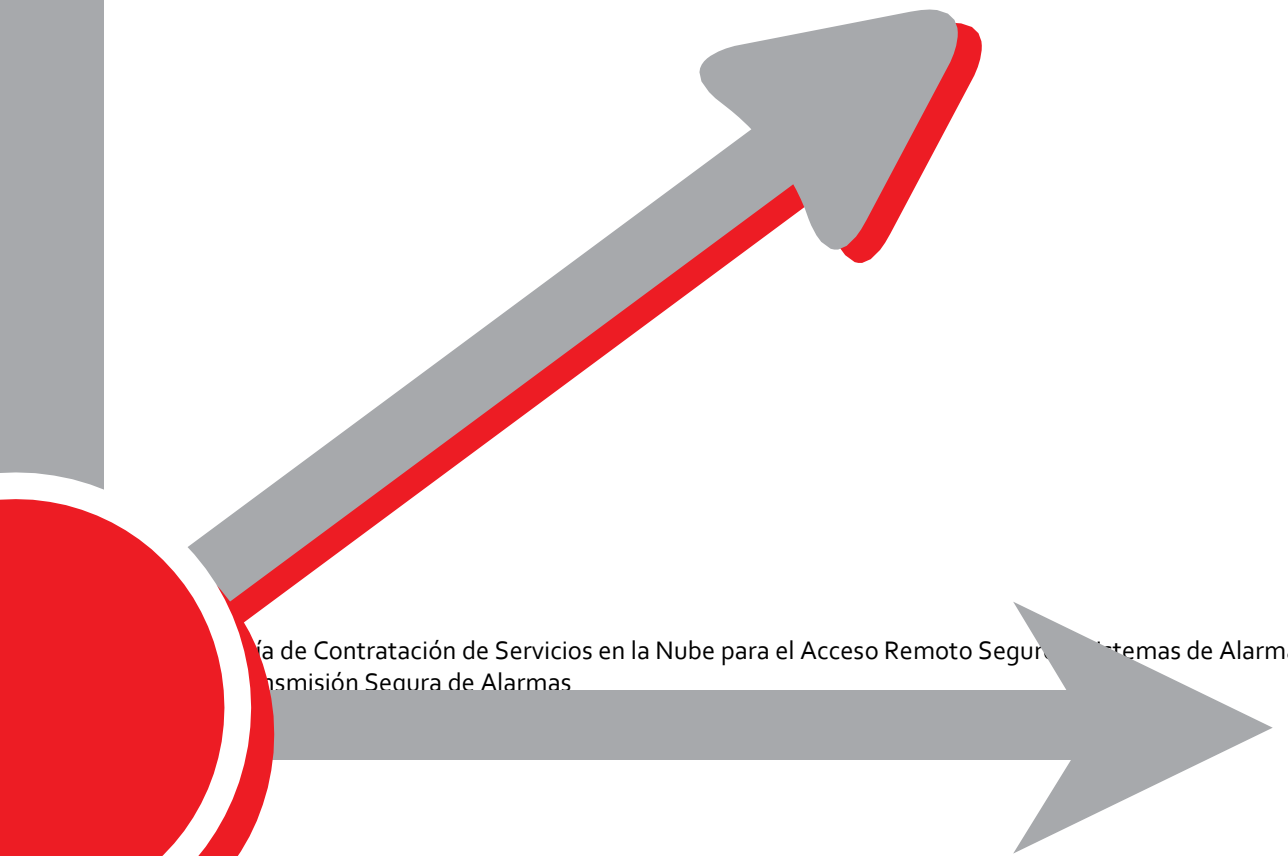
Guía de Contratación de Servicios en la Nube para el Acceso Remoto Seguro a Sistemas de Alarma y para la Transmisión Segura de Alarmas



Registro de versions

Fecha	Rev #	Párrafo / Página	Cambio
Febrero 2025	1.0		First release

INTRODUCCIÓN

Este documento está destinado a servir como una guía general y no sustituye el asesoramiento detallado en circunstancias específicas. Aunque se ha tenido mucho cuidado en la recopilación y preparación de esta publicación para garantizar su exactitud, Euralarm no puede aceptar, bajo ninguna circunstancia, responsabilidad por errores, omisiones o consejos dados, ni por cualquier pérdida derivada de la confianza en la información contenida en esta publicación..

DISCLAIMER

Este documento está destinado únicamente a servir de orientación a los miembros de Euralarm Si bien se ha hecho todo lo posible para garantizar su exactitud, los lectores no deben confiar en su integridad o corrección, ni confiar en él como interpretación legal. Euralarm no será responsable de la provisión de cualquier información incorrecta o incompleta.

Nota: la versión en inglés de este documento es la aprobada como documento de referencia.

Euralarm • Gubelstrasse 11 • CH-6300 Zug • Switzerland

E: secretariat@euralarm.org
W: www.euralarm.org

Índice

1. Introducción

Cada vez es más habitual utilizar la última tecnología para proporcionar transmisión de alarmas basada en IP y acceso remoto a sistemas de seguridad contra incendios y/o sistemas de seguridad (FSSS) y, como tal, ubicar parte del equipo fuera de las instalaciones del proveedor de servicios FSSS. Este documento ayudará a los proveedores de servicios FSSS (por ejemplo, instaladores) cuando utilicen los servicios de un centro de datos para alojar parte de los equipos.

Aquí se analizan dos casos de uso diferentes con sus requisitos específicos y público objetivo.

- Un caso de uso es la transmisión de alarmas a través de un sistema de transmisión de alarmas (ATS) operado y gestionado por un proveedor de servicios de transmisión de alarmas (ATSP) para el cual la disponibilidad, el tiempo de transmisión, el informe de fallos y la protección contra la sustitución son factores clave. La norma para sistemas de transmisión de alarmas (ATS) EN 50136-1 permite configuraciones alojadas en las que el elemento de la nube debe estar en una ubicación segura, que puede ser un centro de datos. Las categorías más altas de ATS incluyen requisitos de seguridad que deben cumplirse en todo el sistema. La guía para este caso de uso está dirigida a cualquier entidad que asuma el papel de ATSP.
- Otro caso de uso es el acceso remoto al FSSS a través de una infraestructura de acceso remoto (RAI) operada y gestionada por un proveedor de servicios de infraestructura de acceso remoto (RAISP) para el cual el acceso seguro al FSSS y a los datos son características clave, mientras que la disponibilidad es solo por conveniencia. La especificación técnica para la infraestructura de acceso remoto (RAI) CLC/TS 50136-10 requiere que el servidor de acceso remoto (RAS) esté en una ubicación segura e incluye requisitos para la seguridad de los datos transferidos. La guía para este caso de uso está dirigida a cualquier entidad que asuma el papel de RAISP, más específicamente a los pequeños y medianos proveedores de servicios FSSS que tengan la intención de asumir el papel de RAISP y no estén familiarizados con los servicios en la nube y deseen prestar servicios remotos de acuerdo con la norma EN 50710.

Aunque hay varias buenas razones para considerar las soluciones en la nube, los proveedores de servicios de FSSS deben comprender el impacto en su negocio, incluyendo la disponibilidad, los contratos de nivel de servicio, la seguridad de los datos, el cumplimiento y los requisitos legales y contractuales. Los proveedores de servicios de FSSS seguirán teniendo que demostrar el cumplimiento de las normas existentes, por ejemplo, en cuanto a rendimiento y disponibilidad, copias de seguridad, control de acceso, etc. Las responsabilidades de mantenimiento deben ser claramente entendidas y aceptadas por todas las partes interesadas. Estas incluirán la gestión del ciclo de vida de los sistemas operativos, las plataformas (por ejemplo, bases de datos, virtualización, etc.) y las aplicaciones. El proveedor de servicios de FSSS debe poder confirmar que estas actividades se han llevado a cabo de acuerdo con las expectativas y los contratos de servicio de los proveedores de servicios de FSSS.

