Requisitos de seguridad para proveedores

Lo mejor de las TIC con
un toque humano

Versión del documento

Versión	Fecha	Cambio
v.1.0	03/02/2023	Creación del documento

Control del Documento

	Nombre	Dpto.	Fecha
Creado por	Seguridad Corporativa	Seguridad Corporativa	24/11/2022
Revisado por	Calidad y Normativa	Servicios Corporativos	03/02/2023
Aceptado por	Calidad y Normativa	Servicios Corporativos	03/02/2023

Derechos de propiedad

ÍNDICE

1. OBJETO

El presente documento recoge los requerimientos de seguridad de la información, que AXIANS establece para la prestación de servicios, y es de carácter obligatorio para sus PROVEEDORES en el ámbito de los productos y servicios contratados.

El objetivo último de este documento es la protección de los intereses de AXIANS, de sus CLIENTES y de sus EMPLEADOS, en el ámbito de la seguridad de la información.

2. REQUERIMIENTOS DE SEGURIDAD

2.1. Introducción

Este documento se elabora tomando como marco de referencia la normativa ISO/IEC 27001, en su versión en vigor, para la protección de la información de AXIANS. En el mismo:

- Se describen las funciones y responsabilidades de las partes (AXIANS y PROVEEDOR).
- Por cada punto definido el PROVEEDOR confirma su capacidad de cumplir los requisitos establecidos en el ámbito del servicio contratado, debiendo comunicarlo si en algún caso suponen un coste adicional no incluido en la oferta económica presentada.
- Todos los requerimientos que se describen a continuación aplican únicamente al servicio contratado y no representan una obligatoriedad para cualquier otro ámbito del proveedor, excepto que así se establezca por las partes, en atención a la naturaleza del servicio prestado.

2.2. Seguridad de los Recursos Humanos y proveedores

El PROVEEDOR debe:

- Garantizar que todos sus colaboradores disponen de las competencias adecuadas para llevar a cabo el servicio contratado y conocen sus obligaciones en materia de seguridad de la información establecidas en este documento.
- Incluir cláusulas en materia de seguridad de la información en los contratos de todos los empleados y contratistas, si los hubiera, y evidenciar el cumplimiento de este requisito, si se le solicitara.
- Llevar a cabo acciones de formación y concienciación en materia de seguridad de la información. En concreto, debe disponer de un plan de formación y concienciación, con revisiones periódicas.
- Asegurar que sus empleados respeten las exigencias de confidencialidad exigidas en el contrato con AXIANS.
- En caso de que se requiera subcontratación, previa autorización de AXIANS, de alguna actividad del servicio, el PROVEEDOR es responsable de trasladar los requisitos de este documento al contratista y asegurar su cumplimiento.

2.3. Control de Accesos lógicos

El PROVEEDOR debe:

- Disponer de un procedimiento interno de control de acceso (incluyendo alta, baja y modificación de usuarios en sus sistemas informáticos) basado en los siguientes requisitos de seguridad de la información:
  - ✓ Principio de mínimo privilegio: limitar el acceso a los sistemas y aplicaciones en función del rol del colaborador y a su 'necesidad' de saber.
  - ✓ Inicio de sesión seguro (usuario/contraseña segura) para todos los sistemas que contengan información del servicio o proyecto.
  - ✓ Custodia de contraseñas de los sistemas y aplicaciones necesarios para el proyecto. Contraseñas únicas e intransferibles.
  - ✓ Tratamiento específico y diferenciado para usuarios con privilegios (administradores de sistemas, BBDD, etc.).

2.4. Seguridad física y del entorno

El PROVEEDOR debe:

- Proteger las instalaciones (oficinas, centros de procesamiento de datos (CPD), salas de comunicaciones, etc.), desde las que se prestan los servicios contratados, frente a amenazas y desastres físicos y ambientales, o con causas en la acción humana, garantizando el suministro eléctrico, cableado, etc.
- Proteger los dispositivos frente a accesos no autorizados, pérdida de datos o daños de la información.
- Tener control sobre las intervenciones (instalaciones y desinstalaciones de equipos, revisiones, etc.) en las zonas restringidas.
- Disponer de controles para la gestión del acceso físico, únicamente al personal autorizado.

2.5. Seguridad de los activos y las operaciones

El PROVEEDOR debe:

- Designar un Responsable de Seguridad de la Información o persona de contacto con quien AXIANS pueda contactar cuando sea necesario.

- Tener identificados e inventariados todos los activos dedicados al proyecto/servicio y asegurar el uso, mantenimiento y protección adecuados de los mismos.
- Documentar y mantener procedimientos operativos relacionados con el servicio prestado.
- Tener definidos procedimientos u operativas para la Gestión de Cambios que se han realizado en los sistemas, aplicaciones, etc.
- Llevar a cabo un procedimiento de Gestión de la Capacidad, haciendo seguimiento de la utilización de los recursos y anticipando futuras necesidades de capacidad que garanticen los niveles de servicio contratados.
- Desplegar medidas de control adecuadas y efectivas que eviten ataques, intrusiones y/o infecciones de código malicioso que puedan afectar a la disponibilidad, confidencialidad y/o integridad de la información de AXIANS.
- Realizar copias de seguridad de la información, del software y de las imágenes del sistema con la política de retención y archivado que garanticen los niveles de servicio contratados.
- Mantener un registro que permita trazar la actividad de los usuarios pudiendo detectar comportamientos anómalos, fallos y eventos que afecten a la seguridad de la información en los sistemas y aplicaciones dedicados al proyecto/servicio. En particular, disponer de un registro de actividad para usuarios privilegiados.
- Disponer y ejecutar un procedimiento de Gestión de Vulnerabilidades que aseguren el parcheo de los sistemas, minimizando la exposición de los sistemas a las vulnerabilidades altas y críticas reportadas por los fabricantes de software y sistemas. En caso de vulnerabilidades críticas, que puedan afectar a AXIANS, deben comunicarse lo antes posible, tras su detección.

