Requisitos de seguridad de la información para proveedores

ISRS

Requisitos de seguridad

Introducción

Los requisitos de seguridad de la Información de Ericsson para proveedores (los “Requisitos”) representan el nivel mínimo de requisitos de seguridad de la información que el Proveedor debe cumplir con respecto a todas las relaciones en que el Proveedor:

1. Procesa, almacena y/o tiene acceso a la Información de Ericsson.
2. Tiene acceso a la red/infraestructura de Ericsson.
3. Desarrolla o personaliza software para Ericsson.
4. Proporciona productos de hardware o software de TI junto con servicios de soporte y mantenimiento.

Los Requisitos no pretenden ser una lista exhaustiva de requisitos de seguridad de la información. Además de los Requisitos, cada oferta de Servicio puede exigir requisitos específicos que deben abordarse con los controles de seguridad de la información adecuados que se definirán con más detalle en el Acuerdo correspondiente.

Este documento se revisa periódicamente y se actualizará en cada momento.

Índice

1 Requisitos de seguridad de la información

El Proveedor debe evidenciar un enfoque sistemático hacia la gestión de la seguridad de la información mediante la adhesión a la última versión de la norma internacional ISO/IEC 27001 o, con supeditación a un acuerdo escrito, una norma equivalente.

1.1 Gestión de la seguridad de la información

a. La alta dirección del Proveedor debe establecer la dirección y demostrar compromiso con la seguridad de la información. Como mínimo, debe haber una política de seguridad de la información de alto nivel y un programa de apoyo que se aplique en toda la empresa.

b. La política de seguridad de la información a que se refiere el inciso a. anterior deberá ser aprobada por la dirección del Proveedor, publicada en el seno de la organización del Proveedor y comunicada al personal pertinente del Proveedor.

c. La política de seguridad de la información de los proveedores habrá de ser revisada por el Proveedor a intervalos planificados, pero no menos de una vez cada veinticuatro (24) meses, o si se producen cambios significativos, con el fin de garantizar que siga resultando apta, adecuada y eficaz.

d. Se deben designar una o más personas calificadas con la responsabilidad de mantener el programa de seguridad de la información.

e. El Proveedor realiza campañas periódicas de concientización sobre seguridad de la información para educar a los empleados sobre sus responsabilidades en la creación y el mantenimiento de un lugar de trabajo seguro.

f. El Proveedor debe mantener una segregación adecuada de funciones cuando sea pertinente.

1.2 Gestión de riesgos

El Proveedor debe tener un marco/proceso de gestión de riesgos que identifique y aborde los riesgos de seguridad de la información.

1.3 Seguridad de los recursos humanos

a. El Proveedor debe realizar Verificaciones de Antecedentes previas al empleo para todo su personal de acuerdo con las leyes aplicables. Se debe conservar evidencia de dichas verificaciones de antecedentes y proporcionarla a Ericsson (a solicitud de Ericsson).

b. Antes de obtener acceso a la Información de Ericsson, el personal del Proveedor debe estar supeditado a restricciones de confidencialidad según acuerdo escrito con el Proveedor (como un contrato de trabajo o un acuerdo de confidencialidad). Tal acuerdo prohibirá al personal del Proveedor revelar Información de Ericsson a terceros y no deberá ser menos restrictivo que los compromisos de confidencialidad del Proveedor hacia Ericsson previstos en el Acuerdo.

c. El personal del Proveedor con acceso a la infraestructura de red de Ericsson y/o a la Información de Ericsson deberá firmar el documento de Instrucciones de Confidencialidad y Acceso (NDI) de Ericsson.

d. El Proveedor debe contar con un proceso disciplinario para abordar las violaciones de seguridad de la información.

