I. OBJETIVO

Establecer los lineamientos para gestionar los riesgos de seguridad de la información en las relaciones con terceros (proveedores) de productos y servicios de **CENTRIA** (en adelante **LA EMPRESA**).

II. ALCANCE

El presente documento es aplicable a todo tercero (proveedor) de productos y servicios de **LA EMPRESA**.

III. REFERENCIAS

- Ley N°29733, Protección de datos personales, su reglamento y directivas asociadas.
- NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos.
- NTP-ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. 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.
- POL-SI-01-22 Política de Gobierno y Seguridad en la Nube.
- 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

- **Colaborador**

Personal que trabaja en la empresa en la modalidad de planilla.

- **Tercero**

También llamado **Proveedor**. Es cualquier persona, natural o jurídica, externa a **LA EMPRESA** que provee de productos o servicios bajo una relación contractual con **LA EMPRESA.**

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.
- Remediar oportunamente las brechas de seguridad de la información reportadas por **LA EMPRESA.**
- Brindar las facilidades a **LA EMPRESA** cuando ésta realice la gestión de riesgos de seguridad de la información de terceros.
- Reportar inmediatamente cualquier incidente de seguridad de la información al responsable de **LA EMPRESA** a su cargo o al correo seguinfo@centria.net.

VI. POLÍTICAS

1. Generalidades

- **LA EMPRESA** identifica y documenta un Inventario de Terceros que pueden afectar la confidencialidad, integridad y disponibilidad de la información.
- **LA EMPRESA** como parte de su programa anual de concientización en ciberseguridad, incluye material de concientización para el personal de **LA EMPRESA** que interactúa con **Terceros**.
- El **Área de Supply Chain** de **LA EMPRESA** establece los mecanismos de evaluación y selección de terceros, en donde se incluyen la evaluación del producto o servicio ofertado; y con apoyo del Área de Seguridad de la Información se establecen los requisitos de evaluación de los aspectos de seguridad de la información.
- El **área de Seguridad de la Información** de **LA EMPRESA** es responsable de ejecutar anualmente la gestión de riesgos de seguridad de la información sobre los terceros críticos, teniendo en cuenta lo siguiente:
  - El uso que hacen los terceros de la información corporativa y de los activos de información asociados.
  - Las vulnerabilidades de los productos o servicios que prestan a **LA EMPRESA**.

  Esta gestión de riesgos es realizada en base a **DOC-SI-01-30 Metodología de gestión de riesgos y oportunidades del SGSI, de riesgos de seguridad de la información de procesos y proyectos.**
- El Tercero deberá acceder a las instalaciones de LA EMPRESA, cumpliendo los lineamientos de POL-SI-01-15 Política de Seguridad en las Instalaciones.
- El Colaborador de LA EMPRESA a cargo del Tercero es responsable de:
  - Monitorear el cumplimiento de los requisitos contractuales y de seguridad de la información establecidos con el Tercero.
  - Informar inmediatamente a **Mesa de Servicios** cualquier incidente que comprometa la confidencialidad, integridad y disponibilidad de la información corporativa, mientras existan obligaciones contractuales entre **LA EMPRESA** y el Tercero.
  - Informar al Tercero que tiene a cargo sus responsabilidades en cuanto a la seguridad de la información y asegurarse que las cumpla.
  - Asegurar que el Tercero mitigue las brechas de seguridad de la información reportadas por el **Área de Seguridad de la Información** de **LA EMPRESA**.
  - Informar al Tercero que cualquier incidente de seguridad de la información debe ser reportado inmediatamente a su persona o al correo seguinfo@centria.net.
  - Ser la persona de contacto para atender los asuntos de seguridad de la información del Tercero que tiene a su cargo.

2. 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:

a. 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 el Tercero respecto a las obligaciones de ambas partes para cumplir con los requisitos relevantes de seguridad de la información y con los demás requisitos contractuales (por ejemplo: presentación de informes, envío de entregables, entre otros).

  Entre los requisitos de seguridad de la información, deben estar presente las condiciones para la autorización y revocación del acceso a la información corporativa y los activos asociados; debiendo el Colaborador responsable del Tercero mantener una lista de personal Tercero autorizado. Así también, la posibilidad de que **LA EMPRESA** pueda auditar los procesos y controles del tercero relacionados con el contrato; e incluir las obligaciones para la transferencia segura de la información y las obligaciones del Tercero una vez terminada la relación contractual.