El almacenamiento, la compartición y la seguridad de los datos son de vital importancia y requerirán una consideración legal más allá de lo que establece este documento, por lo que este documento no pretende interpretar esos requisitos legales ni proporcionar orientación al respecto.

Se han extraído secciones significativas de la presente guía de orientación de la BSIA « ARC considerations when utilising data centre or cloud services », con la debida aceptación de la BSIA. EURALARM agradece a su miembro, la Asociación Británica del Sector de la Seguridad, esta contribución.

Esta guía proporciona una descripción de conceptos importantes relacionados con los servicios en la nube,

considera las normas pertinentes y ofrece una visión general de los criterios legales para la elección del CSP. Sin embargo, la guía no pretende abordar todos los requisitos legislativos de los distintos países de Europa. Debe tenerse cuidado al considerar la guía en el contexto de cualquier requisito legislativo local que tenga prioridad.

2. Abreviaturas

AICPA:	2307
AMS:	Alarm Management System, Sistema Gestor de Alarmas
ANSI:	American National Standards Institute, Instituto Nacional Americano de Normalización
ARC:	Alarm Receiving Centre, Centro de recepción de alarmas
AS:	Alarm System, Sistema de alarma
ATS:	Alarm Transmission System, Sistema de transmisión de alarmas
BSIA:	British Security Industry Association, Asociación Británica de la Industria de la Seguridad
CLC:	CENELEC
CSP:	Cloud Service Provider, Proveedor de servicios en la nube
EN:	European Standard (Norm), Norma europea
FaaS:	Function as a Service, Función como servicio
FSSS:	Fire Safety Systems and/or Security Systems, Sistemas de seguridad contra incendios y/o sistemas de seguridad
IaaS:	Infrastructure as a Service, Infraestructura como servicio
IEC:	International Electrotechnical Committee, Comité Electrotécnico Internacional
ISO:	International Standardisation Organisation, Organización Internacional de Normalización
IT:	Information Technology, Tecnología de la información
MARC:	Monitoring and Alarm Receiving Centre, Centro de monitorización y recepción de alarmas
PaaS:	Platform as a Service, Plataforma como servicio
PSTN:	Public Switched Telephone Network, Red telefónica pública conmutada
RAC:	Remote Access Client, Cliente de acceso remoto
RAE:	Remote Access Endpoint, Punto final de acceso remoto
RAI:	Remote Access Infrastructure, Infraestructura de acceso remoto
RAISP:	Remote Access Infrastructure Service Provider, Proveedor del Servicio de Infraestructura para Acceso Remoto
RAS:	Remote Access Server , Servidor de acceso remoto
RCT:	Receiving Centre Transceiver, Transceptor del centro receptor
RCT-A:	RCT at the ARC, RCT en el ARC
RCT-H:	Hosted RCT, RCT alojado
SaaS:	Software as a Service, Software como servicio
SLA:	Service Level Agreement, Contrato de nivel de servicio
SOC:	System and Organization Controls, Controles del sistema y la organización
SPT:	Supervised Premises Transceiver, Transceptor en instalaciones supervisadas
TIA:	Telecommunications Industry Association, Asociación de la Industria de las Telecomunicaciones
TS:	Technical Specification, Especificación técnica

3. Asunto

Este documento aborda el elemento en la nube de una infraestructura de acceso remoto (RAI, por sus siglas en inglé), utilizada para acceder de forma remota a las funcionalidades del FSSS) y de un sistema de transmisión de alarmas (ATS, por sus siglas en inglés, utilizado para transmitir alarmas desde el FSSS al centro receptor de alarmas).

3.1. Acceso remoto al FSSS

En el caso de un RAI, este elemento de la nube se identifica como el RAS en la Figura 1.

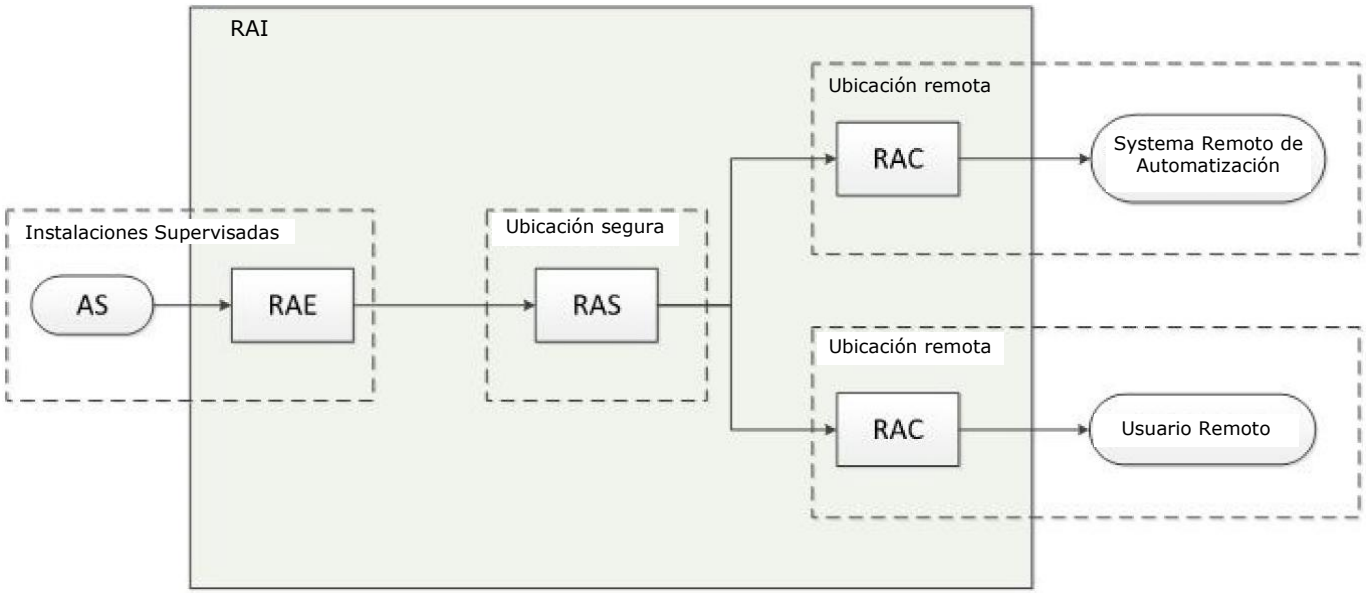


Figura 1. Diagrama lógico de la infraestructura de acceso remoto (extraído de CLC/TS 50136-10:2022)

3.2. Transmisión de Alarmas

En el caso de un ATS, la norma europea permite una configuración no alojada, como se muestra en la Figura 2a. En esta configuración, se establece un enlace directo entre el sistema de alarma (AS) y el ARC (MARC). La norma también permite una configuración alojada, representada en la Figura 2b. En esta configuración, los mensajes de alarma de numerosos sistemas de alarma convergen en un receptor alojado en un centro de datos e identificado como RCT-H, donde se procesan, reconocen y almacenan, y la CRA obtiene acceso a ellos a través de una vía de comunicación segura. Las consideraciones para abordar los cambios de las comunicaciones PSTN a la transmisión de alarmas IP se han dado en un libro blanco de Euralarm en 2019: "Redes de Nueva Generación para Comunicaciones de Alarma"[1]. El proveedor de servicios FSSS debe asegurarse de que el ATS cumple con la norma EN 50136-1, el SPT cumple con la norma EN 50136-2 y el RCT, RCT-H y RCT-A cumplen con la norma EN 50136-3 (ver A2.2 en el Anexo 2 para obtener una explicación de esas normas). Esto garantizará que todo el ATS envíe los mensajes de alarma a tiempo y que se controle si hay fallos en el envío de las alarmas.

