| | |
|---|---|
| **PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL SERVICIO DE ALOJAMIENTO, COMUNICACIONES Y CIBERSEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE ENRESA**<br><br>EXPTE Nº CO-SI-24-001 | Clave: 000-ES-SI-0188<br><br>Páginas: 50 |

# Índice

| | |
|---|---|
| **PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL SERVICIO DE ALOJAMIENTO, COMUNICACIONES Y CIBERSEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE ENRESA**<br><br>EXPTE Nº CO-SI-24-001 | Clave: 000-ES-SI-0188<br><br>Páginas: 50 |

# 1 Objeto

Este pliego establece las prescripciones técnicas requeridas para la prestación de los servicios de alojamiento, comunicaciones y ciberseguridad de los sistemas de información de Enresa.

# 2 Alcance

Enresa, Empresa Nacional de Residuos Radiactivos, S.A. S.M.E., es la entidad integrada en el sector público institucional encargada de gestionar el servicio público esencial de gestión de los residuos radiactivos y el desmantelamiento y clausura de las centrales nucleares, tal y como establece el Real Decreto 102/2014, de 21 de febrero.

Desarrolla su actividad de acuerdo con lo previsto en el Plan General de Residuos Radiactivos (PGRR), que es revisado periódicamente por el Gobierno y establece las estrategias y líneas de actuación a llevar a cabo en cada momento por la compañía.

Esta actividad se sustenta en procesos de negocio que son soportados por sistemas de información bajo la responsabilidad de la Dirección de Sistemas y Documentación, y que están alojados en infraestructuras ubicadas en Centros de Procesos de Datos (CPD) de Enresa, de terceros o a través de servicios proporcionados en Cloud.

El vigente "X Plan de Sistemas y Tecnologías de la Información de Enresa" recoge la planificación de actividades y proyectos a realizar en el ámbito de las tecnologías de la información en apoyo de las actuaciones previstas para la compañía en el PGRR. Entre otras cosas, el plan requiere:

- Reducir la obsolescencia tecnológica en infraestructuras y sistemas de Enresa, estableciendo mecanismos para asegurar que los sistemas se mantienen actualizados, así como priorizar productos frente a desarrollos a medida.
- Incorporar tecnología que habilite la automatización de tareas, trazabilidad de las actividades, simplificar la gestión, y favorecer la movilidad de los empleados.
- Implantar la estrategia de infraestructuras más adecuada para el contexto de Enresa.
- Garantizar la seguridad de los sistemas de información adecuándose al Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo).

La infraestructura tecnológica de Enresa es compleja en cuanto al número y diversidad de los sistemas que la integran, las particularidades del negocio al que dan soporte, la existencia de distintos centros de trabajo y las condiciones de sus emplazamientos, así como las necesidades técnicas y funcionales en movilidad de los empleados para el correcto desempeño de sus funciones.

En este contexto, para llevar a cabo de forma eficiente la actividad de la organización es necesario disponer de un servicio que permita la adecuada ubicación de los servidores e infraestructuras en Centros de Procesos de Datos (en adelante, CPD) que garanticen el correcto funcionamiento de los sistemas de información de Enresa, y que proporcione las comunicaciones necesarias para permitir la conectividad de los distintos centros de trabajo entre sí, con Internet y con los sistemas de información de Enresa, con independencia de donde se encuentren alojados y desde donde se conecten los empleados, colaboradores o los propios sistemas, proporcionando a su vez las capacidades necesarias para gestionar los riesgos de ciberseguridad que puedan comprometer la confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad de los activos de información de Enresa.

# 3 Actividades

Las actividades del servicio se estructuran en los siguientes sub-servicios, tomando como referencia las funciones y categorías establecidas en el Marco de trabajo para la ciberseguridad del NIST (Instituto Nacional de Estándares y Tecnología), que proporcionan una visión estratégica de alto nivel del ciclo de vida del proceso de gestión de riesgos de la ciberseguridad en una organización:

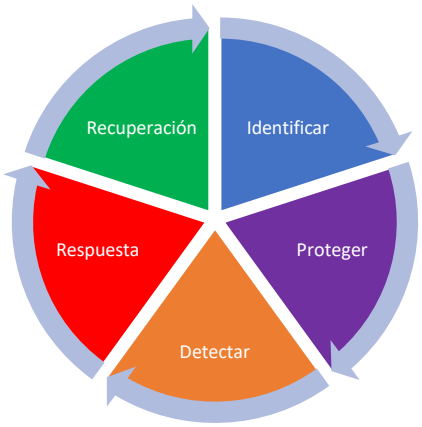



Ilustración 1: Funciones del marco de ciberseguridad NIST

(https://www.nist.gov/cyberframework/framework)

## 3.1 Identificar

Con el objeto de obtener la necesaria compresión de Enresa, para gestionar el riesgo de ciberseguridad de los activos de información de la organización, el contratista realizará las siguientes actividades:

### 3.1.1 Entorno empresarial

En el contexto de la seguridad de la información y de los ciberataques es fundamental conocer la empresa a la que se va a proteger. Por lo tanto, el contratista deberá:

- Adquirir el conocimiento necesario sobre el contexto de Enresa y su negocio, en concreto su objeto, misión y funciones, tipo de organización, marco legal al que está sujeto, estructura organizativa, los proyectos estratégicos que lleva a cabo, principales factores de influencia o dependencias, etc. Este conocimiento específico de Enresa permitirá al contratista interpretar las amenazas al contexto específico de Enresa.
- Conocer la Política de Seguridad de Enresa y los procedimientos que se deriven de ella, para adaptar sus tareas a los mismos. Como parte de la mejora continua y debido al trabajo realizado en este contrato, el contratista propondrá los cambios necesarios o recomendaciones de mejora derivados de los trabajos realizados.
- Conocer las infraestructuras, las aplicaciones de Enresa y su ciclo de vida, las comunicaciones: la red LAN, la red WIFI, las infraestructuras de hiperconvergencia, almacenamiento, backup&restore, Servicios MS 365 Defender, interconexión con Red SARA, etc.

### 3.1.2 Evaluación de riesgos

Enresa, dentro de su proceso de adecuación al ENS, ha identificado los activos de información de la organización, determinado los niveles y categorías de los servicios y sistemas de información según la valoración del impacto que tendría en la organización un incidente de seguridad, plasmando toda esta información en un documento de Inventario de activos categorizado. Posteriormente ha realizado una evaluación o análisis de riesgos de los citados activos de información, valorando las salvaguardas existentes en la fecha de ejecución, cuyos resultados se han recogido en un Informe de Análisis de riesgos, para finalmente recoger las medidas de seguridad que aplican a los activos esenciales identificados y en función del riesgo detectado, formalizándose en el documento de Declaración de aplicabilidad.

A partir de esta información, que Enresa proporcionará al contratista, este con carácter anual realizará una evaluación o análisis de riesgos haciendo uso de la herramienta PILAR (CCN-STIC 470) que implementa la metodología MAGERIT, valorando cualitativamente los activos más valiosos del sistema, cuantificando las amenazas más

probables, valorando las salvaguardas que protegen dichas amenazas en la ejecución, y valorando el riesgo residual (riesgo que permanece en Enresa tras mitigar/reducir o eliminar los riesgos con la implantación de medidas).

Una vez realizado el análisis o evaluación de los riesgos, el contratista deberá proponer la actualización de la Declaración de aplicabilidad de Enresa, conforme la guía CCN-CERT BP/14, que contendrá una relación de las medidas del ENS de aplicación al sistema o subsistemas, elaborando una lista priorizada de las medidas que se deberían de aplicar, ordenadas según el riesgo resultante, y las que tengan que ser modificadas.

