Normativa de Seguridad para Proveedores y Contratistas

NOVIEMBRE. 2024

El propósito de esta normativa es establecer los requisitos mínimos de seguridad que deben cumplir los proveedores, contratistas, subcontratistas y terceros de las empresas del grupo Obremo para proteger la confidencialidad, integridad, disponibilidad y privacidad de los activos de información que gestionen o a los que accedan.

1. PRINCIPIOS GENERALES

SEGURIDAD COMPARTIDA

Los proveedores son responsables de garantizar la seguridad de los activos que gestionen o accedan en nombre de Obremo.

CUMPLIMIENTO LEGAL Y NORMATIVO

Todos los proveedores deberán cumplir con la normativa aplicable en materia de protección de datos y seguridad de la información, así como con las políticas internas de Obremo.

MEJORA CONTINUA

Los proveedores deben colaborar en la identificación y adopción de mejores prácticas de seguridad.

SEGURIDAD POR DISEÑO

Los servicios ofrecidos deben incorporar medidas de seguridad desde su planificación y durante todo su ciclo de vida.

COLABORACIÓN

Los proveedores deben participar activamente en la mejora continua de la seguridad, colaborando en auditorías, análisis de riesgos y planes de mitigación de incidentes.

2. REQUISITOS GENERALES PARA PROVEEDORES

2.1. GESTIÓN DE ACCESOS

- El acceso del proveedor a los sistemas, redes y datos deberá estar limitado al mínimo necesario para cumplir sus funciones.
- Se utilizarán mecanismos de autenticación segura, como contraseñas robustas y autenticación multifactor.
- Los accesos serán monitoreados, registrados y revocados al finalizar el contrato o cuando dejen de ser necesarios.

2.2. POLÍTICAS DE SEGURIDAD Y GOBERNANZA

Los proveedores deben contar con políticas de seguridad documentadas, aprobadas por la dirección y comunicadas a su personal. Estas políticas deben incluir:

- Gestión de contraseñas: Implementación de políticas que garanticen el uso de contraseñas robustas, almacenamiento seguro y renovación periódica.
- Seguridad en el acceso: Procedimientos para la gestión de accesos y autenticación multifactor.
- Gestión de datos: Directrices claras sobre el tratamiento de datos personales y sensibles, cumpliendo con el RGPD.

2.3. SEGURIDAD EN LAS REDES Y SISTEMAS

Los sistemas y redes utilizados para procesar información de Obremo deberán:

- Estar segmentados para separar los datos de otros clientes o actividades del proveedor.
- Contar con medidas de protección frente a amenazas como malware y accesos no autorizados.

- Ser monitoreados continuamente para detectar actividades sospechosas.
- Disponer de un firewall y configuraciones seguras para prevenir accesos externos no autorizados.
- Los proveedores deberán aplicar actualizaciones y parches de seguridad regularmente.

2.4. CUMPLIMIENTO DEL RGDP Y PROTECCIÓN DE DATOS

Los proveedores que gestionen datos personales deberán:

- Actuar como encargados del tratamiento conforme a lo establecido en el RGPD, firmando los correspondientes contratos de encargado con Obremo.
- Implementar medidas de seguridad técnicas y organizativas adecuadas para proteger los datos personales.
- Garantizar que todo su personal esté formado en la normativa de protección de datos y conozca sus obligaciones.
- Notificar cualquier violación de seguridad que afecte a datos personales en un plazo máximo de 24 horas.

2.5. PROTECCIÓN DE LA INFORMACIÓN

- Los proveedores deberán implementar medidas para proteger la información frente a pérdida, alteración, acceso no autorizado o divulgación indebida.
- La información sensible deberá ser cifrada tanto en tránsito como en reposo.
- No se permitirá el uso de dispositivos personales para gestionar información de Obremo sin autorización previa.

2.6. CONTINUIDAD DEL NEGOCIO

Los proveedores deberán disponer de:

- Un Plan de Recuperación ante Desastres (DRP) con pruebas periódicas de su efectividad.
- Garantías de que el Tiempo Objetivo de Recuperación (RTO) y el Punto Objetivo de Recuperación (RPO) se ajustan a los requisitos del Grupo Obremo.

2.7. GESTIÓN DE CAMBIOS

Cualquier cambio en los sistemas, procesos o servicios del proveedor que pueda afectar a Obremo deberá ser previamente comunicado y aprobado.

2.8. GESTIÓN DE INCIDENTES DE SEGURIDAD

- Notificación Obligatoria: Los proveedores deberán informar a Obremo de cualquier incidente de seguridad que afecte los sistemas, datos o servicios relacionados, en un plazo no superior a 24 horas desde su detección.

- Investigación y Mitigación: El proveedor deberá colaborar activamente en la investigación del incidente y en la implementación de medidas correctivas.

- Informe de Incidente: El proveedor deberá entregar un informe detallado que incluya:
  - Causa raíz del incidente.
  - Impacto sobre los activos de Obremo.
  - Acciones correctivas y preventivas adoptadas.