  Estos requisitos deben ser cumplidos por el Tercero incluso por los subcontratistas de éste.

-
  - 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.
  - 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.
  - 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 los requisitos de seguridad de la información. En ese sentido, deberá definirse las indemnizaciones a **LA EMPRESA** por estos incumplimientos.
  - 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.

b. Cadena de suministro de tecnología de información y comunicación (TIC)

Además de los requisitos expuestos en el acápite anterior, deben considerarse adicionalmente los siguientes:

-

- Los acuerdos con **Terceros** deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los productos y servicios de tecnología de la información y comunicaciones, con el fin de asegurar que se brinden de manera adecuada y segura en toda la cadena de suministro.
- Los **Terceros** de productos TIC deben proporcionar a **LA EMPRESA** información sobre los componentes de software, las funciones de seguridad y las configuraciones requeridas para una operación segura de sus productos.
- Considerar la identificación y documentación de los componentes críticos del producto o servicio TIC para mantener la funcionalidad y seguridad.
- **LA EMPRESA** establece los requisitos de seguridad de la información para el uso seguro de servicios en la nube a través de **POL-SI-01-22 Política de Gobierno y Seguridad en la Nube.**

2. 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:

a. Monitoreo y revisión de servicios de los terceros

-
- El Colaborador responsable del **Tercero** debe monitorear el cumplimiento de los requisitos contractuales (lo que incluye los de seguridad de la información, niveles de servicio, entre otros), e informar al área de Seguridad de la Información de cualquier situación del tercero que afecte o pueda afectar la confidencialidad, integridad y disponibilidad de la información de **LA EMPRESA**.

Para monitorear el cumplimiento el Colaborador responsable del **Tercero** podrá revisar los informes de control de servicios, agendar reuniones de seguimientos, entre otros.

-
- El **área de Seguridad de la Información** es responsable de realizar la gestión de riesgos de seguridad de la información a Terceros críticos de **LA EMPRESA** de forma anual y cuando existen cambios significativos en la prestación del producto o servicio que impacten a la seguridad de la información.
- 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 eventos o incidentes de seguridad de la información que puedan afectar o afecten a **LA EMPRESA** (estén o no asociados al producto o servicio que ofrece) al Colaborador responsable a su cargo y/o a través del correo seguinfo@centria.net. En caso de que, la resolución del evento o incidente de seguridad de la información esté bajo su alcance deberá informar a **LA EMPRESA** las medidas de control tomadas, el impacto y cualquier otra información relevante.
- 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.

b. Gestión de cambios a los servicios de terceros

El Colaborador responsable del Tercero, con el apoyo del **Área de seguridad de la Información** de **LA EMPRESA**, debe gestionar los cambios en 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.

3. Término de la relación con un Tercero

- Al término de contrato con un **Tercero**, se debe remover los accesos a la información y activos de información asociados de **LA EMPRESA** y garantizar que se devuelva o destruya (según aplique) la información y recursos de propiedad de **LA EMPRESA**.
- El **Tercero** deberá mantener la confidencialidad de toda información de **LA EMPRESA** a la cual haya tenido acceso como parte de la relación contractual.

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

N° Versión	Fecha	Descripción del Cambio	Participantes
1	17/11/2022	No aplica, es primera versión	**Elaborado por:** JEFE DE GOBIERNO Y RIESGOS DE SEGURIDAD ANALISTA SENIOR DE GOBIERNO Y RIESGOS DE SEGURIDAD **Revisado por:** ANALISTA DE PROCESOS **Aprobado por:** GERENTE DE SEGURIDAD DE LA INFORMACION
2	17/11/2022	N/A.	**Elaborado por:** JEFE DE GOBIERNO Y RIESGOS DE SEGURIDAD **Revisado por:** ANALISTA DE PROCESOS **Aprobado por:** GERENTE DE SEGURIDAD DE LA INFORMACION