Los entregables de esta actividad anual serán:

- Un informe de análisis de riesgos conforme metodología MAGERIT y uso de herramienta PILAR, así como el fichero utilizado en la herramienta.
- Propuesta de actualización de la Declaración de aplicabilidad de Enresa, que incluirá las medidas de seguridad de aplicación, conforme el Anexo II del RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

### 3.1.3 Gestión de Activos y Vulnerabilidades

El contratista deberá proporcionar todos los recursos necesarios, incluidos el hardware, software y las licencias necesarias, para implantar y operar una solución de gestión de activos de información y vulnerabilidades para Enresa, con los siguientes requisitos:

- Capacidad de descubrimiento automático y continuo de activos (Hardware y Software) internos a la organización. La solución deberá ser capaz de identificar cualquier activo TI que se encuentre conectado en las redes de la organización y almacenarlos en una base de datos o inventario de activos.
- Análisis de vulnerabilidades automático sobre los activos internos descubiertos, con una periodicidad de escaneos **mensual**. Las vulnerabilidades detectadas deberán clasificarse en base a su criticidad tomando como referencia el sistema de puntuación CVSS (Common Vulnerability Scoring System), priorizarse en función del riesgo y el impacto para la organización, y comunicar la alerta a Enresa indicando las recomendaciones para su mitigación.
- El contratista junto con Enresa, revisarán la base de datos de activos resultante del proceso de descubrimiento automático de activos, y complementarán si procede con aquellos activos conocidos que no hayan podido descubrirse con el fin de obtener la visión más completa posible de los activos de Enresa.
- El contratista comprobará mensualmente el inventario actualizado de activos con la base de datos de vulnerabilidades publicadas contenida en los estándares CVE (Common Vulnerabilities and Exposures) o NVD (National Vulnerability Database), para que en el caso de identificar vulnerabilidades clasificadas como

críticas, que sean explotables en los activos de información de Enresa y de riesgo elevado.

- El contratista comunicará a Enresa las alertas de vulnerabilidades detectadas, se realizarán conforme los requisitos que se definen en el apartado 3.4.1 "Centro de Operaciones y Soporte".
- El contratista proporcionará una única consola o herramienta con una visión unificada de todos los activos y sus vulnerabilidades asociadas, independientemente de su tipología o ubicación, que sea accesible por personal de Enresa al menos en modo lectura.
- El método de descubrimiento o recolección de información de los activos, así como los mecanismos de escaneo si proceden, podrán ser cualquiera que determine el contratista, considerando que en ningún caso deben ser intrusivo y afectar al rendimiento de los activos o sistemas de información de la organización.
- La solución deberá soportar al menos 1400 activos de información, considerando un activo como una entidad de información que se puede analizar, por ejemplo, un ordenador personal, un servidor, un dispositivo de almacenamiento, dispositivos en red, un smartphone, una máquina virtual, una instancia en la nube, un contenedor, un sistema operativo o una plataforma de software.
- Si el contratista ha asumido el compromiso de incorporar una solución de descubrimiento de superficie de ataque indicando *SI* en la casilla de compromiso del Anexo 5 del PCAP, esta tendrá las siguientes características:

    - Proporcionará todos los recursos necesarios para implantar y operar una solución que soportará al menos 100 activos de información.
    - Tendrá capacidad de descubrimiento automático de los activos de Enresa expuestos a Internet, identificando las conexiones que tengan los activos desde Internet a las redes de Enresa y viceversa, obteniendo una aproximación de la superficie de ataque expuesta a internet de la organización.
    - Se realizará un descubrimiento **semestral** de los activos de Enresa expuestos, realizando un análisis de vulnerabilidades sobre los activos descubiertos.
    - Siempre que sea posible, se integrará la información de los activos expuestos en la misma consola o herramienta que para la gestión de activos internos. Si no es factible, se realizará un informe por cada descubrimiento, identificando los activos descubiertos y las vulnerabilidades asociadas si las hubiese.
    - Toda la operación, mantenimiento y soporte será realizada por el contratista, integrándose dentro de la gestión de activos y vulnerabilidades

del servicio, permitiendo el acceso en modo lectura, para al menos un usuario de Enresa.

## 3.2 Proteger

Con toda la información recogida de la identificación, el contratista deberá realizar las actividades correspondientes a su protección.

### 3.2.1 Alojamiento de los sistemas de información

El contratista proporcionará todos los recursos necesarios, para proveer un espacio técnico de alojamiento para las infraestructuras que soportan los sistemas de Información de Enresa.

#### 3.2.1.1 Centros de Proceso de Datos (CPD) Principal y Secundario

El contratista proporcionará el CPD Principal y el CPD Secundario para Enresa, conforme los siguientes requisitos:

- Los CPD principal y secundario estarán en ubicaciones separadas físicamente a una distancia de **5 km, como mínimo, dentro de la Comunidad de Madrid**.
- Cada CPD dispondrá de una sala técnica, con doble techo y suelo técnico. En cada uno se provisionará un rack para el alojamiento de los servidores, almacenamiento, infraestructura de comunicaciones, de seguridad y cualquier otro que Enresa considere en función de sus necesidades.
- Los racks tendrán un formato de bastidor estándar de 19" y capacidad de 42 "u". Dispondrán de un sistema de control de acceso mediante llave custodiada para garantizar que solo accede al equipamiento de Enresa quien este autorizado para ello.
- El contratista proporcionará todos los elementos necesarios para la correcta instalación del equipamiento (guías, pasacables, bandejas, etc), así como la infraestructura de red necesaria (cableado de cobre o fibra, etiquetas, conversores de medios) para cubrir todas las necesidades de interconexión de todo el equipamiento alojado y con las líneas externas de operadores o comunicaciones de datos. El contratista proporcionará, además, las conexiones y paneles de parcheo para operadores de comunicaciones del servicio o que Enresa disponga.
- En cada rack se habilitarán los circuitos eléctricos necesarios para alimentar los equipos instalados de acuerdo con sus especificaciones. Cada rack dispondrá de doble acometida eléctrica, con al menos dos circuitos totalmente independientes (líneas, cuadros eléctricos y SAIs diferentes). La capacidad eléctrica de estos circuitos deberá ser suficiente para soportar la densidad de equipos máxima en cada rack.
- Los CPD,s deben de estar conectados entre sí por 2 enlaces con las siguientes características:

- 2 conexiones Ethernet de 1 Gb de ancho de banda, 5 ms de latencia máxima y de nivel 2 (tipo Metrolan, MetroEthernet o equivalente), gestionados por el contratista. En ambos extremos Enresa podrá optar por que le sea entregado el enlace en fibra óptica (10GBaseSR) o en cobre (10GBASE-T).

- Las conexiones deben de realizarse por operadores diferentes o caminos físicos diferentes.

- En la reunión de lanzamiento del servicio como plazo máximo, el contratista proporcionará la certificación **Tier II o superior**, que deberá estar en vigor durante toda la vigencia del contrato, expedido por Uptime Institute o en su defecto el contratista acreditará la homologación de los requisitos o capacidades conforme a esta certificación.

### 3.2.2 Comunicaciones de datos

El contratista proporcionará todos los recursos necesarios, para implantar y operar una arquitectura de comunicaciones que soporte todo el tráfico de datos de Enresa.

Las sedes a las que hay que dar cobertura se muestran en la siguiente tabla:

| | Nombre | Dirección | Código Postal | Población | Provincia |
|---|---|---|---|---|---|
| 1 | Sede Madrid | C/Emilio Vargas, 7 | 28043 | Madrid | Madrid |
| 2 | C.A. El Cabril | Carretera A- 447 dirección Fuente Obejuna- Cazalla de la Sierra Km 17, 8 | 14200 | Hornachuelos | Córdoba |
| 3 | C.N. José Cabrera | Carretera de Almonacid - Pastrana | 19118 | Almonacid de Zorita | Guadalajara |
| 3 | C.N. Vandellós I | Central Nuclear | 43891 | Hospitalet de L'Infant | Tarragona |
| 5 | C.N. Santa Mª de Garoña | Santa Maria de Garoña, s/n | 09210 | Valle De Tobalina | Burgos |
| 6(*) | Azure | Nube de Microsoft | - | - | |
| 7(**) | CPD principal | | | | Madrid |
| 8(**) | CPD secundario | | | | Madrid |

*(*) No es una sede física, pero contiene infraestructuras de Enresa que hay que comunicar y proteger.*

*(**) Estos CPD son proporcionados por el contratista para Enresa conforme los requisitos determinados en el apartado 3.2.1.1 "Centros de Procesos de Datos Principal y Secundario"*

- Requisitos de enlaces, anchos de banda y medios físicos

En la siguiente tabla se muestran las necesidades de acceso a Internet que debe de cubrir el proveedor para las distintas sedes desde el punto de vista de numero de enlaces, anchos de banda y medios físicos.

| | Nombre | Medio físico | Ancho de banda |
|---|---|---|---|
| 1 | Sede Madrid | Fibra óptica | 1 Gb |
| | | Fibra óptica | 1 Gb |
| 2 | C.A. El Cabril | Fibra óptica | 100 Mb |
| | | 4G/5G | 75 Mb |
| 3 | C.N. José Cabrera | Fibra óptica | 100 Mb |
| | | 4G/5G | 75Mb |
| 4 | C.N. Vandellos I | Fibra óptica | 100Mb |
| | | 4G/5G | 75 Mb |
| 5 | C.N. Santa Maria de Garoña | 5G | 1 Gb |
| 6 | Azure | Express Route (**) | 200Mb |
| 7 | CPD Principal | Fibra óptica | 1 GB |
| 8 | CPD Secundario | Fibra óptica | 1 GB |