[1] https://www.euralarm.org/resource-report/white-paper-new-generation-networks-for-alarm-communications.html

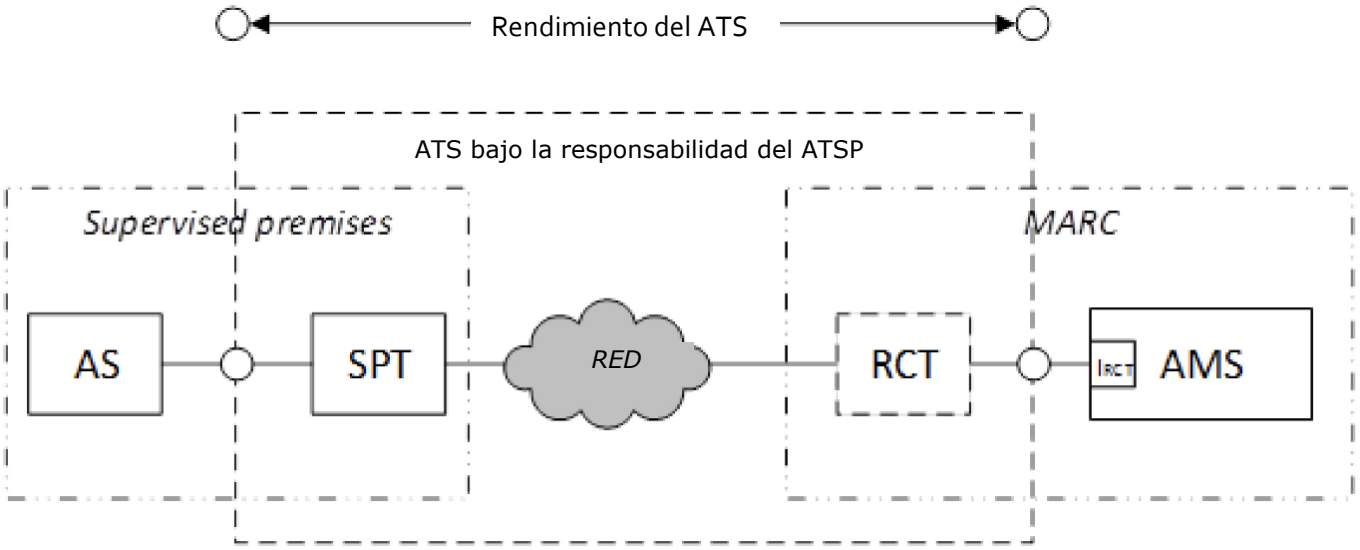


Figura 2a. Ejemplo de un sistema sistema de transmisión de alarmas **no alojado** (extraído de EN 50136-1/A1:2018)

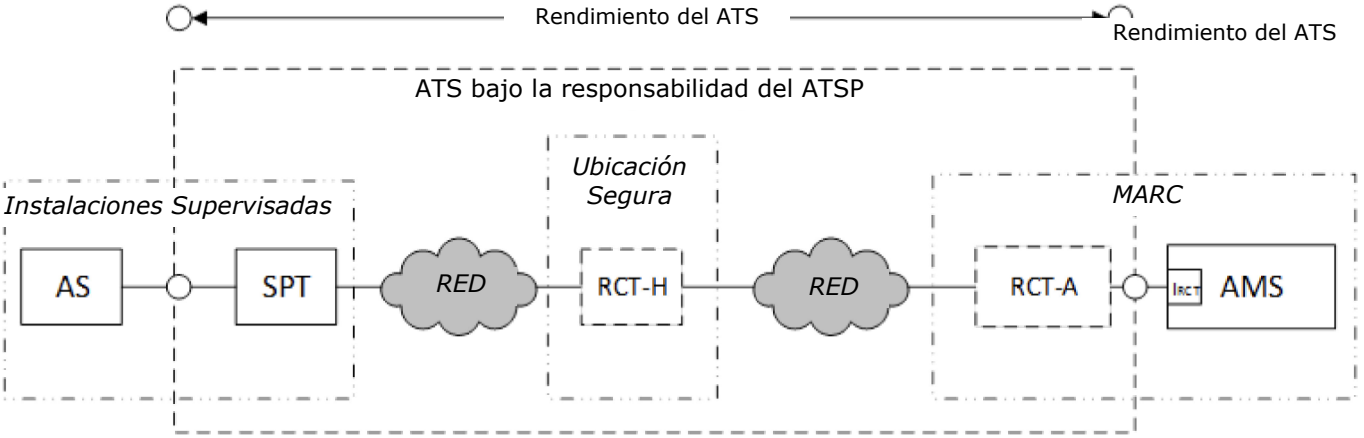


Figura 2b. Ejemplo de un sistema de transmisión de alarmas **alojado** (extraído de EN 50136-1/A1:2018)

3.3. General

El presente documento describe las consideraciones del proveedor de servicios FSSS a la hora de elegir utilizar los servicios de un centro de datos o servicios en la nube. Esto debería ayudar a decidir qué parte del proveedor de servicios FSSS debería/podría alojarse (o alojarse parcialmente) de forma segura en un entorno en la nube.

Un proveedor de servicios de FSSS protege constantemente la vida y la propiedad y, en este sentido, los requisitos son más críticos que en la mayoría de las demás organizaciones.

4. Entornos en la Nube

4.1. Introducción

La diligencia debida es crucial a la hora de evaluar y seleccionar proveedores de servicios en la nube. La diligencia debida consiste en investigar y evaluar a fondo a los posibles vendedores o proveedores de servicios antes de entablar una relación comercial con ellos. Este proceso le ayudará a comprender mejor las capacidades del proveedor, su fiabilidad, sus medidas de seguridad y su idoneidad general para sus necesidades específicas.

La diligencia debida es crucial a la hora de evaluar y seleccionar proveedores de servicios en la nube. La diligencia debida consiste en investigar y evaluar a fondo a los posibles vendedores o proveedores de servicios antes de entablar una relación comercial con ellos. Este proceso le ayudará a comprender mejor las capacidades del proveedor, su fiabilidad, sus medidas de seguridad y su idoneidad general para sus necesidades específicas.

Este documento no implica que las soluciones de nube empresarial privada o los entornos de nube sean el único modo de funcionamiento para todas las aplicaciones, pero se reconoce que el proveedor de servicios de FSSS puede operar y operará aplicaciones en múltiples modelos de entorno. En otras palabras, pueden utilizar los tres entornos operativos en mayor o menor medida, dependiendo de los requisitos del servicio.

Los proveedores de servicios FSSS también deben tener en cuenta sus requisitos de certificación de terceros a la hora de elegir su propia solución o centro de datos o soluciones en la nube.

El uso de centros de datos/servicios en la nube no excluye las responsabilidades del proveedor de servicios FSSS, tal como se detallan en las normas EN 16763, EN 50710 o EN 50136-1 (ver A2.2 en el Anexo 2 para la explicación de dichas normas). Una guía[2] Euralarm dedicada a la implementación de servicios remotos, que puede encontrar en el sitio web. Ayuda al proveedor de servicios FSSS a comprobar previamente su cumplimiento de los requisitos de estas normas.

4.2. Solución en cloud propietaria

Las soluciones propietarias son gestionadas por el proveedor de servicios FSSS. Los servidores se instalan en el mismo edificio o local donde se encuentra el proveedor de servicios FSSS o en otro edificio bajo la responsabilidad del proveedor de servicios FSSS. Un proveedor de aplicaciones suministrará a la empresa de servicios el software para ejecutar en los servidores. Los servidores son adquiridos por el proveedor de servicios FSSS o comprados como parte del servicio del proveedor de aplicaciones.