1.4 Gestión de activos

a. El Proveedor debe tratar la Información de Ericsson como Información Confidencial y protegerla adhiriéndose a los Requisitos descritos en este documento.

b. El Proveedor debe registrar y mantener un inventario de activos de tecnologías de la información que formen parte del Servicio.

c. El Proveedor se abstendrá de almacenar, imprimir, copiar, divulgar y tratar la Información de Ericsson para fines distintos del de cumplir las obligaciones que se le atribuyen en el Acuerdo.

d. El Proveedor deberá establecer procesos para la devolución de los activos de Ericsson para casos de resolución o cambio de empleo del personal del Proveedor.

e. El Proveedor debe establecer y mantener procedimientos para la eliminación segura de la Información de Ericsson de acuerdo con las Mejores Prácticas del Sector (incluidos soportes electrónicos antes de que esté disponible para su reutilización).

f. Al concluir o finalizar el Acuerdo, el Proveedor debe devolver o destruir de forma segura, de acuerdo con las Mejores Prácticas del Sector, todas las copias de la Información de Ericsson en su posesión, incluidas todas las copias de respaldo y de archivo, en cualquier formato electrónico o no electrónico. Si se lo solicita, el Proveedor deberá proporcionar confirmación por escrito o, cuando corresponda, certificación de destrucción a Ericsson.

1.5 Control de acceso

a. El acceso a los activos de Ericsson desde una red fuera del control de Ericsson por parte de personas u organismos que no sean parte de Ericsson solo está permitido a través de una solución de acceso remoto aprobada por Ericsson.

b. El acceso a la Información de Ericsson debe restringirse a individuos únicos y según la necesidad de conocerla.

c. Las cuentas compartidas están terminantemente prohibidas. Cada persona que acceda a la Información de Ericsson debe tener su propia cuenta única.

d. La autenticación multifactor (MFA) se debe implementar para todo acceso a sistemas y redes que contengan Información de Ericsson de acuerdo con las Mejores Prácticas del Sector.

e. El Proveedor debe implementar controles de selección y gestión de contraseñas de acuerdo con las Mejores Prácticas del Sector al acceder a la Información de Ericsson, tocantes, entre otros aspectos, a la complejidad de la contraseña, el máximo de intentos de inicio de sesión incorrectos permitidos y la duración de la caducidad de todas las contraseñas.

f. El Proveedor debe tener un proceso que requiera aprobación para agregar, cambiar o eliminar usuarios de sus redes y sistemas que procesan, transmiten o almacenan Información de Ericsson.

g. El Proveedor debe tener un proceso para revocar/actualizar el acceso en caso de terminación o cambio de empleo.

h. El Proveedor debe revisar los privilegios de acceso a los sistemas y redes que manejan Información de Ericsson, incluidos los privilegios de acceso administrativo. Las revisiones periódicas deberán realizarse al menos cada doce (12) meses y para usuarios privilegiados al menos cada tres (3) meses.

i. El Proveedor debe tener un proceso para administrar y gestionar cuentas privilegiadas.

j. Los registros deberán almacenarse de manera que permitan comprobar cuál ha sido el acceso, el cambio, la revelación o la eliminación de Información de Ericsson.

1.6 Criptografía

a. Los controles criptográficos deben implementarse de conformidad con todos los acuerdos, leyes y regulaciones pertinentes.

b. El Proveedor debe tener la capacidad de comunicarse de forma segura con Ericsson a través de correo electrónico cifrado, utilizando técnicas de cifrado conformes con las Mejores Prácticas del Sector.

c. La Información de Ericsson debe protegerse mediante técnicas de cifrado en tránsito y en reposo de acuerdo con las Mejores Prácticas del Sector.

d. Las claves criptográficas deben administrarse de forma centralizada con procesos establecidos para la generación, la renovación, el acceso, la distribución, el almacenamiento, el archivo, la revocación y la destrucción de claves de acuerdo con las Mejores Prácticas del Sector.

e. Los certificados raíz no deben utilizarse en un entorno operativo.