*(*) Si el proveedor no puede garantizar que este enlace vaya por un camino físico diferente desde la sede de Emilio Vargas hacia Internet, deberá contratar un enlace por internet con otros proveedores que garantice camino físico diferente desde la acometida del edificio*
*(**) Esta conectividad se realiza entre el contratista y la nube de Microsoft*

- En el caso de las conexiones de Fibra óptica el ancho de banda será simétrico y garantizado, las conexiones deben ser dedicadas extremo a extremo y no se compartirá el ancho de banda con otros clientes.
- En el caso de las conexiones 4G/5G la velocidad requerida será sólo de bajada, siendo la de subida, la máxima que proporcione la tecnología.
- En el caso de la conexión 5G de la C.N. Santa Maria de Garoña el ancho de banda deberá estar garantizado para todos los usuarios de Enresa. Los usuarios (se estiman aproximadamente un máximo de 60 para esta sede) dispondrán de una SIM la cual asegurará mediate credenciales y claves internas el registro y las comunicaciones en dicha red. Este registro no será público, sólo para las SIM de Enresa. Adicionalmente el proveedor dotará de todos los elementos para conectar a dicha conexión 5G a los Router/firewall de la sede para la conexión de equipos que no disponen de SIM.
- En el caso de las dos fibras de la sede de Madrid estas deben de estar diversificadas, es decir, el proveedor debe de garantizar que el camino de las fibras hacia el proveedor es diferente desde la salida de la sede en la calle Emilio Vargas 7.

- La solución debe contar con capacidad de agregar el ancho de banda de todos los enlaces para cada sede dónde haya más de uno.
- En todas las sedes el proveedor dotará de toda la tecnología y equipamiento necesarios para la conexión de la red de comunicaciones a la red de Enresa.
- El contratista debe de contemplar dentro del alcance de este servicio, posibles cambios en la ubicación de la entrega de las comunicaciones derivados de reestructuraciones físicas de las diferentes sedes. Estos cambios, en caso de ser necesarios, no deben de suponer un coste adicional para Enresa.

- Conexión Azure:
  Enresa tiene firmado con Microsoft un contrato que le permite disponer de una conexión llamada "Express Route" con Azure, que le garantiza un ancho de banda y una estabilidad en la conexión en los servicios que Enresa utiliza en esta nube. Para poder completar esta infraestructura es necesario que el operador realice las tareas necesarias, incluido su coste, que permitan completar este servicio. La comunicación mínima que se debe de garantizar es de 200 Mb simétricos.
- Conexiones red SARA:
  Enresa hace uso de servicios de la red SARA (Sistema de Aplicaciones y Redes para las Administraciones) a través de internet con su ministerio de referencia. El proveedor será el encargado de configurar, mantener estas conexiones con dicha red y garantizar la conectividad de estas.
- Electrónica de red LAN:
  Enresa dispone de una solución de red de área local en todas sus sedes tipo SD-ACCESS del fabricante Cisco. Todos los elementos que formen parte de la solución de comunicaciones y/o seguridad deben de ser compatibles con las soluciones de este fabricante. La solución de este fabricante esta soportada sobre equipos Catalyst de la serie 9000.
- Direccionamiento IP público enresa.es y gestión DNS
  El nombre de dominio a gestionar será: enresa.es y tendrá asignado un pool de 24 direcciones públicas proporcionadas por el contratista, para la resolución de nombres asociados a dicho dominio. Estas direcciones IP públicas serán las utilizadas por los servicios de Enresa, el contratista proporcionará además todas las IP públicas necesarias para dar cobertura al diseño realizado y a la correcta operación del servicio.

### 3.2.3 SD-WAN

El contratista proporcionará todos los recursos necesarios, incluidos el hardware, software y licencias o suscripciones necesarias para implantar y operar una red de área amplia definida por software (SD-WAN) con los servicios de seguridad asociados, que

posibilite el acceso eficiente y seguro desde los distintos centros de trabajo entre sí, con internet y con los sistemas de información de Enresa, con los siguientes requisitos:

- Todo el equipamiento que se proporcione para la solución SD-WAN se debe integrar con la arquitectura de comunicaciones definida en el apartado 3.2.2 "Comunicaciones de datos", siendo dicho equipamiento propiedad del contratista, quien suministrará todos los elementos necesarios para su operatividad y puesta en marcha, tanto desde el punto de vista de licencias software como cualquier otro elemento y accesorios (cables, conectores, adaptadores, transceivers, etc), para dotar de conectividad a la red WAN y hasta los puntos de conexión con las diferentes LAN de Enresa en cada centro de trabajo o sede. Enresa sólo suministrará la corriente eléctrica y los espacios en los racks.
- El contratista proporcionará el servicio SD-WAN a través de Cortafuegos de Generación Futura (NGFW Next Generation FireWall) en **cada sede o centro de trabajo**, **en la nube de Azure, y en el CPD Principal y Secundario de Enresa**, con las siguientes características:
    - Instalación en los Centros de Procesos de Datos o Salas técnicas de Enresa en cada sede o centro de trabajo, de un clúster activo/pasivo de NGFW, con montaje en bastidor estándar de 19", sin superar las 2 "u" de rack por cada dispositivo. Deberá disponer de marca de conformidad CE (Conformité Européenne) e incluir fuente de alimentación redundante para cada dispositivo.
    - Para la nube de Azure, el contratista proporcionará e implantará un único NGFW en formato virtual, indicando los requisitos técnicos necesarios de la máquina virtual que será proporcionada por Enresa a través de su suscripción en Azure.

Enresa requiere establecer para la adecuada protección de los flujos de información de los sistemas de información corporativos y las interconexiones con terceros, una arquitectura de protección perimetral basada en la Arquitectura de protección de perímetro de tipo 6 (APP-6) conforme la Guía de Seguridad de los TIC CCN-STIC 811 "Interconexión en el ENS", por lo que el contratista debe desplegar un intermediario (reverse proxy) entre los dos cortafuegos NGFW que separan las redes externas de las redes internas, sin que exista un tramo directo de red entre ellos.

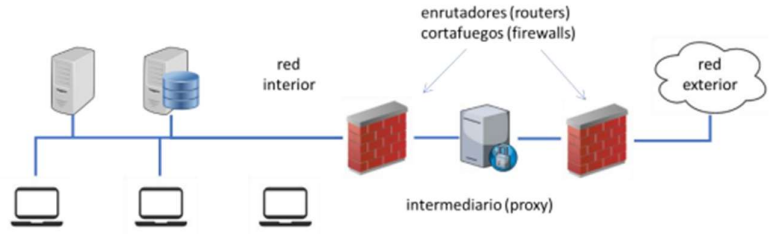



Ilustración 2: Arquitectura de protección de perímetro tipo 6

(https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/521-ccn-stic-811-interconexion-en-el-ens/file.html).

El reverse proxy, dispondrá de las siguientes características:

- Montaje en bastidor estándar de 19", sin superar los 2U en rack, con fuente de alimentación redundante, y capacidad para implementar un clúster activo/pasivo.
- Throughput: 750 Mbps
- Procesamiento SSL por Hardware
- Puertos mínimos 4 GE RJ45, 4 SFP GE y 1 USB
- Protección de ataques en la capa de aplicaciones, de las API (Application Programming Interfaces), y de botnets maliciosos, incluyendo servicios de antimalware avanzado y de día cero con análisis en tiempo real, así como servicios de reputación IP. El contratista proveerá las suscripciones de seguridad necesarias para la correcta operación de las funcionalidades requeridas.

La arquitectura de protección de perímetro tipo 6 se implementará en el CPD Principal (con dos NGFW y un reverse proxy o firewall de aplicación de intermediario) y en el CPD Secundario (con dos NGFW y un reverse proxy o firewall de aplicación de intermediario), que a su vez estarán interconectados para proporcionar alta disponibilidad (en activo/pasivo) y continuidad de los sistemas de información de Enresa.

- Implementación de funcionalidades SD-WAN y de seguridad integradas de forma nativa en una única solución, que proporcione capacidades para gestionar la conectividad a internet, entre sedes y a las aplicaciones o sistemas, a través de los enlaces de acceso a internet existentes en cada sede, conforme los requisitos enunciados en el apartado 3.2.2 "Comunicaciones de datos". La solución soportará las siguientes características:
  - Topología en estrella "hub and spoke" con configuración automática de túneles IPSEC y/o de malla ("full mesh").
  - Mediciones del estado de la conectividad basadas en métricas de calidad del servicio o QoS (tales como pérdida de paquetes, latencia, etc) y control de tráfico ("traffic shaping") que permita el enrutamiento dinámico del tráfico.
  - Conmutación automática de enlace o camino por fallo, rendimiento y/o por prioridad.
  - Gestión centralizada en una única consola, con panel de monitorización y visualización del estado de las redes o enlaces.