Las actualizaciones de los sistemas operativos del servidor, las bases de datos y el software de aplicación se coordinarán entre el proveedor de servicios FSSS y el proveedor de aplicaciones. La seguridad (cifrado en reposo, etc.) y la fiabilidad (como la replicación de bases de datos con diversidad geográfica) son soluciones que generalmente construye el proveedor de aplicaciones.

4.3. Centro de datos externo

Las soluciones de centros de datos son servidores que se instalan en dependencias gestionadas por una empresa externa que proporciona seguridad física, energía y espacio en bastidor para alojar servidores. Estos servidores pueden estar dedicados a un proveedor de servicios FSSS específico o funcionar en un entorno multiinquilino. Estos servidores son mantenidos por el proveedor de servicios FSSS o por el proveedor de aplicaciones como un servicio gestionado.

[2] https://www.euralarm.org/resource/guidance-on-remote-services---final-xlsx.html

4.4. Solución en nube externa

4.4.1. Descripción

Las soluciones en la nube incluyen todas las características de la solución del centro de datos, pero los servidores y otras tecnologías relacionadas (bases de datos, etc.) son proporcionados y mantenidos por el proveedor de servicios en la nube (por ejemplo, AWS - Amazon Web Services, Microsoft Azure, Google Cloud, IBM). El Modelo de Responsabilidad Compartida (SRM) en la nube es un marco que delimita las responsabilidades entre un proveedor de servicios en la nube y el proveedor de aplicaciones para asegurar el entorno de la nube.

El proveedor de servicios en la nube protege los activos del entorno del desarrollador de aplicaciones. Por ejemplo, proporciona seguridad física y protege los servicios de virtualización. El proveedor de aplicaciones protege los activos en su instancia en la nube, es decir, el proveedor de aplicaciones protege el sistema operativo que instala en los servidores y mantiene quién tiene acceso a su entorno en la nube.

La computación en la nube abarca varios modelos que satisfacen diferentes necesidades y casos de uso. Es importante señalar que estos modelos no son mutuamente excluyentes, y los proveedores de servicios en la nube a menudo ofrecen una combinación de ellos para satisfacer diferentes requisitos y preferencias. En las siguientes secciones se describen cuatro modelos de nube diferentes.

4.4.2. Infraestructura como Servicio (IaaS)

Este modelo proporciona recursos de computación virtualizados a través de internet. Ofrece máquinas virtuales, almacenamiento y redes que los usuarios pueden aprovisionar y gestionar. Los usuarios tienen más control sobre la infraestructura, incluyendo sistemas operativos y aplicaciones.

4.4.3. Plataforma como Servicio (PaaS)

La PaaS ofrece una plataforma para que los desarrolladores creen, implementen y gestionen aplicaciones sin preocuparse por la infraestructura subyacente. Proporciona un entorno preconfigurado con herramientas, marcos y tiempo de ejecución para el desarrollo de aplicaciones. Los usuarios pueden centrarse en la codificación y la lógica de la aplicación mientras la plataforma se encarga de la escalabilidad, el equilibrio de carga y el despliegue.

4.4.4. Arquitectura sin Servidor

La computación sin servidor es un modelo en el que los desarrolladores escriben e implementan código como funciones individuales o unidades de código. El proveedor de servicios en la nube gestiona la infraestructura y escala y proporciona recursos automáticamente en función de la demanda. Los desarrolladores no tienen que preocuparse por la gestión de servidores o infraestructuras, y pueden centrarse únicamente en escribir el código.

4.4.5. Software como Servicio (SaaS)

El SaaS es una aplicación de software completa que se entrega a través de Internet. Los usuarios finales de los proveedores de servicios FSSS o FSSS pueden acceder al software y utilizarlo sin necesidad de instalación ni gestión. Los proveedores de soluciones SaaS ejecutarán sus servidores en modelos informáticos IaaS, PaaS o sin servidor.

4.4.6. Consideraciones para los modelos nativos de la nube

Es importante considerar cuidadosamente los requisitos y limitaciones específicos de una aplicación de misión crítica al elegir entre entornos. Se deben sopesar factores como las necesidades de rendimiento, los requisitos de escalabilidad, las opciones de gestión y las consideraciones de coste para determinar la mejor configuración para los objetivos de la aplicación.

Consulte el Anexo 1 para obtener más información.

4.5. Solución de fabricante

Los fabricantes de FSSS han desarrollado sus soluciones y las ofrecen a los proveedores de servicios de FSSS que utilizan sus sistemas. Dicha solución puede basarse en cualquiera de los 3 entornos descritos anteriormente. El proveedor de servicios de FSSS no tiene que preocuparse por el mantenimiento de los servidores, el software y la aplicación. Debe garantizar un contrato que se ajuste a sus necesidades y expectativas.

Por lo general, el proveedor de servicios de FSSS no tiene contrato con el fabricante para el uso de su solución, pero acepta las condiciones generales al iniciar sesión en la aplicación en la nube. Por lo tanto, se aconseja que el fabricante elabore un documento para el instalador en el que quede claro, sobre su aplicación en la nube:

- Cuál es el proveedor de servicios en la nube,
- Dónde se ubicarán los datos,
- Cómo se puede acceder a ellos, incluidas las medidas de seguridad,
- El nivel de servicio, como el tiempo de recuperación y el mantenimiento,
- A qué certificación puede hacer referencia el fabricante,
- Cómo debe conectar correctamente el proveedor de servicios FSSS,
- ...

4.6. Consideraciones para entornos operativos

Las soluciones privadas de nube empresarial y de centro de datos requieren inversión en hardware, software e infraestructura, así como experiencia para configurarlas y mantenerlas. Las soluciones basadas en la nube siguen exigiendo que el proveedor de la aplicación tenga las habilidades necesarias para comprender, supervisar y escalar la funcionalidad requerida. El proveedor de servicios en la nube agrupa servicios informáticos expertos para la implementación y el mantenimiento del hardware, los sistemas operativos y el software de bases de datos.

Deben tomarse medidas para considerar la seguridad de los datos accesibles a través de conexiones en línea o basadas en la nube.

5. Criterios legales para la ubicación de los servidores

5.1. Introducción

Las normativas sobre servidores de datos en los países europeos se rigen por una combinación de leyes nacionales y reglamentos de la Unión Europea. A continuación, se ofrece una visión general de las normas clave en varios países europeos, así como del marco general de la UE.

5.2. Reglamento General de Protección de Datos (RGPD) de la Unión Europea

El RGPD, en vigor desde mayo de 2018, es el principal reglamento que rige la protección de datos y la privacidad en la UE. Rige en todos los estados miembros e incluye:

- Principios del tratamiento de datos: licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del almacenamiento, integridad y confidencialidad;
- Derechos del interesado: derecho de acceso, rectificación, supresión (derecho al olvido), limitación del tratamiento, portabilidad de los datos y oposición;
- Transferencia de datos: restricciones a la transferencia de datos personales fuera de la UE/EEE, garantizando niveles adecuados de protección;
- Notificaciones de vulneración de datos: obligación de notificar a las autoridades y a las personas afectadas las vulneraciones de datos en un plazo de 72 horas.

5.3. Ejemplos de regulaciones específicas de cada país

Alemania

Ley Federal de Protección de Datos (Bundesdatenschutzgesetz, BDSG): Complementa el RGPD con requisitos adicionales, incluidas normas más estrictas sobre el tratamiento de datos con fines laborales y obligaciones específicas para los responsables de la protección de datos.