1.7 Seguridad física y ambiental

a. El Proveedor debe restringir el acceso físico a las instalaciones y los centros de datos donde se trate o almacene Información de Ericsson a aquellas personas concretas que deban conocerla.

b. Las Instalaciones de Tratamiento de Información donde se trate Información de Ericsson deben ser verificadas y el acceso debe ser controlado en todo momento (24 horas al día, 7 días a la semana).

c. El Proveedor deberá proteger las Instalaciones de Tratamiento de Información donde se trate Información de Ericsson contra amenazas y peligros externos y ambientales.

d. Se debe implementar una política de escritorio despejado y pantalla en blanco para proteger la Información de Ericsson y sus activos.

e. El acceso físico a las ubicaciones donde se prestan Servicios para Ericsson debe estar restringido, mediante el uso de tarjetas individuales de proximidad/deslizante u otro sistema equivalente.

f. El acceso físico a las ubicaciones donde se prestan Servicios para Ericsson debe registrar continuamente eventos relacionados con el acceso físico, como fecha, hora, identificación de tarjeta de proximidad/deslizante, identificación de puerta, acceso denegado o acceso concedido.

1.8 Seguridad de operaciones

a. Los sistemas del Proveedor deben estar provistos de capacidad suficiente para garantizar la disponibilidad continua en caso de un incidente de seguridad o un aumento de la demanda.

b. El Proveedor debe garantizar que se implemente en sus sistemas protección contra software malicioso y que se mantenga actualizada, de acuerdo con las Mejores Prácticas del Sector.

c. Deberán registrarse todas las acciones de usuarios privilegiados. Debe ser detectable cualquier cambio en estos registros, ya sea por parte de un sistema, un usuario privilegiado o un usuario final. Los registros de actividad también deben revisarse de forma independiente periódicamente.

d. La información sobre eventos importantes relacionados con la seguridad debe hacerse constar en registros, incluidos tipos de eventos, como inicios de sesión fallidos, fallos del sistema y cambios en los derechos de acceso, y atributos del evento, como la fecha, la hora, la ID de usuario, el nombre del archivo, el tipo de actividad del usuario y la dirección IP.

e. Los registros de actividad deben almacenarse cifrados durante al menos seis (6) meses y deben estar disponibles para Ericsson previa solicitud de esta.

f. Se deben realizar y mantener copias de seguridad para garantizar la continuidad y las expectativas de entrega según el Acuerdo.

g. Debe existir un proceso de gestión de vulnerabilidades para priorizar y remediar las vulnerabilidades en función de su naturaleza y gravedad.

h. Debe existir un proceso de gestión de parches para garantizar que los parches se apliquen de manera oportuna.

i. El Proveedor debe realizar pruebas de penetración de los sistemas y las infraestructuras que se utilizan para respaldar la implicación de Ericsson al menos una vez al año, utilizando las Mejores Prácticas del Sector.

j. El Proveedor debe sincronizar los relojes de todos los sistemas de tratamiento de la información relevantes con una Fuente de Tiempo de Referencia Única.

k. El endurecimiento siguiendo las Mejores Prácticas del Sector se deben aplicar a todos los sistemas para reducir la superficie de ataque.

l. El Proveedor deberá implementar políticas diseñadas para evitar el almacenamiento de Información de Ericsson en dispositivos portátiles sin autorización previa por escrito de Ericsson.

m. El Proveedor debe garantizar que la Información de Ericsson y las aplicaciones o los sistemas de Ericsson estén separados de los sistemas y los datos propios del Proveedor o de otros clientes por medios físicos, técnicos y/o lógicos adecuados.

n. Los entornos de desarrollo, prueba y producción que contengan Información de Ericsson deben estar separados lógica y físicamente entre sí.

o. El Proveedor no utilizará la Información de Ericsson en ningún tipo de inteligencia artificial a menos que se pacte expresamente otra cosa en el Acuerdo.

1.9 Seguridad de las comunicaciones

a. Los sistemas que contienen Información de Ericsson deben reforzarse de acuerdo con las Mejores Prácticas del Sector, lo que incluye, entre otras cosas, eliminar o deshabilitar el software y las funcionalidades que no se estén utilizando.

b. El Proveedor debe implementar un enfoque de seguridad en capas, utilizando firewalls reforzados, sistemas de detección/prevención de intrusiones, segmentación de red y otras medidas relevantes de acuerdo con las Mejores Prácticas del Sector con el fin de proteger la Información de Ericsson.

c. El Proveedor debe implementar una solución de seguridad de correo electrónico de acuerdo con las Mejores Prácticas del Sector con el fin de protegerse contra ataques maliciosos como malware, suplantación de correo electrónico, ataques de phishing y spam.