- Proporcionar informes detallados del rendimiento de la red SD-WAN en general, y de las aplicaciones empresariales de Enresa en particular, incluyendo las aplicaciones en modalidad de despliegue SaaS (Software como Servicio) que hace uso Enresa, como por ejemplo Office 365.

- El equipamiento NGFW debe incluir al menos los siguientes requisitos **mínimos** en cuanto a su rendimiento:

| REQUISITO | SEDE | MINIMO REQUERIDO |
|---|---|---|
| Número máximo de sesiones TCP concurrentes | MADRID, CPD Principal y Secundario | 800.000 |
| | CABRIL, VANDELLÓS, ZORITA, GAROÑA y Azure | 200.000 |
| Nuevas sesiones TCP por segundo | MADRID, CPD Principal y Secundario | 70.000 |
| | CABRIL, VANDELLÓS, ZORITA, GAROÑA y Azure | 30.000 |
| Throughput de FW de nueva generación (NGFW) con todas las funcionalidades de seguridad activadas | MADRID, CPD Principal y Secundario | 3 Gb/s |
| | CABRIL, VANDELLÓS, ZORITA, GAROÑA y Azure | 1 Gb/s |
| Throughput de FW de Nueva Generación (NGFW) de VPN IPsec | MADRID, CPD Principal y Secundario | 4 Gb/s |
| | CABRIL, VANDELLÓS, ZORITA, GAROÑA y Azure | 1,5 Gb/s |
| Numero de puertos GE RJ45 por dispositivo para conexión con LAN Enresa | MADRID, CPD Principal y Secundario | 4 |
| | CABRIL, VANDELLÓS, ZORITA, GAROÑA y Azure | 2 |

- En cuanto al número de puertos definido como mínimo, el contratista proporcionará el equipamiento con los puertos necesarios para prestar el servicio.

- Además de la funcionalidad principal SD-WAN, cuya suscripción será proporcionada por el contratista, la solución dispondrá de las siguientes características de red básicas:

  - Soporte de protocolos RIP, OSPF, BGP, PPPoE, DHCP y DNS.
  - Soporte Dual Stack IPV4 e IPV6 simultáneamente.
  - Traducción de direcciones de red NAT IPv4 y NAT64
  - Soporte Redes VLAN (IEEE 802.1q), agregación de interfaces (802.1ad) y creación de enlaces LACP para agregación de puertos (802.3ad).

- Capacidad de segmentar la red en interfaces o zonas para aplicación de políticas de seguridad por zonas.

- En cuanto a la seguridad, el equipamiento deberá tener la capacidad de realizar las siguientes funcionalidades mínimas, incluyendo en la solución las suscripciones necesarias para su correcta operación:

  - Visibilidad y control de aplicaciones: Capacidad para identificar las aplicaciones en la red, en lugar de solamente el puerto o protocolo.

  - Visibilidad y control de usuarios: Capacidad para identificar el usuario, independientemente de la dirección IP que tenga, integrándose con los directorios corporativos de la organización (Active Directory y/o LDAP) para aplicación de políticas de seguridad.

    Adicionalmente, tendrá la capacidad de integrarse con otros sistemas y fuentes de repositorios que puedan contener información del usuario, tales como servidores Radius, soluciones de autenticación 802.1x, controladores inalámbricos, etc.

  - Inspección profunda de paquetes, tráfico encriptado y contenido tunelizado: Descifrar y examinar el tráfico para ofrecer visibilidad, control y seguridad granular, aplicando políticas de seguridad.

    Deberá tener la capacidad de descifrar tráfico TLS (incluida la v1.3), SSL y SSH, así como de inspeccionar el contenido del tráfico tunelizado de los protocolos no cifrados: GRE, IPSec no cifrado, GTU-U y VXLAN.

  - Filtrado de paquetes y de archivos: Capacidad de filtrar paquetes con estado en protocolos tales como ICMPv4, ICMPv6, IPv4, IPv6, TCP y UDP.

  - Protección frente a vulnerabilidades: Detectar y prevenir ataques de red contra vulnerabilidades, tanto en sistemas cliente como servidor, contra diferentes exploits y técnicas de evasión.

  - Prevención de amenazas avanzadas conocidas y protección antimalware: Funcionalidad de análisis en tiempo real para la detección y prevención sobre transmisión de malware sobre protocolos http, smtp, imap, pop3 y ftp.

    Protección de malware en línea mediante firmas basadas en carga y análisis de flujos de datos, bloqueando malware conocido y variantes futuras, así como bloqueo de la actividad de comando y control.

  - Auditoria: Funcionalidades de auditoría, que incluya el almacenamiento en el disco duro del equipo, los logs del sistema, de configuración y de los eventos del tráfico y amenazas. Los datos deberán almacenarse al menos durante 30 días.

  - Dispondrá de una API abierta para su integración con herramientas de seguridad de terceros, así como con el sistema gestión de información,

eventos, orquestación y automatización de la seguridad, enunciado en el apartado 4.1.3.2 "Gestión de información y eventos de seguridad".

- Dado que los NGFW van a conformar el core de la arquitectura de comunicaciones y seguridad para Enresa, para garantizar que su funcionalidad de seguridad esta correctamente acreditada, se precisa que todos los modelos de equipamiento de NGFW propuestos deben estar incluidos como producto STIC **cualificado** dentro del Catálogo de Productos y Servicios de Seguridad (CPSTIC) del Centro Criptológico Nacional (Guía de Seguridad de las TIC: CCN-STIC 105) en epígrafe 7.5.3"Cortafuegos" para el tipo ENS Medio o superior, o acreditar documentalmente que se encuentran en el proceso formal de inclusión en el Catálogo. El contratista acreditará este requisito en la reunión de lanzamiento del servicio como plazo máximo.

### 3.2.4 Servicios de anti-DDoS

Proporcionar todos los recursos necesarios, hardware y software, para implantar y operar un servicio gestionado anti-DDoS (anti-ataques de denegación de servicio distribuidos), con las siguientes características:

- Protección para los servicios publicados por cuatro rangos de direcciones IP, a través del acceso a internet en los CPDs Principal y Secundario de Enresa, que consta de dos enlaces de comunicaciones (dos routers de acceso, uno en cada centro de proceso de datos).
- Despliegue de la solución en la infraestructura externa a Enresa.
- La solución monitorizará en 24x7 y analizará la información estadística del tráfico de comunicaciones (netflow/cflowd) a los servicios de Enresa objeto de protección, no permitiéndose la inspección del contenido de las comunicaciones salvo que Enresa lo autorice expresamente.
- Como mecanismo de mitigación, ante un ataque volumétrico, tendrá la capacidad de separar el tráfico malicioso del legítimo, durante al menos 8 horas desde la activación de la mitigación y hasta un máximo de 500 Gbps, permitiendo únicamente el paso de tráfico legítimo y bloqueando o desviando el tráfico malicioso.
- En el supuesto de un ataque de denegación de servicio que implique la activación del mecanismo de mitigación, deberá ser siempre comunicado a Enresa, conforme los requisitos establecidos en el apartado 3.4.1 "Centro de Operaciones y Soporte".
- Se estima la necesidad de disponer de 10 mitigaciones Anti-DDoS durante la ejecución del contrato (con disponibilidad 24x7 en cualquier día del año), que se ejecutarán según las necesidades de Enresa, sin que Enresa quede obligada a la ejecución total de las mismas.