Francia

Ley de Protección de Datos (*Loi Informatique et Libertés*): Hace cumplir las disposiciones del RGPD y añade especificidades nacionales, como normas sobre el tratamiento de datos sanitarios y competencias adicionales para la autoridad nacional de protección de datos (CNIL).

Reino Unido

Ley de Protección de Datos de 2018 (Data Protection Act 2018):: Implementa el RGPD e incluye disposiciones específicas para el tratamiento de datos por parte de las autoridades y los organismos encargados de hacer cumplir la ley. Tras el Brexit, el Reino Unido ha adoptado el RGPD del Reino Unido, que refleja el RGPD de la UE pero funciona de forma independiente.

Italia

Código de Protección de Datos (*Codice in materia di protezione dei dati personali*): Se alinea con el RGPD, con normas nacionales adicionales sobre el tratamiento de datos para la investigación científica e histórica y con fines periodísticos.

España

Ley Orgánica de Protección de Datos y Derechos Digitales (LOPDGDD): complementa el RGPD con normas específicas sobre derechos digitales y protecciones adicionales para menores y personas vulnerables.

Países Bajos

Ley de Implementación Holandesa (Uitvoeringswet AVG): complementa el RGPD con disposiciones nacionales, en particular en lo que respecta al tratamiento de antecedentes penales y datos de empleados.

Bélgica

Ley de Implementación Belga (*Gegevensbeschermingsautoriteit GBA*): Ley Marco del 30 de julio de 2018

Los temas comunes en todos los países son:

- Localización de datos: algunos países tienen requisitos específicos para la localización de datos, en particular para datos sensibles como los registros sanitarios;

- normativas específicas del sector: muchos países imponen normativas adicionales para determinados sectores, como el financiero, el sanitario y el de las telecomunicaciones;
- Autoridades de Protección de Datos (APD): cada país tiene una APD nacional responsable de hacer cumplir las leyes de protección de datos y de gestionar las reclamaciones. Algunos ejemplos son la CNIL en Francia, la ICO en el Reino Unido y la BfDI en Alemania;
- Transferencias de Datos Transfronterizas: Los países de la UE generalmente siguen el marco del RGPD para las transferencias internacionales de datos, que incluyen mecanismos como las Cláusulas Contractuales Tipo (CCT), las Normas Corporativas Vinculantes (NCV) y las decisiones de adecuación..

Esta lista de legislaciones específicas de cada país no es exhaustiva. Para conocer normativas más específicas y las últimas actualizaciones, es aconsejable consultar las respectivas DPA nacionales y los textos legales de cada país.

5.4. Referencias de utilidad

- Comisión Europea - Protección de Datos[3]
- Texto del RGPD[4]
- CNIL (Francia)[5]
- ICO (Reino Unido)[6]
- BfDI (Alemania)

6. Distribución de roles y responsabilidades

6.1. Impacto de las actividades de mantenimiento (planificadas/no planificadas)

La disponibilidad de la infraestructura puede ser de distinta importancia en función de los servicios que se presten con ella. Los servicios de transmisión de alarmas requieren una alta disponibilidad definida por la categoría aplicable de la norma EN 50136-1. La disponibilidad se considera generalmente menos importante para los servicios de acceso remoto.

El proveedor de servicios de FSSS o el fabricante en el entorno de solución del fabricante) debe contar con procesos para gestionar las actividades de mantenimiento y, cuando sea necesario, mitigarlas, por ejemplo, disponibilidad del sistema secundario o infraestructura duplicada, etc.

Los proveedores de servicios FSSS que estén considerando una solución alojada deben asegurarse de que existen acuerdos (SLA) con los proveedores de servicios en la nube para garantizar que se notifique al proveedor de servicios FSSSIcon antelación la duración de los períodos fuera de línea durante el mantenimiento planificado. Estos contratos también deben incluir la forma en que se gestiona y comunica el mantenimiento no planificado.

Cuando los proveedores de servicios de FSSS dependan de terceros para los servicios de TI, el proveedor de servicios de FSSS debe considerar cómo los incidentes pueden afectar a la capacidad de los proveedores de servicios de TI para prestar asistencia.

[3] https://commission.europa.eu/law/law-topic/data-protection_en
[4] https://eur-lex.europa.eu/eli/reg/2016/679/oj
[5] https://www.cnil.fr/en
[6] https://ico.org.uk

6.2. Competencia en TI

El proveedor de servicios de FSSS es el responsable final de sus propios equipos y sistemas y requerirá cierto nivel de competencia local en TI para garantizar la gestión de las actividades rutinarias de supervisión y mantenimiento de la solución del proveedor de servicios de FSSS.

6.3. Seguridad

Los proveedores de servicios FSSS deben considerar quién tiene acceso a sus sistemas y datos, así como los requisitos de selección del personal. Existen varias opciones para resolver los problemas de seguridad, entre ellas:

- Gestión de identidades y acceso (IAM)
- Cifrado
- Supervisión y registro de seguridad
- Cumplimiento y certificaciones
- Seguridad de red

Las soluciones de centros de datos requieren personal in situ o acceso remoto para gestionar y mantener la infraestructura, lo que incluye el mantenimiento del hardware, las actualizaciones de software y los parches de seguridad. Por el contrario, las soluciones en la nube son gestionadas por el proveedor de servicios en la nube, que se encarga de todo el mantenimiento de la infraestructura, las actualizaciones de software y los parches de seguridad, liberando al personal interno de TI para que se concentre en las funciones principales de negocio.

En cualquier entorno en la nube, existe una responsabilidad compartida entre el proveedor de servicios en la nube (CSP) y el usuario (proveedor de servicios FSSS o fabricante). La seguridad de aspectos como la clasificación de datos, los controles de red y la seguridad física necesita propietarios claros. La división de estas responsabilidades se conoce como modelo de responsabilidad compartida (SRM) para la seguridad en la nube. Consulte este gráfico para ver dónde recaen las responsabilidades dentro de los diferentes entornos en la nube.

Solución en cloud propietaria	**Infraestructura como Servicio *IaaS***	**Plataforma como Servicio *PaaS***	**Software como Servicio *SaaS***
Datos y configuraciones	Datos y configuraciones	Datos y configuraciones	Datos y configuraciones
Código de aplicación	Código de aplicación	Código de aplicación	Código de aplicación
Escalado	Escalado	Escalado	Escalado
Tiempo de ejecución	Tiempo de ejecución	Tiempo de ejecución	Tiempo de ejecución
Sistema operativo	Sistema operativo	Sistema operativo	Sistema operativo
Virtualización	Virtualización	Virtualización	Virtualización
Hardware	Hardware	Hardware	Hardware
Gestionado por el proveedor de servicios FSSS o el fabricante			
Gestionado por un proveedor de servicios en la nube			

Puede encontrar más información y orientación sobre SRM en el sitio web del Centro para la Seguridad en Internet (CIS)[7].