1.10 Relaciones con subcontratistas

a. La divulgación de Información de Ericsson a un subcontratista solo se puede permitir con el consentimiento previo por escrito de Ericsson y únicamente con el fin de cumplir con las obligaciones del Proveedor según el Acuerdo.

b. El subcontratista debe estar restringido únicamente al acceso, uso, retención y divulgación de la Información de Ericsson necesarios para cumplir con las obligaciones contractuales.

c. El Proveedor es responsable de transmitir las mismas obligaciones aquí descritas mediante acuerdo escrito a sus subcontratistas.

d. El Proveedor debe evaluar el riesgo asociado con los nuevos subcontratistas antes de su integración y debe contar con un proceso de gestión de riesgos de terceros.

e. El Proveedor debe supervisar, revisar y auditar periódicamente el cumplimiento de los Requisitos por parte de los subcontratistas.

1.11 Gestión de incidentes

a. El Proveedor debe tener un proceso de gestión de incidentes de seguridad documentado para detectar y manejar incidentes.

b. El Proveedor deberá notificar a Ericsson cualquier incidente que afecte a la Información de Ericsson, en cuanto tenga conocimiento de él. Tal notificación deberá efectuarse en ningún caso transcurridas más de veinticuatro (24) horas o según se acuerde de otro modo, tras tener conocimiento de cualquier incidente real o que se sospeche. La notificación deberá cursarse:

   i. al contacto de Ericsson establecido en el Acuerdo; y a

   ii. gs.sim.dispatch@ericsson.com

c. Todos los informes de incidentes relacionados con la seguridad se tratarán como información confidencial y se cifrarán mediante métodos de cifrado conformes con las Mejores Prácticas del Sector.

d. El Proveedor debe cooperar plenamente con Ericsson en el manejo de estos informes. Tal cooperación puede implicar brindar acceso a datos probatorios informatizados para realizar exámenes forenses.

e. El Proveedor deberá cooperar con Ericsson para garantizar que se implementen medidas y procedimientos de seguridad apropiados y mutuamente aceptables como parte de las acciones de remediación contra un incidente o debilidad de seguridad que afecte los Servicios o involucre Información de Ericsson.

1.12 Gestión de la continuidad del negocio

a. El Proveedor debe implementar planes de continuidad del negocio y recuperación ante desastres que se documenten y prueben al menos una vez al año y, previa solicitud de Ericsson, proporcionar copias.

b. El Proveedor debe garantizar que los requisitos de seguridad de la información y preparación de las TIC estén integrados en los planes de continuidad del negocio y recuperación ante desastres.

c. A solicitud de Ericsson, el Proveedor debe contribuir a las actividades mutuas de continuidad del negocio y de recuperación ante desastres según lo designado por Ericsson.

1.13 Adquisición, desarrollo y mantenimiento de sistemas

Los siguientes requisitos de seguridad de la información son aplicables a los proveedores que brindan servicios de desarrollo o personalización de software o hardware, incluido el procesamiento de Información de Ericsson.

a. El Proveedor debe tener una metodología de ciclo de vida de desarrollo de software (SDLC) documentada.

b. El código fuente/objeto del sistema debe estar protegido contra el acceso no autorizado. Los privilegios de acceso al repositorio de código fuente deben revisarse periódicamente y limitarse a los empleados autorizados.

c. La Información de Ericsson de un sistema de producción no se utilizará en sistemas de prueba y desarrollo.

d. El Proveedor debe garantizar que el software y/u otros productos que procesen Información de Ericsson estén libres de toda vulnerabilidad de seguridad conocidas u otros defectos de seguridad.

e. Previa solicitud de Ericsson, el Proveedor comunicará cualquier software/complemento de terceros (propio o de código abierto) utilizado en el desarrollo del software que respalda el tratamiento de la Información de Ericsson.

f. El Proveedor debe seguir procedimientos documentados de gestión de cambios para solicitar, probar y aprobar cambios relacionados con la aplicación y la infraestructura.