### 3.2.5 Servicios de voz y fax

Proporcionar todos los recursos necesarios, para implantar y operar una arquitectura de comunicaciones que proporcione soporte a todo el tráfico de voz y fax de Enresa, con los siguientes requisitos:

- El esquema de la solución requerida es la siguiente:

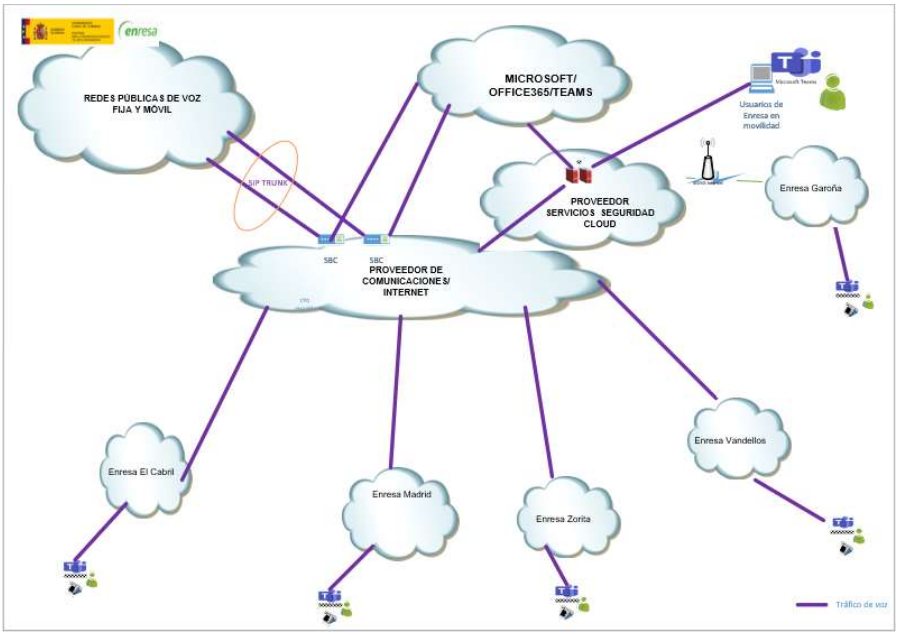



Ilustración 3: Esquema de comunicaciones voz y fax

- La solución de voz fija para comunicación con las redes públicas de voz tanto fija como móvil estará integrada con la solución de Microsoft Teams. Enresa dispone de las licencias necesarias de Microsoft para que los usuarios tengan estas capacidades, concretamente disponemos de Licencias E5 que incorpora licencia de Phone System para todos los usuarios, así como licencias para dispositivos de área común.

  El resto de la infraestructura para conectar Teams con las redes públicas de voz fija y móvil deberá de ser suministrado por el proveedor.

- Los SBC´s que sean necesarios para completar la solución serán ofrecidos por el contratista, siempre en servicios de nube pública o privada, en alta disponibilidad y con enlaces redundantes de voz en distintas localizaciones geográficas. Estos servicios serán totalmente transparentes para Enresa.

- Voz fija/Sip trunk.

Para el dimensionamiento del SIP TRUNK se ha tenido en cuenta la volumetría de usuarios de Enresa y aplicado el estándar de mercado para el cálculo de los canales necesarios. El servicio de telefonía fija prestado deberá estar soportado por dos enlaces SIP Trunk dimensionados cada uno con 90 canales, que garanticen la alta disponibilidad del servicio. El contratista deberá garantizar un bloqueo inferior al 1%.

Las funcionalidades básicas para los servicios de voz fija de Enresa deberán incluir al menos:

- Capacidad para realizar llamadas a cualquier tipo de destino, tanto fijo como móvil, a servicios especiales (100X, 0XY, 118AB), números de emergencia (112) y servicios de red inteligente (90X, 80X).
- Posibilidad de implantar restricciones de llamadas (globales o para una extensión o línea particular): al exterior, nacionales, internacionales, además de una lista de número prefijados, llamadas según horarios, y a servicios de tarificación adicional.
- Portabilidad de la numeración actual al nuevo contratista
- Numeración geográfica
- Volumetrías: El servicio de tarificación de voz estará basado en una tarifa plana. Como referencia, los datos de consumo del año 2022 se pueden ver en la siguiente tabla.

| SEDES | Volumetría | Tránsito nacional | Tránsito a móviles | Tránsito internacional | Tránsito de tarificación especial |
|---|---|---|---|---|---|
| C.A. El Cabril | Llamadas | 3.338 | 7.648 | 7 | 167 |
| | Minutos | 7.197 | 14.697 | 10 | 829 |
| Sede Madrid | Llamadas | 6.841 | 7.510 | 39 | 453 |
| | Minutos | 23.808 | 22.626 | 160 | 2.143 |
| C.N. Vandellós I | Llamadas | 1.100 | 2.468 | 5 | 111 |
| | Minutos | 1.850 | 2.499 | 17 | 429 |
| C.N. José Cabrera | Llamadas | 521 | 1.505 | - | 36 |
| | Minutos | 1.833 | 3.084 | - | 164 |
| C.N. Santa María de Garoña (*) | Llamadas | - | - | - | - |
| | Minutos | - | - | - | - |

(*) En el caso de la C.N. Santa María de Garoña al ser una nueva sede se estima que el consumo habría sido como la de la C.N. José Cabrera.

  - Numeración actual de las sedes

| Localización | Rango DDI | Libres | Ocupadas | TOTAL |
|---|---|---|---|---|
| Sede Madrid | Rango 1 (340 DDIs): 915668100- 915668439 | 96 | 244 | 340 |
| C.A. El Cabril | Rango 1 (200 DDIs): 957575100-957575299 | 48 | 151 | 200 |
| C.N José Cabrera | Rango 1 (57 DDIs): 949750441-949750499)<br>Rango 2 (60 DDIs): 949750540-949750599<br>Rango 3 (60 DDIs): 949750800-949750859 | 97 | 80 | 177 |
| C.N. Vandellós I | Rango 1 (39 DDIs): 977818500-977818538 | 7 | 32 | 39 |
| C.N. Santa María de Garoña | Rango 1 (60 DDI): (*) | 60 | 0 | 60 |
| | TOTAL | 241 | 507 | 749 |

*(*) Garoña actualmente no tiene numeración asignada por lo que la numeración será la que asigne el proveedor*

- Servicio de Fax

La solución de faxes debe de ser una solución en la nube. Estos son los servicios que de fax que actualmente utiliza Enresa, así como su numeración. Estos servicios deben de ser portados al servicio de Fax en la nube que ofrezca el nuevo proveedor.

Sede Madrid: 915668167.
Sede Madrid: 915668186.
C.N. Vandellós I: 977818507.
C.N. José Cabrera: 949750478.
C.A. Cabril: 957575175.
C.A. Cabril: 957575137.
C.N. Santa María de Garoña: *Tendrá una numeración correspondiente al nuevo pool de telefonía que nos asigne el proveedor con numeración perteneciente a la provincia de Burgos.*

### 3.2.6 Navegación segura

El contratista proporcionará todos los recursos necesarios, incluidos el hardware, software y licencias o suscripciones necesarias para 500 usuarios, para implantar y operar una solución de navegación segura y control del tráfico, que posibilite el acceso seguro de los usuarios de Enresa desde cualquier ubicación a los servicios de Internet, a las aplicaciones alojadas en la nube o en los centros de procesos de datos de Enresa, con los siguientes requisitos:

- Adopción de un modelo de servicio de perímetro seguro (SSE Security Service Edge) a través de una arquitectura nativa en la nube del proveedor de la solución que no requiera la adquisición de ningún elemento adicional por parte de Enresa.

- Los usuarios de Enresa, independientemente de su ubicación, para la navegación a Internet se conectarán a la nube del proveedor del servicio SSE, que gestionará la navegación segura hacia cualquier tipo de destino (web, SaaS, IaaS, etc). Para garantizar el acceso eficiente de los usuarios de Enresa, la conexión a la nube del proveedor deberá asegurar unas latencias máximas (con inspección de paquetes) de 10 milisegundos para el tráfico http y un ancho de banda que garantice soportar el ancho de banda agregado de todas las sedes de Enresa hacia internet.
- Con el objeto de asegurar las condiciones de seguridad necesarias sobre los datos que se cursen en el tráfico de Enresa y posibles listas de reputación, no se compartirá infraestructura con ningún otro cliente de la nube del proveedor, así como el direccionamiento IP que se proporcione será dedicado para la solución SSE de Enresa, no permitiéndose compartir direccionamiento público con terceros.
- El contratista proporcionará los clientes software necesarios para 500 usuarios, así como las licencias o suscripciones asociadas. La solución cliente, tendrá las siguientes características:
    - Será desplegado en Ordenadores Personales (incluyendo máquinas virtuales), Smartphones y Tablets, con soporte para al menos los sistemas operativos Windows, MacOS, Android e IoS y mediante herramientas de despliegues centralizadas y automáticas, en el caso de Enresa se utiliza InTune de Microsoft.
    - El agente desplegado en los ordenadores personales será compatible, manteniendo todas sus funcionalidades, con el sistema de protección antivirus del puesto de trabajo (EPP Endpoint Protection Platform) Microsoft Defender for Endpoint, y con la solución “MicroClaudia” del Centro Criptológico Nacional, existentes en los puestos finales de Enresa, así como con el agente necesario para los requisitos establecidos en el apartado 3.3.1 “Detección y respuesta gestionada ante amenazas”.
    - Tendrá la capacidad de realizar la verificación de la identidad del usuario y analizar la evaluación del dispositivo y del contexto (localización, husos horarios, contenido de la información,..) de manera continua (verificación continua de confianza), para aplicar políticas de seguridad basadas en el mínimo privilegio (ZTNA Zero Trust Network Access), como por ejemplo: si el usuario está en la red de Enresa o fuera de la misma, los permisos o grupos del directorio activo a los que pertenece, patrones de comportamiento o contexto del usuario, el nivel de parches del sistema operativo o los requisitos del software antimalware del equipo cliente.
    - Ante posibles problemas con el cliente suministrado por el contratista, éste proporcionará una solución clásica de VPN para la conexión entre las infraestructuras de Enresa.