3	11/08/2023	Se actualizó el código de la entidad	**Elaborado por:** JEFE DE GOBIERNO Y RIESGOS DE SEGURIDAD ANALISTA SENIOR DE GOBIERNO Y RIESGOS DE SEGURIDAD ANALISTA SENIOR DE GOBIERNO Y RIESGOS DE SEGURIDAD **Revisado por:** JEFE DE PROCESOS Y RIESGOS **Aprobado por:** GERENTE GENERAL GERENTE DE GESTIÓN HUMANA AUDITOR GENERAL GERENTE DE SEGURIDAD DE LA INFORMACION GERENTE DE SISTEMAS E INNOV. EN TECNOLOG
4	11/03/2024	1. Se agregaron nuevas referencias normativas. 2. Se añadio el punto que hace referencia al análisis y evaluación de terceros basados en el documento "**DOC-SI-01-30 Metodología de gestión de riesgos y oportunidades del SGSI, de riesgos de seguridad de la información de procesos y proyectos."** 3. Se añadio el código de la política de seguridad en las instalaciones. 4. Se actualizo el nombre de la política.	**Elaborado por:** ANALISTA SENIOR DE GOBIERNO Y RIESGOS DE SEGURIDAD ANALISTA DE GOBIERNO Y RIESGOS DE SEGURIDAD AP **Revisado por:** JEFE DE GOBIERNO Y RIESGOS DE SEGURIDAD ANALISTA DE PROCESOS **Aprobado por:** GERENTE GENERAL GERENTE DE GESTIÓN HUMANA GERENTE DE SEGURIDAD DE LA INFORMACION GERENTE DE SISTEMAS E INNOV. EN TECNOLOG
5	25/11/2024	Se actualizó el objetivo y las referencias con las nuevas versiones de la ISO 27001 e ISO 27002 y se agregó la POL-SI-01-22 Política de Gobierno y Seguridad en la Nube. Se agregó el término “Colaborador” y se actualizó el término “Tercero”, y se actualizaron sus responsabilidades.	**Elaborado por:** ANALISTA SENIOR DE GOBIERNO Y RIESGOS DE SEGURIDAD ANALISTA DE GOBIERNO Y RIESGOS DE SEGURIDAD AP ANALISTA DE GOBIERNO Y RIESGOS DE SEGURIDAD

		En la sección “Políticas” se agregó el item#1 “Generalidades” y si hicieron actualizaciones en el item#2 “Previo a la relación con un Tercero”, y finalmente se agregó un nuevo lineamiento en el item#3 “Término de la relación con un Tercero”.	ANALISTA DE GOBIERNO Y RIESGOS DE SEGURIDAD **Revisado por:** ANALISTA DE PROCESOS **Aprobado por:** GERENTE GENERAL GERENTE DE SEGURIDAD DE LA INFORMACION GERENTE DE PROYECTOS DE TRANSFORMACIÓN DIGITAL Y MEJORA GERENTE DE GESTIÓN HUMANA

IX. APROBACIÓN

	Nombre	**Cargo**	**Fecha**
1. Dueño	VERONICA VANESSA ORDOÑEZ	JEFE DE GOBIERNO Y RIESGOS DE SEGURIDAD	18/09/2024
2. Editor	ALESSANDRA PEREZ	ANALISTA DE GOBIERNO Y RIESGOS DE SEGURIDAD AP	18/09/2024
2. Editor	CARLOS REYES	ANALISTA DE GOBIERNO Y RIESGOS DE SEGURIDAD	18/09/2024
2. Editor	RAUL ARAGON	ANALISTA DE GOBIERNO Y RIESGOS DE SEGURIDAD	18/09/2024
2. Editor	LIVIA JACKELYNE CORTEZ	ANALISTA SENIOR DE GOBIERNO Y RIESGOS DE SEGURIDAD	18/09/2024
3. Revisor	ANGELLO GIURIA	ANALISTA DE PROCESOS	22/09/2024
4. Aprobador	ELIZABETH KIYAN	GERENTE DE GESTIÓN HUMANA	25/09/2024
4. Aprobador	GINO HERRERA	GERENTE DE PROYECTOS DE TRANSFORMACIÓN DIGITAL Y MEJORA	27/09/2024
4. Aprobador	JUAN CARLOS MENDOZA	GERENTE DE SEGURIDAD DE LA INFORMACION	24/09/2024
4. Aprobador	PEDRO TRINIDAD LOZADA	GERENTE GENERAL	23/09/2024