[7] https://www.cisecurity.org/insights/blog/shared-responsibility-cloud-security-what-you-need-to-know

7. Contratación de servicios en la nube

La Comisión Europea escribió en 2012 en su comunicado titulado Aprovechar el potencial de la computación en la nube en Europa[8]:

> *"Los acuerdos tradicionales de subcontratación de TI se negociaban habitualmente y estaban relacionados con el almacenamiento de datos, las instalaciones de procesamiento y los servicios definidos y descritos en detalle y por adelantado. Los contratos de computación en la nube, por otro lado, crean esencialmente un marco en el que el usuario tiene acceso a capacidades de TI infinitamente escalables y flexibles según sus necesidades. Sin embargo, actualmente la mayor flexibilidad de la computación en la nube en comparación con la subcontratación tradicional se ve a menudo contrarrestada por una menor certeza para el cliente debido a contratos insuficientemente específicos y equilibrados con los proveedores de la nube.*
>
> *La complejidad e incertidumbre del marco legal para los proveedores de servicios en la nube implica que a menudo utilizan contratos complejos o contratos de nivel de servicio con amplias exenciones de responsabilidad. El uso de contratos estándar de "lo tomas o lo dejas" puede suponer un ahorro de costes para el proveedor, pero a menudo no es deseable para el usuario, incluido el consumidor final. Estos contratos también pueden imponer la elección de la ley aplicable o impedir la recuperación de datos. Incluso las empresas más grandes tienen poco poder de negociación y los contratos a menudo no prevén la responsabilidad por la integridad de los datos, la confidencialidad o la continuidad del servicio."*

Con el fin de ayudar a abordar esta complejidad e incertidumbre, puede encontrar una guía detallada sobre los elementos contractuales clave en Guías sobre la subcontratación a proveedores de servicios en la nube[9] emitida por la Autoridad Europea de Valores y Mercados (ESMA) en 2021 en numerosos idiomas europeos. En particular, las siguientes secciones del documento pueden ser relevantes:

- Guía 3 – Elementos contractuales clave
- Guía 4 – Seguridad de la información
- Guía 5 – Estrategias de salida
- Guía 6 – Derechos de acceso y auditoría.

NOTA: Se pueden encontrar unas directrices similares en el sitio web de la Autoridad Europea de Seguros y Pensiones de Jubilación (AESPJ)[10].

Además, en el marco de la Ley de Datos ((UE) 2023/2854), la Comisión Europea está preparando cláusulas contractuales tipo para orientar a las partes interesadas en la aplicación de las disposiciones relativas al cambio de proveedor de servicios en la nube y al intercambio de datos. Se espera que esta guía se publique en el transcurso de 2025.

Por último, el anexo 2 de esta guía de Euralarm proporciona referencias a normas y sistemas de certificación cuyo cumplimiento puede exigirse en el contrato con el proveedor de servicios en la nube.

Puede encontrar más información sobre los contratos de computación en la nube en el sitio web de la CE:

- Contratos de computación en la nube[11]

[8] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF
[9] https://www.esma.europa.eu/document/guidelines-outsourcing-cloud-service-providers
[10] https://www.eiopa.europa.eu/system/files/2020-04/guidelines_on_outsourcing_to_cloud_service_providers_en.pdf
[11] https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/cloud-computing/cloud-computing-contracts_en

- Estudio comparativo sobre contratos de computación en la nube[12]

8. Conclusiones

Dado que no existe un sistema de certificación único ni unificado para los centros de datos y los servicios en la nube, el proveedor de servicios FSSS debe tener la seguridad de que el CSP se asegura de que el centro de datos cumple los requisitos de fiabilidad y seguridad necesarios para el caso de uso considerado. Cualquier declaración de cumplimiento que alegue el CSP o el fabricante para demostrar la fiabilidad y seguridad del servicio en la nube debe abarcar al menos las siguientes consideraciones:

- Con respecto al centro de datos utilizado:
  - Su nombre y ubicación(es);
  - Nivel de garantía de continuidad del negocio, desde la ausencia de continuidad hasta la continuidad total en caso de fallo del centro de datos (fundamental para la transmisión de alarmas y conveniente para el acceso remoto);
  - Medios para minimizar el riesgo de fallo, como la selección de uno o varios centros, la estructura del edificio, los sistemas de alimentación, los sistemas de refrigeración, los sistemas mecánicos, la arquitectura, la seguridad física, la ciberseguridad, la infraestructura de cableado, los sistemas de telecomunicaciones, la política de copias de seguridad, la protección contra incendios y la seguridad (fundamental para la transmisión de alarmas y la facilidad de acceso remoto);
- Entorno de nube utilizado:
  - Entorno en la nube utilizado;
  - Distribución clara de roles y responsabilidades debidamente establecidos en un SLA;
  - Plan de Recuperación de Desastres (DRP) en vigor (crítico para la transmisión de alarmas y conveniente para el acceso remoto);
  - Plan de pruebas después de una actualización de software;
  - Notificación al proveedor de servicios de FSSS en caso de actualizaciones del sistema, actualizaciones de software o cambio de proveedores;
- En cuanto a la ciberseguridad y la privacidad del centro de datos y el servicio en la nube:
  - Cumplimiento de la norma ISO/IEC 27001;
  - Certificado bajo el esquema de certificación EUCS (cuando esté disponible, consulte A2.6);
  - Mecanismos seguros de control de acceso con autenticación para acceder a los datos y funciones almacenados;
  - Cifrado de datos en tránsito;
  - Mitigación de los efectos de los ataques (D)DoS;
  - Proceso de gestión de vulnerabilidades;
  - Verificación mediante pruebas de penetración;
- Para la transmisión de las alarmas:
  - Cumplimiento del ATS con la norma EN 50136-1 en una categoría declarada que sea apropiada para el riesgo protegido (tiempo de transmisión, disponibilidad, tiempo de notificación en caso de fallos de transmisión, requisito de cifrado, seguridad de sustitución, modo de reconocimiento, etc.);
  - Categoría de doble vía (DP) donde se cubren riesgos elevados o para sistemas vitales (que ponen en peligro la vida);
- Para el acceso remoto al FSSS:
  - Cumplimiento desde la ley RAI a la norma CLC/TS 50136-10.

[12] https://op.europa.eu/en/publication-detail/-/publication/40148ba1-1784-4d1a-bb64-334ac3df22c7

9. Bibliografía

"ARC considerations when utilising data centre or cloud services", BSIA (British Security Industry Association), Issue 1, Octubre de 2023.

Anexo 1 - Centro de Datos/IaaS y Sin Servidor

Para una aplicación de misión crítica, tanto la IaaS (Infraestructura como Servicio) como los entornos sin servidor tienen sus pros y sus contras. Aquí tiene una comparativa entre ambos:

- Complejidad de Gestión: En un entorno IaaS, los usuarios tienen control total sobre la infraestructura, lo que significa que deben manejar tareas como el aprovisionamiento y la gestión de servidores, la configuración de redes y la garantía de alta disponibilidad. Esto requiere más experiencia, tiempo y recursos en comparación con un entorno sin servidor, en el que no se gestiona la infraestructura. Con el modelo sin servidor, los proveedores de aplicaciones pueden centrarse únicamente en la prestación de servicios de software, pero tienen menos conocimiento de la infraestructura subyacente, lo que puede ser una limitación para ciertas aplicaciones de misión crítica.

- Escalabilidad: En un entorno IaaS, escalar la infraestructura para gestionar el aumento del tráfico o de la demanda requiere intervención y configuración manual. Por otro lado, los entornos sin servidor escalan automáticamente los recursos en función del número de solicitudes o eventos activados, lo que permite una escalabilidad más dinámica. Sin embargo, los entornos sin servidor pueden tener ciertas limitaciones de escalabilidad, como el número máximo de ejecuciones simultáneas o la duración de la ejecución, lo que puede afectar a las aplicaciones más exigentes.

- Arranque en frío y Rendimiento: Los entornos sin servidor a menudo tienen un concepto llamado «arranque en frío», en el que la primera ejecución de una función incurre en latencia adicional debido a la necesidad de inicializar el entorno de ejecución. Esta latencia puede afectar a las aplicaciones en tiempo real o de baja latencia. En un entorno IaaS, las aplicaciones se ejecutan en servidores dedicados o máquinas virtuales, que suelen ofrecer un rendimiento constante sin retrasos por arranque en frío. Además, los entornos sin servidor pueden tener limitaciones en los recursos asignados a las funciones individuales, lo que puede afectar al rendimiento de las aplicaciones que consumen muchos recursos.