- Debe soportar el establecimiento de túneles de red privada virtual IPSec/SSL/GRE, desde las sedes de Enresa hacia el servicio SSE haciendo uso del ancho de banda de los enlaces de internet que se dispongan en cada sede, permitiendo forzar que estén siempre activos, así como permitir la división de túneles por el tipo de aplicación.
- Para la autenticación permitirá la integración con los productos de Microsoft AD (Active directory), AAD (Azure active directory) y con las soluciones MFA (Autenticación Multifactor) de dicho fabricante. En general deberá tener en cuenta la evolución tecnológica de este fabricante para la realización de las diferentes integraciones de autenticación cuyo uso en Enresa esta extendido.

- El contratista, en el servicio de navegación segura proporcionará las siguientes funcionalidades de seguridad, incluyendo en la solución las suscripciones necesarias para su correcta operación:
  - Todas las funcionalidades mínimas de seguridad especificadas en el apartado 3.2.3 “SD-WAN” en modalidad Firewall como Servicio (FWaaS).
  - Protección de amenazas avanzadas desconocidas, que incluirá capacidades de análisis estático, dinámico, en sandbox, recursivo y mediante tecnología de aprendizaje automático. Deberá disponer de un servicio de inteligencia de amenazas colectiva que permita el acceso a una amplia fuente de conocimiento, así como recoger, agregar y normalizar Indicadores de Compromiso (IOCs) para su uso en Enresa.
  - Protección de amenazas basados en el acceso a webs, analizando el contenido y bloqueando URLs maliciosas en tiempo real, incluyendo protección contra amenazas de phishing, entregas de kits de exploits o actividades de comando y control.
    La solución dispondrá de un motor de clasificación dinámica de URLs en base a su contenido, y debe permitir crear categorías propias y listados de URLs permitidas o bloqueadas por Enresa.
  - Protección de amenazas DNS (Domain Name System) mediante inspección del tráfico DNS para detectar solicitudes de dominios maliciosos, con capacidad para bloquear y redirigir el tráfico para su análisis y detección de los endpoints o clientes desde donde se realizan las solicitudes a los dominios maliciosos.
- La solución de navegación segura se integrará en la arquitectura de comunicaciones y seguridad del servicio, así como con el sistema gestión de información, eventos y automatización de la seguridad, enunciado en el apartado 3.3.2 “Gestión de información y eventos de seguridad”.

### 3.2.7 Protección del dato y aplicaciones en la nube

El contratista deberá proporcionar todos los recursos necesarios, incluidos el hardware, software y licencias o suscripciones necesarias, para implantar y operar una solución de protección de los datos que se gestionan en los procesos de negocio en Enresa, y que se gestionan en aplicaciones en la nube desplegadas en modalidad Software como Servicio (SaaS), con los siguientes requisitos:

- Analizar el tráfico de navegación de los usuarios de Enresa para el descubrimiento y detección de forma automática de las aplicaciones y servicios en la nube que hacen uso los usuarios de Enresa, tanto aquellas que sean corporativos y preautorizados (por ejemplo, MS Office 365, Exchange Online y Teams) como aquellas no autorizadas por defecto (Shadow IT). Para el cumplimiento de este requisito, la solución deberá integrarse con la solución de navegación segura, enunciada en el apartado anterior.
- Proporcionar visibilidad de la actividad de los usuarios de Enresa en las aplicaciones SaaS que hace uso, analizando las acciones y los datos que se intercambian, para que aplicando políticas de seguridad se pueda alertar o bloquear una acción que suponga un riesgo de seguridad para Enresa. Los datos deberán retenerse en la plataforma por un plazo mínimo de 30 días, con disponibilidad para su análisis por parte del servicio.
- Incluir un sistema de indicadores de la valoración de posibles riesgos de las aplicaciones en la nube y la actividad realizada por los usuarios de Enresa.
- Identificar, clasificar, inspeccionar y bloquear los datos confidenciales o sensibles en tránsito entre los usuarios y las aplicaciones en la nube, incluyendo los datos que se cursen cifrados por protocolos SSL/TLS, así como la inspección de datos ocultos y metadatos en ficheros ofimáticos.
- La solución dispondrá de perfiles precargados de identificación de información orientados al cumplimiento de la normativa de protección de datos de carácter personal en la Unión Europea (REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)) parametrizados al idioma castellano.
- Permitirá la creación de nuevos identificadores, perfiles o casos de uso personalizados y adaptados al contexto especifico de Enresa.
- La solución se integrará en la arquitectura de comunicaciones y seguridad del servicio, así como con el sistema gestión de información, eventos y automatización de la seguridad, enunciado en el apartado 3.3.2 “Gestión de información y eventos de seguridad”.

### 3.2.8 Protección de Accesos Privilegiados

El contratista deberá proporcionar todos los recursos necesarios, incluidos el hardware, software y licencias o suscripciones necesarias, para implantar y operar una solución de gestión de los accesos privilegiados (PAM - Privileged Access Management) a las infraestructuras y sistemas de información de Enresa, con los siguientes requisitos:

- Se considerarán accesos privilegiados aquellos que proporcionan un alto nivel de permisos a recursos TI (aplicaciones, software o hardware, con independencia de si se encuentran desplegados sobre entornos locales, en la nube o híbridos) de Enresa a través de cuentas privilegiadas o de administración. Estas cuentas pueden corresponder a una persona física o no, como las cuentas que utilizan las aplicaciones para ejecutar servicios o comandos que requieren permisos especiales.
- El contratista realizará un análisis previo, tal y como se detalla en la fase de ejecución del servicio, de la situación actual de la gestión de accesos privilegiados de Enresa, mediante reuniones de trabajo con el personal técnico de Enresa que les facilitarán la información disponible sobre los procesos existentes, el entorno tecnológico actual y los requisitos de los sistemas a integrar, para realizar el diseño técnico y funcional de la solución.
- La solución estará dimensionada para su uso por 25 administradores y sin límite de credenciales o privilegios de administración ni recursos TI.
- La solución se desplegará en un modelo de Software como Servicio (SaaS) que no requiera la adquisición de ningún elemento adicional por parte de Enresa, y tendrá las siguientes capacidades:
    - Descubrimiento automático de cuentas privilegiadas existentes en los sistemas, dispositivos o aplicaciones de Enresa.
    - Almacén seguro de credenciales cifradas, con el objeto de preservar la confidencialidad e integridad de las credenciales asociadas a las cuentas privilegiadas.
    - Implementación de políticas de contraseñas, permitiendo generar, actualizar y rotar las credenciales de las cuentas privilegiadas.
    - Control de acceso a los recursos TI gestionados a través de cuentas privilegiadas basado en políticas de seguridad y/o autenticación multifactor.
    - Auditoria de usuarios privilegiados, mediante el aislamiento y monitorización de las sesiones de usuarios privilegiados en tiempo real, registrando la actividad en un almacén seguro junto con los eventos de auditoría propios del sistema durante al menos 30 días, permitiendo alertar o suspender automáticamente las sesiones sospechosas de actividades privilegiadas anómalas. Los registros de auditoría deberán incorporar una fuente de tiempo fiable o timestamping.

  - Generación de informes sobre las cuentas privilegiadas, recursos a los que acceden y actividad significativa.
  - Respaldo en copia de seguridad de toda la información necesaria para el restablecimiento de la solución completa ante una incidencia.
- La administración del servicio será realizada por el contratista. Si bien Enresa tendrá la capacidad de acceder de manera autónoma al menos a las funciones de auditoría y generación de informes.
- Integración con las siguientes herramientas de gestión y control de accesos: Windows AD, Azure AD, Azure AD Authenticator o Microsoft Entra, CiscoDNA Center, VMWAre y RADIUS, así como con los Firewalls de Nueva Generación que se incluyan en el servicio conforme el apartado 3.2.2 "SD-WAN", y con el sistema de gestión de información, eventos y automatización de la seguridad, enunciado en el apartado 3.3.2 "Gestión de información y eventos de seguridad".

