTRATÉGICA	12/03/2024
4. Aprobador	PEDRO TRINIDAD LOZADA	GERENTE GENERAL	16/03/2024
4. Aprobador	RICARDO ROJAS	GERENTE DE SISTEMAS E INNOV. EN TECNOLOG	18/03/2024