POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA RELACIÓN CON PROVEEDORES

La seguridad de la información es esencial para la protección de los activos de la entidad y para asegurar la confianza de nuestros usuarios internos y externos. Las relaciones con los proveedores juegan un papel crucial en el ecosistema de seguridad de la información, ciberseguridad y protección de la privacidad, ya que estos pueden tener acceso a datos sensibles y sistemas críticos. Esta política establece las directrices necesarias para gestionar y mantener la seguridad de la información en todas las relaciones con los proveedores, alineándose con el control 5.19 de la GTC ISO 27002:2022.

1. OBJETIVO

Mantener un nivel acordado de seguridad de la información en las relaciones con los proveedores, asegurando que los datos y sistemas de la entidad estén protegidos contra amenazas y vulnerabilidades derivadas de las interacciones con estos terceros.

2. ALCANCE

Esta política se aplica a todos los empleados, contratistas y terceros del proceso de gestión de las TICS que interactúan con proveedores que tienen acceso a la información de la entidad o a sus sistemas. Abarca todas las fases del ciclo de vida de la relación con el proveedor, desde la selección y evaluación inicial hasta la terminación del contrato y la gestión de la salida.

3. RESPONSABLE

- Coordinador de TI
- Líder de infraestructura
- Líder de sistemas de información
- Profesional especializado en seguridad Informatica

4. DEFINICIONES

Acceso: Capacidad de ingresar, ver, modificar o utilizar sistemas, datos o recursos de la organización.

Acuerdo de nivel de servicio (SLA)(ANS): Service Level Agreement (SLA). Un acuerdo entre un proveedor de servicios de Tecnologías de la Información (TI) y un cliente que en este caso será la Oficina de Tecnología e Informática.

Auditoria: La auditoría se refiere a la evaluación sistemática, independiente y documentada para obtener evidencia objetiva y evaluarla de manera imparcial con el fin de determinar en qué medida se cumplen los criterios de auditoría. (ISO/IEC 27001:2022).

Capacidad: El máximo rendimiento que se puede obtener de un Ítem de configuración o Servicio de TI con el objetivo de cumplir los niveles de servicio acordados.

Ciberseguridad: La ciberseguridad se refiere a la protección de los sistemas y datos informáticos contra el acceso no autorizado, el uso malintencionado, la modificación, el robo o la destrucción. La ciberseguridad incluye medidas técnicas, físicas y administrativas para proteger la información. (ISO/IEC 27001:2022).

Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados. (mintic, s.f.)

Contratista: Persona o entidad que realiza trabajos o presta servicios bajo un contrato con la organización.

Datos Sensibles: Información que requiere protección adicional debido a su naturaleza confidencial, como datos personales, financieros o estratégicos.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera. (mintic, s.f.)

Incidente de seguridad de la información: Un incidente de seguridad en informática es la ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de la información y que violan la Política de Seguridad de la Información de la organización, en el caso de que disponga de ella.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Información: Datos relacionados que tienen significado para la entidad1. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada. (mintic, s.f.)

Proveedor: Persona o entidad que proporciona productos, servicios o soluciones a la organización.

Riesgos: Los riesgos se refieren a la posibilidad de que ocurra un evento que pueda tener un impacto negativo en un proyecto, una organización o una persona. Los riesgos pueden ser internos o externos, y pueden ser gestionados mediante la identificación, evaluación y mitigación. (ISO/IEC 27001:2022).

Seguridad de la Información: Protección de la información contra una amplia gama de amenazas para asegurar la continuidad del negocio, minimizar el riesgo y maximizar el retorno de las inversiones y las oportunidades de negocio.
Sistema de Información: Conjunto de aplicaciones, servicios, tecnología de información u otros componentes de manejo de información. (ISO/IEC 27001:2022).

Tercero: Cualquier entidad que no es parte directa de la organización, incluyendo proveedores, socios y subcontratistas.

Usuario: Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información. (mintic, s.f.)

Id.: Un Id. de usuario es un identificador único de cliente mediante el cual un anunciante elige identificar a un usuario que visita su sitio web. (Ayuda de Google Ads, s.f.)

TI.: El concepto de tecnología de la información refiere al uso de equipos de telecomunicaciones y computadoras (ordenadores) para la transmisión, el procesamiento y el almacenamiento de datos. (Pérez Porto, 2014).

5. DESARROLLO

A continuación se definen los lineamientos que la entidad debe identificar e implementar para abordar los riesgos de seguridad asociados con el uso de productos y servicios proporcionados por los proveedores. Esto también debe aplicarse al uso que hace la entidad de los recursos de los proveedores de servicios en la nube

a) Evaluación y Selección de Proveedores

- Realizar una evaluación de riesgos de seguridad de la información antes de seleccionar a un proveedor.
- Incluir criterios de seguridad de la información en el proceso de selección de proveedores.

b) Contratación y Acuerdos

- Establecer cláusulas contractuales que especifiquen las responsabilidades de seguridad de la información del proveedor.
- Asegurar que los contratos incluyan derechos de auditoría y supervisión de las prácticas de seguridad del proveedor.

c) Gestión de Acceso

- Limitar el acceso de los proveedores a la información y sistemas necesarios para cumplir con sus responsabilidades contractuales.
- Revisar y actualizar regularmente los permisos de acceso otorgados a los proveedores.

d) Monitoreo y Revisión

- Monitorear continuamente las actividades de los proveedores para detectar y responder a incidentes de seguridad.
- Realizar revisiones periódicas del cumplimiento de los proveedores con los requisitos de seguridad de la información establecidos.

e) Terminación de la Relación con el Proveedor

- Asegurar la revocación oportuna de los accesos del proveedor a los sistemas y datos de la entidad al finalizar la relación contractual.
- Recuperar todos los activos y datos de la entidad en posesión del proveedor de manera segura.

f) Concienciación y Capacitación

- Proporcionar capacitación y concienciación sobre seguridad de la información a todos los empleados, contratitas o terceros del proceso de gestión de las TICS que gestionan relaciones con proveedores.
- Asegurar que los proveedores también reciban la capacitación necesaria para cumplir con las expectativas de seguridad de la entidad.

g) Gestión de Incidentes

- Establecer procedimientos claros para la notificación y gestión de incidentes de seguridad relacionados con proveedores.
- Colaborar con los proveedores en la resolución de incidentes y la implementación de medidas correctivas.

5.1. REVISIONES Y ACTUALIZACIONES

Esta política será objeto de revisiones periódicas para asegurar su relevancia y eficacia. El Profesional especializado en seguridad Informatica coordinará estas revisiones, realizando ajustes según sea necesario para adaptarse a cambios en la infraestructura tecnológica, regulaciones y mejores prácticas de seguridad de la información.

6. REFERENCIAS

-, M. d.-M. (2022). *NTC ISO/IEC 27001:2022 Anexo A GTC ISO/IEC 27002:2022, CONTROLES ORGANIZACIONALES 5.19 SEGURIDAD DE LA INFORMACIÓN EN LA RELACIÓN CON PROVEEDORES*

7. CONTROL DE MODIFICACIONES

CONTROL DE MODIFICACIONES			
Versión	**Fecha**	**Descripción de la Modificación**	**Realizada por**
1	4-06-2024	Emisión inicial del documento	Profesional especializado en seguridad Informatica
2	04-02-2025	Cambio en la imagen institucional	Oficina de caldiad