## 3.3 Detectar

El contratista desarrollará e implementará las medidas técnicas adecuadas para identificar que un evento ha ocurrido, asegurándose que los servicios o sistemas a desplegar registrarán las actividades de los usuarios, sin que se realice su perfilado, únicamente almacenando la información necesaria para monitorizar, analizar, investigar y documentar los eventos relacionados.

### 3.3.1 Detección y respuesta gestionada ante amenazas

El contratista proporcionará todos los recursos necesarios, incluidos el hardware, software y licencias o suscripciones necesarias, para implantar y operar una solución de Detección y respuesta gestionada ante amenazas (MDR Managed Detection and Response) para los equipos de usuario y servidor (endpoints) y para las redes corporativas de Enresa, con los siguientes requisitos:

- La solución integrará las capacidades de detección y de respuesta ante amenazas en los ámbitos de los endpoints (EDR Endpoint Detection and Response) y de las redes (NDR Network Detection and Response) de Enresa, en una única solución, es decir, se podrán usar distintas herramientas o soluciones para cada ámbito, pero se deberán integrar todas ellas en una única base de datos accesible a través de una única consola que permita agregar y correlar toda la información de los eventos en tiempo real de ambos entornos para que se puedan detectar automáticamente las amenazas, clasificarlas, y permitir realizar su gestión y respuesta.
- Toda la información de los eventos se guardará en tiempo real en un sistema de almacenamiento proporcionado por el contratista y disponible durante al

menos 30 días para la realización de investigaciones, búsqueda de amenazas o análisis forenses.

- La solución, que deberá permitir el traspaso de información con otros sistemas de Enresa, soportará al menos los formatos Syslog, Bases de datos MSSQL, Netflow, Windows Events, HTTP, Listener o XDR Collectors. Todas las comunicaciones necesarias para la comunicación de la información de los eventos de seguridad serán cifradas.
- La solución proporcionará informes y un cuadro de mando, que incluya puntuación de riesgo de las amenazas. Además, la solución debe comunicar alertas debidas a la detección en tiempo real de amenazas por correo electrónico.
- La solución permitirá realizar automatizaciones de tareas y respuestas automáticas en base a los criterios de detección y respuesta ya determinados.
- La solución se deberá integrar en la arquitectura de comunicaciones y seguridad del servicio, así como con el sistema gestión de información, eventos y automatización de la seguridad, enunciado en el apartado 3.3.2 “Gestión de información y eventos de seguridad”.
- La solución para el ámbito de los endpoints debe cumplir los siguientes requisitos mínimos (EDR):
    - Debe ser una solución nativa en cloud, que no requiera instalación de ningún elemento físico o virtual en las infraestructuras de Enresa, salvo la instalación de un único agente de software en cada elemento de puesto de usuario o servidor.
    - El contratista proporcionará los agentes software necesarios para 1500 endpoints, así como las licencias o suscripciones asociadas.
    - Los endpoints, tendrán las siguientes características:
        - Soporte para al menos los sistemas operativos Windows, Linux, MacOS, Android e IoS, y compatibilidad para infraestructuras físicas y virtuales.
        - Capacidad para despliegue y actualización mediante herramientas de despliegues centralizadas y automáticas (InTune) sin necesidad de interrupción de la actividad del endpoint y sin la intervención del usuario.
        - Compatibilidad, manteniendo todas sus funcionalidades, con el sistema de protección antivirus del puesto de trabajo (EPP Endpoint Protection Platform) Microsoft Defender for Endpoint, y con la solución “MicroClaudia” del Centro Criptológico Nacional, existentes en los puestos finales de Enresa, así como con el agente necesario para los requisitos establecidos en el apartado 3.2.6 “Navegación segura”.

- La solución debe ser capaz de agrupar host basados en identificadores de host, OU de Active Directory o etiquetas para la aplicación de políticas.
- La solución soportará las siguientes funcionalidades, incluyendo en la solución las suscripciones necesarias para su correcta operación:
  - Prevención de amenazas en el endpoint, mediante técnicas de aprendizaje automático previas a la ejecución de malware conocido y desconocido (zero-day).
  - Protección de conexiones con dispositivos externos del endpoint (USB, Unidades de disco, etc) mediante aplicación de políticas de seguridad.
  - Protección de los datos, con funcionalidad de Cifrado de disco compatible con BitLocker para Windows y FileVault para macOS y control de conexiones mediante firewall de host.
  - Detección basada en análisis de comportamiento e inteligencia de amenazas posterior a la ejecución de un malware.
  - Prevención mediante bloqueo de técnicas de explotación de software vulnerable.
  - Generación de listas dinámicas con Indicadores de Compromisos (IOCs) que puedan ser distribuidos y orquestados por los NGFW del servicio.
  - Capacidades de respuesta automática para gestionar los procesos en ejecución y el sistema de ficheros, de modo que se pueda bloquear ficheros, ponerlos en cuarentena, ejecutar scripts, terminar la ejecución de procesos involucrados en una amenaza o aislar un endpoint y evitar la comunicación con el resto.

- Para el ámbito de las redes corporativas de Enresa (NDR) el contratista la deberá integrar en la solución de MDR, en concreto:
  - Integrará la información de los NGFW del servicio requeridos en el apartado 3.2.3 “SD-WAN”, que incluyen funcionalidades de análisis e inspección del tráfico de red, así como protección frente a vulnerabilidades, antimalware y prevención de amenazas avanzadas conocidas.
  - Incluirá toda la información sobre protección de amenazas avanzadas desconocidas, amenazas basadas en el acceso a webs y amenazas DNS, tal y como se detalla en la solución SSE requerida en el apartado 3.2.6 ”Navegación segura”.

- Incorporará la protección de los datos y aplicaciones en la nube que se usan en Enresa, tal y como se especifica en el apartado 3.2.7 "Protección del dato y aplicaciones en la nube".

- Si el contratista ha asumido el compromiso de incorporar una solución de análisis de tráfico de red indicando *SI* en la casilla de compromiso del Anexo 5 del PCAP, esta tendrá las siguientes características:

  - Proporcionará todos los recursos necesarios para implantar y operar una solución que soportará al menos 1000 direcciones IP de las redes de Enresa.
  - Tendrá capacidad de analizar de manera pasiva, mediante copias de tráfico (mirror) y sin necesidad de desplegar agentes de software, el tráfico IP de las redes de Enresa en todas sus sedes, y buscar amenazas mediante mecanismos de inteligencia artificial basados en patrones de comportamiento.
  - Podrá ejecutar respuestas autónomas para bloquear un equipo o usuario ante una posible amenaza.
  - Toda la operación, mantenimiento y soporte será realizada por el contratista, integrándose dentro de la Detección y respuesta gestionada ante amenazas del servicio, permitiendo el acceso en modo lectura, para al menos un usuario de Enresa.

La solución MDR debe proporcionar capacidad para realizar investigaciones o búsquedas proactivas de amenazas (threat hunting) que no han sido detectadas con las medidas de seguridad del servicio de comunicaciones y seguridad, es decir son actividades proactivas que se inician sin una alerta o amenaza asociada.

El contratista realizará un proceso iterativo de threat hunting, con un máximo de 4 anuales, basándose en el siguiente proceso:

- Crear una hipótesis o supuesto de ataque o amenaza, que podrá ser formulada en base a una biblioteca de amenazas, como por ejemplo la matriz ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) de MITRE, o en base a indicadores de compromiso o de ataque en función del contexto de cada momento.
- Procesar, correlacionar y analizar los datos almacenados en el MDR y generados por los endpoints y las redes de Enresa, con el fin de identificar y caracterizar tácticas, técnicas y procedimientos utilizados por las amenazas.
- Automatizar mediante herramientas o algoritmos los datos encontrados para enriquecer el proceso en próximas iteraciones.
- En el supuesto de que se detecte una posible amenaza, se seguirán los mecanismos definidos en el apartado 3.4.1.3 "N3 Gestión de ciberincidentes".

- Generar un documento con la información del proceso, indicando los hallazgos existentes y su severidad, y la forma de detección en el sistema.