- Vinculación con el Proveedor: Aunque tanto los entornos IaaS como los entornos sin servidor implican cierto nivel de vinculación con el proveedor, los entornos sin servidor suelen tener servicios más estrechamente integrados y arquitecturas basadas en eventos, lo que puede dificultar la migración de aplicaciones entre diferentes proveedores de servicios en la nube o a la infraestructura local. En un entorno IaaS, los usuarios tienen más flexibilidad para trasladar sus aplicaciones entre diferentes proveedores o incluso para incorporarlas internamente.

- Coste y Previsibilidad: Los entornos sin servidor siguen un modelo de precios de pago por uso, que puede ser rentable para aplicaciones con cargas de trabajo esporádicas o variables. Sin embargo, la estructura de precios puede ser a veces compleja e impredecible, especialmente con cargos adicionales por llamadas a la API, transferencia de datos y uso de recursos. En un entorno IaaS, los usuarios tienen más control sobre la asignación de recursos y los precios, lo que permite una mejor previsibilidad de los costes, pero con costes fijos potencialmente más elevados.

Anexo 2 - Normas y sistemas de certificación

A2.1. Introducción

Las siguientes son normas básicas relativas a la transmisión de alarmas, el acceso remoto y los centros de datos que pueden ser útiles a la hora de determinar el rendimiento de un sistema o servicio en términos de resistencia, solidez y fiabilidad.

A2.2. Normas para la transmisión de alarmas, el acceso remoto a sistemas de alarma y los servicios remotos

EN 50136-1 Requisitos generales para los sistemas de transmisión de alarmas

Esta norma europea especifica los requisitos de rendimiento, fiabilidad y seguridad de los sistemas de transmisión de alarmas. Especifica los requisitos de los sistemas de transmisión de alarmas que proporcionan transmisión de alarmas entre un sistema de alarma en un local supervisado y un equipo de aviso en un centro receptor de alarmas.

Esta norma europea se aplica a los sistemas de transmisión para todo tipo de mensajes de alarma, como incendios, intrusión, control de acceso, teleasistencia, etc.

Un proveedor de servicios FSSS que asuma el papel de ATSP (proveedor de servicios de transmisión de alarmas) debe cumplir con las disposiciones de esta norma.

CLC/TS 50136-10 Sistemas de alarma: Requisitos para el acceso remoto

Este documento especifica los requisitos mínimos para una conexión y sesión seguras para el acceso remoto a uno o más sistemas de alarma, por ejemplo, sistemas de seguridad contra incendios, sistemas de alarma contra intrusos y atracos, sistemas electrónicos de control de acceso, sistemas de seguridad perimetral externa, sistemas de videovigilancia y sistemas de teleasistencia.

Este documento especifica los requisitos de rendimiento, fiabilidad, integridad y seguridad de una infraestructura de acceso remoto.

Este documento especifica los requisitos para una infraestructura de acceso remoto entre un cliente de acceso remoto y un sistema de alarma en las instalaciones supervisadas y puede integrarse como parte del ATS o como una infraestructura independiente.

Un proveedor de servicios FSSS que asuma el papel de RAISP (proveedor de servicios de infraestructura de acceso remoto) debe cumplir con las disposiciones de esta especificación técnica.

UNE-EN 50710: Requisitos para la prestación de servicios remotos seguros para sistemas de protección contra incendios y sistemas de seguridad.

Este documento especifica los requisitos mínimos para la prestación de servicios remotos seguros a través de una infraestructura de acceso remoto (RAI) realizada en el sitio o fuera de él (por ejemplo, a través de conexiones IP) a los siguientes sistemas:

a) sistemas de seguridad contra incendios, incluidos, entre otros, sistemas de detección y alarma de incendios, sistemas fijos de extinción de incendios, sistemas de control de humo y calor;
b) sistemas de seguridad, incluidos, entre otros, sistemas de alarma contra intrusos y atracos, sistemas electrónicos de control de acceso, sistemas de seguridad perimetral externa y sistemas de videovigilancia;
c) sistemas de alarma social;
d) sistemas de sonido de emergencia;
e) una combinación de tales sistemas;
f) sistemas de gestión conectados a sistemas a) – e).

Esta norma pretende complementar EN 16763 *Servicios para sistemas de seguridad contra incendios y sistemas de seguridad.*

A2.3. Norma para servicios en la nube

CEN/TS 18026 Enfoque de tres niveles para un conjunto de requisitos de ciberseguridad para servicios en la nube

Esta Especificación Técnica (TS) proporciona un conjunto de requisitos de ciberseguridad para los servicios en la nube. Esta TS es aplicable a las organizaciones que prestan servicios en la nube y a sus organizaciones de subservicios.

Nota: se espera que este nuevo TS se publique durante el verano de 2024.

A2.4. Norma para sistemas de gestión de seguridad de la información

ISO/IEC 27001 Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de la seguridad de la información - Requisitos

La ISO/IEC 27001 es una norma internacional ampliamente reconocida que describe las mejores prácticas para implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI). Esta norma proporciona un marco para la gestión de los riesgos de seguridad de la información, incluyendo personas, procesos y tecnología.

La ISO/IEC 27001 cubre todos los aspectos de la seguridad de la información, incluyendo la confidencialidad, integridad y disponibilidad, y requiere que las organizaciones implementen controles para garantizar la confidencialidad, integridad y disponibilidad de sus activos de información.

La norma también exige que las organizaciones adopten un enfoque basado en el riesgo para la gestión de la seguridad de la información, lo que implica identificar y evaluar los riesgos, implementar controles adecuados para mitigarlos y supervisar y revisar continuamente la eficacia de los controles.

Al implementar la norma ISO/IEC 27001, las organizaciones pueden demostrar su compromiso con la seguridad de la información y ofrecer garantías a las partes interesadas de que sus activos de información se gestionan de forma segura y eficaz. La norma es aplicable a organizaciones de todos los tamaños y sectores, y está ampliamente reconocida como referencia para la gestión de la seguridad de la información.

A2.5. Normas para centros de datos

ISO/IEC 22237 (y EN 50600) Tecnología de la información: instalaciones e infraestructuras de centros de datos

La ISO 22237 es la serie de normas ISO que rige el diseño, la estructura, el funcionamiento y la seguridad física y de la información de los centros de datos. La intención de la norma es definir las condiciones necesarias para permitir que se alcancen los objetivos de la norma ISO 27001 en un entorno de centro de datos.

La norma EN 50600 es la serie de normas EN que regula la planificación, el diseño, la adquisición, la integración, la instalación, el funcionamiento y el mantenimiento de las instalaciones y las infraestructuras de los centros de datos. Aunque la serie EN 50600 establece disposiciones similares a las normas ISO 22237, no están totalmente alineadas.

La norma EN 50600 es una familia de normas en crecimiento que actualmente consta de las siguientes partes:

- EN 50600-1, Conceptos generales
- EN 50600-2-1, Construcción de edificios
- EN 50600-2-2, Suministro y distribución de energía
- EN 50600-2-3. Control ambiental
- EN 50600-2-4, Infraestructura de cableado de telecomunicaciones
- EN 50600-2-5, Sistemas de seguridad
- EN 50600-3-1, Información de gestión y operativa
- EN 50600-4-1, Resumen y requisitos generales de los indicadores clave de rendimiento
- EN 50600-4-2, Eficacia en el uso de la energía
- EN 50600-4-3, Factor de energía renovable

La norma EN 50600 establece un sistema de clasificación basado en los criterios clave de disponibilidad, seguridad y eficiencia energética:

1. Nivel de disponibilidad. La clasificación de disponibilidad se define en las áreas de suministro eléctrico, sistemas de ventilación y aire acondicionado y cableado;
2. Nivel de protección. El nivel de proteccion se define para la prevención de intrusiones, la protección contra incendios, la protección contra humos y la protección contra riesgos ambientales. Debe definirse al menos una protección de clase 3.
3. Nivel de granularidad. La capacidad de funcionamiento energéticamente eficiente se define en función de las características y alcance de las mediciones de los sistemas de ventilación y aire acondicionado. La norma distingue entre tres niveles de granularidad diferentes.

