
digilogics

Relación con proveedores (POL-10)

1. Objetivo

Establecer las directrices para garantizar la protección de los activos de la organización que sea accesible a los proveedores y/o terceros relacionados.

2. Alcance

Es de aplicación general a todos los colaboradores que requieran compartir o dar acceso a proveedores y/o terceros a información confidencial o restringida propiedad de DIGILOGICS.

3. Términos y Definiciones

- **Activo de información**: Se refiere a cualquier información o elemento (hardware, software, bases de datos, dispositivos de almacenamiento, edificios, personas, documentos, conocimiento, etc.) que tenga valor para la organización.
- **Información confidencial:** Es la que contiene datos que la organización está obligada a proteger. Información de la organización que por su importancia es imprescindible para el funcionamiento de la misma.
- **Información restringida:** Datos que, si son revelados a individuos no autorizados, podría tener algún impacto en las obligaciones legales o regulatorias de la organización**.**
- **Siniestro:** se refiere a las anomalías, destrucción fortuita o pérdida importante de cualquier activo de información perteneciente a DIGILOGICS.

4. Política

A.5.19 Seguridad de la información en las relaciones con los proveedores

- Se deberá identificar los tipos de proveedores que puedan tener impacto en la seguridad de la información. En el formato **Evaluación de proveedores** en el campo de comentarios dejará evidencia de esa identificación.
- Los proveedores que puedan acceder, procesar, almacenar, transmitir, o proveer componentes de infraestructura de tecnología para la información de la organización deberán:
    - Proporcionar siempre que se requiera, la relación de personas y funciones asociados al servicio que vayan a prestar e informará de cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades).
    - Aceptar que su personal sea acompañado por personal de DIGILOGICS y permanecer dentro de las instalaciones únicamente en el área designada y el tiempo necesario para la ejecución de su trabajo.
    - Asegurar que en caso de ocurrir algún incidente o siniestro con los activos (tecnológicos e información) se solucione el problema recobrando la operación normal de la organización.
    - Comprometerse a no incurrir o participar en ningún tipo de actividad sospechosa o dañina para las instalaciones, información y/o operación de la organización.

A.5.20 Gestión de la seguridad de la información en los acuerdos con los proveedores

- Todas las áreas o responsables que realicen contratos con proveedores y/o terceros deben validar e identificar si es necesario establecer acuerdos o convenios de confidencialidad relativos a la seguridad de la información.
- En dichos convenios o acuerdos se deberá especificar:
    - Qué información debe proporcionarse al proveedor y su medio de transmisión.
    - Establecer el uso que le darán a la información

- Establecer las obligaciones en materia de seguridad de la información.
- Acciones en caso de divulgación de información

A.5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC

- Se deberá realizar el análisis de riesgos para las adquisiciones o actualizaciones de sistemas y/o softwares empresariales desarrollados por terceros para validar el impacto en la operación y la seguridad de la organización.

- Para la adquisición de sistemas se deberá tomar en consideración los siguientes requisitos:

  - ✓ Sistemas empresariales
    - Contar con certificado Microsoft para PC
    - Contar con certificado Apple para Mac
    - Provenir de web o sitio oficial del fabricante
    - Contar con usuario registrado en el sitio
    - Comparación y análisis del producto

  - ✓ Software de propósito general (office, adobe, Windows, etc.)
    - Contar con certificado Microsoft para PC
    - Contar con certificado Apple para Mac
    - Provenir de web o sitio oficial del fabricante

  - ✓ Software desarrollado por terceros
    - Análisis de código
    - Revisar compatibilidad con frameworks
    - Pruebas de estrés
    - Garantizar la funcionalidad
    - Los entornos de desarrollo cuenten con control de cambios verificables mediante control de versiones y perfiles de distribución al momento de instalación.
    - Las versiones de software sean en su versión estable.

- Para la actualización de sistemas se deberá tomar en consideración los siguientes requisitos:

  - ✓ Esperar un periodo de 3 meses después de la liberación de la actualización para garantizar su estabilidad, en caso de ser una actualización crítica por parte del proveedor/fabricante se aplicará de inmediato.
  - ✓ La actualización debe provenir de forma legal.

A.5.22 Monitoreo, revisión y gestión de cambios de los servicios de los proveedores

Se deberá realizar una revisión de la entrega en el servicio del proveedor en donde se especifique si cumplió o no con los requisitos establecidos en el contrato tanto de calidad del servicio como de la seguridad e integridad de la información. De esto se dejará constancia en el formato **Tablero de evaluación de proveedores** o mediante la revisión de reportes de servicios realizados.

- En caso de modificaciones a los términos de contratación, estos deberán quedar establecidos en un adendum.

A.5.23 Seguridad de la información para el uso de servicios en la nube

- Si se requiere acceder a sitios web o servicios en la nube se deberán tomar en cuenta las siguientes medidas de seguridad:

  - El sitio debe contar con certificados SSL (https)
  - Validar que el filtro web no marque la página como maliciosa
  - No proporcionar datos confidenciales de la organización, ni personales en sitios no confiables.
  - La aplicación o servicio debe contar con declaración de prácticas de seguridad y privacidad.
  - Las claves de acceso de los usuarios deben apegarse a lo siguiente:
    - ✓ La contraseña debe tener al menos 8 caracteres.
    - ✓ La contraseña debe contener por lo mínimo una letra mayúscula y una minúscula, cifras y caracteres especiales. Por ejemplo: oNQZnz$Hx2.
    - ✓ Una contraseña segura no debe contener información personal que es fácil de averiguar.
  - Si el sitio o servicio lo permite se debe configurar la autenticación de 2 pasos en las cuentas.

- Cuando se trate de servicios de almacenamiento en la nube, adicional a lo antes expuesto se deberá tomar en cuenta:
  - Clasificar la información que manejamos y separar aquellos archivos con información confidencial o restringida y no alojarlos en la nube.
  - Poner atención cuando aceptamos las condiciones de uso de un determinado programa o aplicación, especialmente lo relativo a la protección de datos y el borrado cuando dejemos el servicio.

- Los equipos de cómputo desde donde se acceda a servicios a la nube deberán contar con antivirus.
- Se deben mantener los navegadores de los dispositivos actualizados.
- Si los servicios se van a usar desde un celular, esté debe estar protegido con una contraseña segura .
- Como medida adicional de seguridad se deberá contar con un respaldo de la información compartida en la nube.