1.14 Seguridad de la cadena de suministro de software

El Proveedor debe especificar y documentar los componentes de software de terceros utilizados y sus respectivos números de versión, tanto los componentes de código abierto como los propios, y proporcionar a Ericsson una factura de materiales de software (SBOM) que cumpla la especificación SPDX V2.2.1/ISO 5962:2021 y la especificación SBOM para proveedores (consulte *Condiciones y directrices - Proveedores y socios - Ericsson)* con respecto a todo el software (proporcionado de forma independiente o integrado en hardware) entregado o puesto a disposición de Ericsson.

2 Cumplimiento

a. Las auditorías internas del Proveedor y/o las evaluaciones relacionadas con la seguridad de la información deben ser realizadas periódicamente por personal capacitado del Proveedor o por un tercero designado por el Proveedor, y cualquier hallazgo debe corregirse rápidamente.

b. A solicitud de Ericsson, el Proveedor deberá dentro de diez (10) días poder demostrar el cumplimiento de los Requisitos y cualquier otro requisito de seguridad de la información acordado con Ericsson. Cualquier incumplimiento identificado deberá corregirse inmediatamente sin coste adicional para Ericsson.

c. El Proveedor deberá, previa solicitud de Ericsson, proporcionar a Ericsson evidencias sobre el cumplimiento de estos Requisitos por parte del subcontratista.

d. Previa solicitud de Ericsson, el Proveedor deberá proporcionar a Ericsson todos y cada uno de los resultados de las pruebas de penetración y/o vulnerabilidad o permitir que Ericsson realice pruebas de penetración y/o vulnerabilidad en sistemas o entornos administrados o alojados por el Proveedor en que se tramite o almacene Información de Ericsson.

e. El Proveedor debe conservar y proteger todos los registros necesarios para demostrar el cumplimiento de los Requisitos.

3 Definiciones

Para los efectos de este documento, las siguientes palabras y expresiones deberán tener el significado que se les asigna a continuación, a menos que el contexto requiera obviamente lo contrario.

Acuerdo	El acuerdo entre el Proveedor y Ericsson, en virtud del cual Ericsson comprará, adquirirá licencias o arrendará productos (incluidos software y otros productos protegidos por derechos de propiedad intelectual), servicios y demás productos del Proveedor, a los que se aplican estos Requisitos.
Verificaciones de Antecedentes	"Verificaciones de Antecedentes" tendrá el mismo significado que el establecido en la norma ISO/IEC 27001/27002.
Información de Ericsson	Información propiedad de Ericsson, los clientes de Ericsson y otros terceros que tienen relaciones comerciales con Ericsson, y demás información que forma parte del Servicio. La Información de Ericsson incluye Información Personal.
Mejores Prácticas del Sector	Se refiere al grado de habilidad, cuidado, previsión y práctica operativa que razonablemente y de forma ordinaria se esperaría de un proveedor de servicios cualificado y competente que participe en el mismo tipo de empresa que la del receptor o cualquier contratista (según corresponda) que se encuentre en las mismas circunstancias o circunstancias similares.
Instalaciones de Tratamiento de Información	Cualquier ubicación física que albergue sistemas que procesen o almacenen Información de Ericsson.
Información Personal	"Información Personal" se refiere a cualquier información que pueda relacionarse con una persona física identificada o identificable ("interesado") o según defina este término de otro modo la ley, la reglamentación o un acuerdo contractual. Se considerará persona identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de su identidad física, fisiológica, psíquica, económica, cultural o social.
Servicio	Cualquier servicio, producto u otro entregable proporcionado por el Proveedor a Ericsson según el Acuerdo.

Fuente de Tiempo de Referencia Única	Fuente de servidor de tiempo que está directamente vinculada a una fuente confiable de UTC (Tiempo Universal Coordinado), que es el principal estándar de tiempo utilizado globalmente para regular los relojes y el tiempo, es decir, Stratum1.
Proveedor	La empresa que ha celebrado el Acuerdo con Ericsson y proporcionará los Servicios. Cuando el término “Proveedor” impone una obligación o requisito al Proveedor según este documento, el término también habrá de incluir a las filiales, los subcontratistas y el Personal del Proveedor.