2.6. Seguridad de las comunicaciones

El PROVEEDOR debe:

- Implementar mecanismos y protocolos de comunicación seguros en sus instalaciones, para la prestación del servicio.
- Establecer canales seguros (tunelización cifrada) entre las instalaciones del PROVEEDOR y AXIANS.
- Notificar a AXIANS cualquier tipo de comunicación de datos personales fuera del ámbito de la Unión Europea.

2.7. Adquisición, desarrollo y mantenimiento de sistemas y licencias de software

El PROVEEDOR debe:

- Todo el software y el equipamiento hardware suministrado o utilizado para la prestación del servicio propio del PROVEEDOR debe disponer de su correspondiente licencia de uso, adquirida a través de los canales autorizados.
- El software propio del PROVEEDOR, necesario para llevar a cabo el proyecto/servicio contratado, debe desarrollarse siguiendo los principios y metodologías de referencia de desarrollo seguro de software, incluyendo la separación de entornos (productivos y no productivos), la seguridad desde el diseño y por defecto, etc.
- Si el servicio contratado con el PROVEEDOR es el desarrollo de software, debe seguirse la metodología y los protocolos de desarrollo seguro internos definidos por AXIANS, basados en estándares reconocidos internacionalmente.
- Todo el software y el equipamiento hardware suministrado o utilizado para la prestación del servicio propio del PROVEEDOR debe disponer de un plan de mantenimiento preventivo y correctivo.

2.8. Protección de la información

El PROVEEDOR debe:

- Respetar las obligaciones de confidencialidad, integridad y disponibilidad de la información en el ámbito de la prestación del servicio.
- Limitar la difusión y el acceso a la información establecidos en el servicio, evitando el almacenamiento no imprescindible para la prestación del servicio.
- No utilizar, en ningún momento, la información para una finalidad distinta a la establecida en el objeto del contrato. Cualquier modificación con respecto al alcance inicial, relacionada con la información necesaria a la que se tiene acceso para la prestación del servicio, debe ser comunicado y autorizado por AXIANS.
- Adoptar mecanismos de cifrado que garanticen la confidencialidad de la información de AXIANS, con independencia del estado en el que se encuentre (en tránsito o en reposo) y en los dispositivos que se maneje.
- Devolver a AXIANS, y eliminar de sus sistemas / instalaciones, a la finalización del proyecto/servicio, o cuando AXIANS lo solicite, toda la información proporcionada,

generada o derivada de la prestación de los servicios, incluyendo las copias de la misma. Se podrá solicitar evidencia del borrado / destrucción de la información.

2.9. Gestión de incidentes de seguridad

El PROVEEDOR debe:

- Actuar de forma diligente en caso de que se materialice un incidente de seguridad, quedando obligado a:
  - ✓ Reportarlo a AXIANS en el plazo máximo de veinticuatro (24) horas naturales desde su conocimiento, a través de las personas de contacto establecidas entre las partes con copia a seguridadcorporativa@axians.es.
  - ✓ Mitigar cualquier impacto o daño que el incidente pudiera causarle a AXIANS.
  - ✓ Colaborar en todo momento con AXIANS durante la investigación del incidente y proporcionar cuanta información sea necesaria para su esclarecimiento.
  - ✓ Mantener informado al Responsable de Seguridad de la Información de AXIANS acerca del estado de la investigación, de las acciones emprendidas y del resultado de las mismas.
  - ✓ Entregar a AXIANS en el plazo de quince (15) días naturales un informe escrito sobre la gestión completa del incidente.
- Disponer de un procedimiento de notificación y gestión de incidentes de seguridad que incluya un registro, tipificación y detalle de los mismos.

2.10. Auditorías

Con el fin de verificar, en cualquier momento, el cumplimiento de los requerimientos de seguridad de la información, descritos en el presente documento, AXIANS podrá llevar a cabo los controles y auditorías que considere convenientes. A tal efecto, el proveedor autoriza a AXIANS a realizar las auditorías que se acuerden, sin que estas interfieran en la prestación normal del servicio.

AXIANS y sus auditores realizarán dichas auditorias de manera que causen los mínimos inconvenientes a las actividades operativas. El PROVEEDOR facilitará la realización de la auditoría, permitiendo el acceso a cuanta información y documentación sea necesaria.

En caso de que AXIANS solicite a un tercero la realización de dichas auditorías, serán compañías que cuenten con acreditada solvencia, garanticen la más estricta confidencialidad y no supongan un conflicto de intereses para el PROVEEDOR.