Para que el diseño de un centro de datos se ajuste a esta norma:

a. Se deberá completar un análisis de riesgos de negocio;
b. Se seleccionará una clase de disponibilidad adecuada utilizando el análisis de riesgos empresariales;
c. Una clase de protección adecuada para las rutas y espacios del centro de datos;
d. Un nivel de granularidad adecuado;
e. Se aplicarán el proceso y los principios de diseño.

Nota: Actualmente, los centros de datos no suelen tener en cuenta ni la norma EN 50600 ni la ISO 22237. Los centros de datos (AWS, etc.) suelen estar certificados por el instituto privado Uptime Institute (certificación Tier) o según la norma ANSI/TIA-942. Estos dos sistemas de certificación se consideran complementarios.

Certificación de Nivel del Uptime Institute

Este organismo de certificación privado aplica sus propios estándares de nivel para la disponibilidad del centro de

datos y el rendimiento general. Permite varios niveles de rendimiento que tienen en cuenta tanto el entorno construido como el enfoque y el rendimiento del equipo de operaciones. Se definen 4 niveles:

- Nivel I: Capacidad básica: Se requieren paradas en todo el centro para trabajos de mantenimiento o reparación. Los fallos de capacidad o distribución afectarán al centro.
- Nivel II: Componentes de capacidad redundantes: Se siguen requiriendo paradas en todo el centro para mantenimiento. Los fallos de capacidad pueden afectar al centro. Los fallos de distribución afectarán al centro.
- Nivel III: Mantenimiento simultáneo: Todos y cada uno de los componentes de capacidad y rutas de distribución de un sitio pueden retirarse de forma planificada para su mantenimiento o sustitución sin que ello afecte a las operaciones. El sitio sigue expuesto a una avería del equipo o a un error del operador.
- Nivel IV: Tolerancia a fallos: Una avería en un equipo o la interrupción de una ruta de distribución no afectará a las operaciones. Un sitio con tolerancia a fallos también es de mantenimiento simultáneo.

ANSI/TIA-942 Norma de Infraestructura de Telecomunicaciones para Centros de Datos

ANSI/TIA-942 es una norma publicada por la Asociación del Sector de las Telecomunicaciones (TIA) que proporciona directrices para el diseño y la construcción de centros de datos, incluidos los sistemas de energía, los sistemas mecánicos, la arquitectura, la seguridad, los sistemas de telecomunicaciones, la protección contra incendios y la seguridad. La norma tiene por objeto garantizar que los centros de datos sean fiables, seguros y escalables para satisfacer las necesidades cambiantes del sector de las tecnologías de la información.

ANSI/TIA-942 proporciona un marco integral para el diseño de centros de datos, que incluye recomendaciones para la selección del emplazamiento, la estructura del edificio, la infraestructura de cableado, los sistemas de refrigeración y alimentación, la seguridad y la gestión.

ANSI/TIA-942 es utilizada por los diseñadores, operadores y auditores de centros de datos para garantizar que los centros de datos se diseñan y construyen de acuerdo con las mejores prácticas y estándares del sector. Los organismos reguladores y los clientes también consultan con frecuencia esta norma para evaluar la fiabilidad y seguridad de los centros de datos.

Controles del Sistema y la Organización (SOC) 2

SOC 2 es un conjunto de normas desarrolladas por el Instituto Americano de Contadores Públicos Certificados (AICPA) para evaluar y auditar la seguridad, disponibilidad, integridad de procesamiento, confidencialidad y privacidad de los sistemas y datos de una organización de servicios.

Nota: mientras que la ISO/IEC 27001 es genérica, SOC 2 está contextualizada para centros de datos.

Los informes SOC 2 son utilizados por organizaciones de servicios (como centros de datos) para demostrar a sus clientes y partes interesadas que cuentan con controles internos eficaces para proteger sus datos confidenciales.

Los informes SOC 2 se basan en los Criterios de Servicios Fiduciarios (TSC), que son un conjunto de principios y criterios utilizados para evaluar la eficacia de los controles de una organización de servicios sobre sus sistemas y datos.

Existen dos tipos de informes SOC 2: Tipo I y Tipo II. Los informes Tipo I evalúan el diseño de los controles de una organización de servicios, mientras que los informes Tipo II evalúan la eficacia de esos controles durante un

período determinado.

Las auditorías SOC 2 son realizadas por auditores externos independientes, que están certificados por el AICPA.

Las auditorías SOC 2 son voluntarias, pero cada vez son más importantes para las organizaciones de servicios que desean demostrar su compromiso con la seguridad y la privacidad.

Para preparar una auditoría SOC 2, las organizaciones de servicios deben realizar una evaluación de riesgos e implementar un conjunto integral de controles para abordar los Criterios de Servicios Fiduciarios.

Las auditorías SOC 2 normalmente implican una combinación de entrevistas, revisiones de documentación y pruebas de sistemas para evaluar la eficacia de los controles de los servicios de la organización.
servicios, así como una descripción de los controles que se han probado y de las deficiencias identificadas.

Los informes SOC 2 pueden compartirse con clientes, partes interesadas y organismos reguladores para garantizar que una organización de servicios ha implementado controles eficaces para proteger los datos confidenciales.

SOC 3

SOC 3 es un tipo de informe de certificación que proporciona una visión general de alto nivel de los controles de una organización relacionados con la seguridad, la disponibilidad, la integridad del procesamiento, la confidencialidad y la privacidad.

A diferencia de los informes SOC 1 y SOC 2, que están destinados a un público específico y proporcionan información más detallada sobre los controles de una organización, los informes SOC 3 están diseñados para un público general y proporcionan un resumen de los controles de la organización que puede compartirse públicamente.

Los informes SOC 3 se basan en los mismos controles y criterios que los informes SOC 2, pero no proporcionan el mismo nivel de detalle. En su lugar, los informes SOC 3 incluyen una breve descripción del sistema y los controles de la organización, junto con una declaración de un auditor independiente que da fe del cumplimiento de la organización con los criterios SOC 2.

Las organizaciones suelen utilizar los informes SOC 3 para demostrar su compromiso con la seguridad y el cumplimiento a clientes, socios y otras partes interesadas. Dado que están disponibles públicamente, también pueden ser utilizados por clientes o inversores potenciales para evaluar la postura de seguridad de una organización antes de hacer negocios con ellos.

A2.6. Sistemas de certificación

La Ley de Ciberseguridad (CSA, (UE) 2019/881) proporciona un marco europeo para la certificación de la ciberseguridad de productos, procesos y servicios. ENISA, la Agencia de la Unión Europea para la Ciberseguridad, está facultada para desarrollar esquemas de certificación de ciberseguridad destinados a ser utilizados de forma voluntaria y válidos en toda la Unión Europea. El segundo esquema pretende abarcar los servicios en la nube (EUCS). Todavía está en preparación en la fecha de redacción de la presente guía. Se espera que este esquema

haga uso de la CEN/TS 18026 presentada anteriormente. Cuando esté disponible, podría convertirse en una herramienta útil para que los CSP demuestren la seguridad de su solución y para que el proveedor de servicios FSSS confíe en el CSP.

Fecha de publicación: 14-02-205

Euralarm
Gubelstrasse 22
CH-6301 Zug (Suiza)

Número de Registro Mercantil Suizo: CHE-222.522.503

E secretariat@euralarm.org
W www.euralarm.org