Política de proveedores de Paradigma SAS

TABLA DE CONTENIDO

5.12 Relaciones con los Proveedores 2
5.13 Gestión de la seguridad de la información en la cadena de suministro TIC 4
5.14 Protección de los activos accesibles por terceras partes o proveedores 4
5.15 Seguimiento, revisión y gestión de cambios en servicios de proveedores 5

5.12 Relaciones con los Proveedores

Paradigma establece mecanismos de control en sus relaciones con terceras partes y proveedores con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos cumpla con las políticas, normas y procedimientos de seguridad de la información y Ciberseguridad, teniendo en cuenta los siguientes aspectos:

- Se deben definir los criterios adecuados que permiten seleccionar y evaluar los proveedores teniendo en cuenta la sensibilidad de la información, que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

- Se deben definir los requisitos de seguridad de la información y Ciberseguridad que deben cumplir los productos, servicios o aplicaciones que se adquieran a proveedores. Estos requisitos deben ser coherentes con las políticas de seguridad de la información de la organización y realizarse a través de proveedores reconocidos, además el dueño del proceso solicitante deberá definir estos requisitos en función del software a contratar o adquirir.

- Se deben evaluar y gestionar los riesgos de SI y Ciberseguridad, asociados con:

  - El uso por parte de los proveedores de la información de la organización y otros activos de información asociados.

  - El mal funcionamiento o las vulnerabilidades de los productos (incluidos los componentes y subcomponentes de software utilizados en estos productos)

  - La adecuada prestación de los servicios enmarcados en los acuerdos contractuales asumidos con el proveedor, la no prestación del servicio, la deficiencia en sus procesos que impida el adecuado servicio o incumplimiento parcial y total del contrato.

- Con el fin de establecer contratos y acuerdos rigurosos en materia de seguridad de la información y ciberseguridad, se deben detallar las cuestiones más relevantes que deben reflejarse en los contratos, acuerdos de confidencialidad y de acceso a datos, teniendo en cuenta las siguientes consideraciones:

  - Determinar qué información es accedida, cómo puede ser accedida la clasificación y protección de esta;

  - Asegurar que, una vez finalizado el contrato el proveedor ya no podrá acceder o mantener la información sensible de nuestra organización;

  - Reflejar los requisitos legales, reglamentarios y contractuales de acuerdo con la legislación vigente en materia de seguridad de la información y Ciberseguridad.

  - Normas de uso aceptable de la información y otros activos asociados.

  - Realización de auditorías periódicas a los servicios prestados por parte de los proveedores e incluidos los proveedores de la cadena de suministro.

  - Indemnizaciones y reparación por incumplimiento de los requisitos del contratista;

  - Requisitos y procedimientos de gestión de incidentes (especialmente notificación y colaboración durante la corrección de incidentes);

- Para los servicios críticos se les debe exigir a los proveedores plan de continuidad de negocio que garantice la prestación del servicio, en caso de Incidentes que afecten la operación.
- El proveedor debe notificar de manera anticipada a la organización, los cambios en los servicios contratados o cambios a nivel de las herramientas de gestión de sus servicios, los cuales deben ser aprobados por Paradigma.
- Se debe establecer y definir claramente por contrato las responsabilidades sobre el servicio contratado, estableciendo sanciones por incumplimiento, incluyendo las relacionadas a los aspectos relativos a seguridad de la información y Ciberseguridad.
- Con el fin de contar con métricas que permitan medir la eficacia de los servicios contratados y las garantías adquiridas, se deben definir y firmar Acuerdo de niveles de Servicios ANS (o SLA en inglés) con los proveedores.

5.13 Gestión de la seguridad de la información en la cadena de suministro TIC

En caso de que el proveedor subcontrate o tercerice servicios, estos proveedores deben cumplir las mismas clausulas o disposiciones pertinentes en cuanto a seguridad de la información y ciberseguridad, incluidos los controles que deberían aplicarse, tales como: el acuerdo sobre el uso de activos, acuerdo de confidencialidad, entre otros.

5.14 Protección de los activos accesibles por terceras partes o proveedores

Dentro de los contratos o acuerdos celebrados con terceras partes o proveedores que requieran acceder a la información de la compañía, se establece el cumplimiento de las políticas de seguridad, protección de activos, protección de datos, autorización de acceso, administración de cambios o aquellas consideradas relevantes para garantizar un adecuado aseguramiento de la información y los alcances frente a su tratamiento y divulgación.

Teniendo en cuenta el tipo de servicios que preste el proveedor, de ser requerido el acceso a las áreas consideradas como críticas o restringidas, este acceso debe hacerse aplicando los debidos controles de seguridad junto con la debida autorización de acceso, dado por el responsable del área o a quien delegue o la Gerencia.

El área de Infraestructura establece las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de las terceras partes o proveedores en la red de datos de la compañía, de igual manera establece las condiciones de comunicación segura, cifrado y transmisión de información requeridos con el proveedor y de gestionar los riesgos relacionados con terceras partes o proveedores que tengan acceso a los sistemas de información y la plataforma tecnológica de Paradigma.

Los proveedores clasificados de impacto crítico deben cumplir con los requisitos y buenas prácticas de seguridad de la información implementadas por Paradigma y estas sean extensivas a sus terceros que intervengan directamente en los servicios prestados a Paradigma.

5.15 Seguimiento, revisión y gestión de cambios en servicios de proveedores

Paradigma debe supervisar y monitorear los contratos con terceras partes y/o proveedores, a fin de asegurar el cumplimiento de los acuerdos de niveles de servicio, confidencialidad, intercambio de información, así como los requisitos de seguridad de la información y ciberseguridad por parte de dichos terceros y/o proveedores en la cadena de suministro. El monitoreo incluirá, entre otros, los siguientes aspectos:

- Mejoras en los servicios ofrecidos
- Implementación de nuevas tecnologías
- Adopción de nuevos productos o versiones actualizadas
- Cambios en la ubicación física de las instalaciones de servicio
- Cambios en los proveedores dentro de la cadena de suministro
- Gestión de eventos e incidentes de seguridad
- Gestión de vulnerabilidades

Paradigma debe asegurar la divulgación de las políticas, normas y procedimientos de seguridad de la información y ciberseguridad, con el objetivo de garantizar que los proveedores y terceras partes conozcan las responsabilidades de seguridad de la información frete a los servicios prestados.

Se debe asegurar que los cambios en el suministro de servicios por parte de los proveedores y terceras partes sean comunicados oportunamente y no afecten la operación y prestación del servicio, asegurando el cumplimiento de los niveles de servicio y seguridad establecidos, mediante una adecuada gestión de riesgos para estos escenarios.

Se debe asegurar que los proveedores y/o terceras partes una vez finalizada la relación contractual, devuelvan y eliminen de manera segura los activos de información que tengan bajo su custodia para la ejecución de sus actividades y se revoquen de manera oportuna los permisos que tenga de acceso a los sistemas de Paradigma.