### 3.3.2 Gestión de Información y eventos de seguridad

El contratista proporcionará todos los recursos necesarios, incluidos el hardware, software y licencias o suscripciones necesarias, para implantar y operar un sistema de gestión de eventos de seguridad (SIEM Security Information and Event Management), que permita la monitorización, análisis y respuesta automática de eventos de seguridad en los servicios e infraestructuras de Enresa, de acuerdo con los siguientes requisitos:

- La solución se desplegará en un modelo de Software como Servicio (SaaS), o en las infraestructuras del contratista, de modo que en ningún caso requiera la adquisición de ningún elemento adicional por parte de Enresa.
- La solución recolectará los eventos de seguridad de todas las herramientas proporcionadas por el contratista en el servicio, así como de las soluciones de identidad, comunicaciones o seguridad que disponga Enresa, directamente o través de terceros. En particular deberá integrar los eventos de:
    - Toda la suite de soluciones de Microsoft 365 Defender
    - Controladores de Dominio Active Directory y Azure Active Directory.
    - Cisco Identity Services Engine.
    - Cisco Wireless.
    - Aquellos que pueda ir incorporando Enresa durante la ejecución del servicio.
- El sistema debe estar dimensionado para:
    - Gestionar todos los eventos (eventos por segundo, EPS) que generen las herramientas proporcionadas y gestionadas por el contratista dentro del alcance del servicio.
    - Incluir, además, hasta un máximo de 300 EPS de fuentes no gestionadas directamente por el contratista en el servicio de alojamiento, comunicaciones y ciberseguridad.
    - Almacenar los eventos durante al menos 30 días para su acceso inmediato, y realizar una copia de seguridad o almacenamiento secundario, garantizados mediante firma y sellado de tiempo, que permita disponer los datos durante al menos 180 días para realizar investigaciones sobre posibles incidentes o análisis forenses.
- La solución SIEM del contratista permitirá el procesado, el establecimiento de una correlación y análisis automatizado de todos los eventos de seguridad registrados, para generar alertas en tiempo real.
- La solución tendrá capacidades de SOAR (Security Orchestration Automation and Response) para automatizar de forma coordinada las actividades de respuesta ante un incidente.

### 3.3.3 Monitorización de la infraestructura de comunicaciones y ciberseguridad

El contratista proporcionará todos los recursos necesarios, incluidos el hardware, software y licencias o suscripciones necesarias, para implantar y operar una solución de monitorización de la infraestructura de comunicaciones y ciberseguridad desplegada en el servicio, con el objetivo de detectar de forma temprana cualquier fallo o degradación de cualquier elemento del servicio.

Si el contratista ha asumido el compromiso de incorporar una solución de monitorización de experiencia de usuario indicando *SI* en la casilla de compromiso del Anexo 5 del PCAP, esta tendrá las siguientes características:

- Proporcionará todos los recursos necesarios para implantar y operar una solución con un alcance de hasta un máximo de 500 usuarios.
- Proporcionará visibilidad y métricas de rendimiento para el tráfico que curse un usuario determinado, independientemente de su ubicación, a las aplicaciones corporativas, a las aplicaciones en la nube o navegando por internet.
- Deberá tener capacidad de parametrización de pruebas sintéticas desde un puesto de trabajo a una aplicación, monitorizando todos los segmentos de red por los que pasa el tráfico.
- Toda la operación, mantenimiento y soporte será realizada por el contratista, integrándose dentro de la Monitorización de la infraestructura de comunicaciones y ciberseguridad del servicio, permitiendo el acceso en modo lectura, para al menos un usuario de Enresa.

## 3.4 Respuesta y Recuperación

El contratista desarrollará e implementará las medidas adecuadas respecto a un incidente con el objetivo de reducir el impacto y restablecer las capacidades o servicios que se hayan visto afectados.

### 3.4.1 Centro de Operaciones y Soporte

El contratista proporcionará un servicio unificado de Centro de Operaciones y Soporte que agregue, de forma integral, todas las funciones de soporte y mantenimiento del alojamiento, un centro de operaciones de comunicaciones (NOC Network Operation Centre) y un centro de operaciones de ciberseguridad (Ciber SOC Security Operation Centre).

La prestación del servicio del Centro de Operaciones y Soporte se realizará en español y desde ubicaciones situadas en la Unión Europea.

El Centro de Operaciones y Soporte realizará un enfoque de servicio basado en buenas prácticas ITIL (Information Technology Infrastructure Library) y ejecutará actividades que se detallan en los siguientes puntos.

#### 3.4.1.1 N1 Primer nivel de Operación y Soporte

Este servicio es el punto de contacto técnico centralizado para la gestión de todos los eventos (incidencias, peticiones, consultas, cambios y problemas) relacionados con el servicio de alojamiento, comunicaciones y ciberseguridad proporcionado a Enresa, se encargará de su recepción y registro hasta su resolución.

El servicio se prestará en modalidad 24x7 los 365 días del año.

#### 3.4.1.2 N2 Segundo nivel de Operación y Soporte

Este servicio realizará todas las tareas de soporte funcional y técnico para todas las soluciones y la infraestructura tecnológica asociada con el servicio, incluyendo su completa operación. Este servicio incluirá la realización de las siguientes actividades:

- Servicio de **manos remotas,** en modalidad 24x7, sobre la infraestructura alojada en los CPDs Principal y Secundario de Enresa, para realizar acciones y comprobaciones básicas del equipamiento:
    - Chequeos de indicadores luminosos
    - El cableado entre puertos de equipos y/o paneles de parcheo.
    - El etiquetado de equipos y cables.
    - El reinicio físico de los servidores.
    - La inserción o extracción de dispositivos de almacenamiento.
    - La realización de tareas de baja complejidad guiadas por el personal de Enresa o quién este designe.
- Gestión de los requisitos determinados en el apartado 4.1.5. “Soporte y mantenimiento”
- Gestión de peticiones y cambios, que engloba la gestión de solicitudes de información y cualquier otra necesidad relacionada con las infraestructuras y sistemas del servicio, así como las solicitudes de cambio motivadas por el mantenimiento evolutivo o por necesidades de Enresa.
  Incluye todas las tareas relacionadas con la implantación y puesta en marcha, conforme los requisitos determinados en el apartado 4.1.3 “Instalación y puesta en marcha”.
- Gestión de incidencias y problemas, que incluye la gestión del mantenimiento correctivo ante cualquier incidente en las soluciones e infraestructuras del servicio, con el principal objetivo de restablecer cuanto antes el funcionamiento normal del servicio.
  Cuando una o varias incidencias se conviertan en recurrentes o exista un fuerte impacto en el servicio de comunicaciones y ciberseguridad, se tratará como un problema, debiéndose analizar la causa raíz que subyace y poner los medios para su resolución efectiva.
- El servicio deberá gestionar una base de datos de conocimiento con el objeto de almacenar y compartir la información y que esté disponible para su análisis

y facilitar la toma de decisiones. Como parte de estas tareas, también se incluye la generación de toda aquella documentación técnica, manuales, procedimientos de operación o cualquier otra documentación adicional que se considere necesario realizar para garantizar la calidad en el servicio prestado.

#### 3.4.1.3 N3 Gestión de ciberincidentes

Cuando una incidencia de seguridad no sea resuelta por el nivel anterior se escalará al servicio de gestión de ciberincidentes. Este servicio realizará un análisis especializado para determinar las siguientes tareas:

- Análisis y selección de las evidencias y su custodia.
- Descripción detallada del incidente, incluyendo toda la información relevante. A modo de ejemplo:
    - Identificador o código único de la alerta o incidente
    - Prioridad requerida
    - Código MITRE
    - Análisis detallado del evento de ciberseguridad
    - Fuente de detección y evidencias
    - Sistemas y/o usuarios afectados
    - Origen de la amenaza, análisis de las IP/Dominios/Usuarios implicados.
    - Riesgos e impacto en los sistemas de Enresa.
    - Posibles relaciones con otros ciberincidentes detectados.
    - Escenario hipotético de ciberataque si aplica.
- Verificación del incidente por sus medios propios para determinar si es un incidente o un falso positivo. En caso necesario se pondrá en contacto con el Centro de Soporte al Usuario (CAU) de Enresa para solicitar información o pedir que ser realicen las acciones necesarias para su verificación. Se realizará un plan de acción para verificar el incidente, contenerlo, mitigarlo y recuperar los sistemas afectados.
- En caso de que sea un incidente:
    - Elaborará planes de respuesta y recuperación (playbooks), que serán aprobados por el técnico de seguridad de Enresa, para remediar de manera automática los incidentes de ciberseguridad conocidos.
    - Notificará el incidente mediante la herramienta “LUCIA” (Listado Unificado de Coordinación de Incidentes y Amenazas) del Centro Criptológico Nacional (CCN). La solución será puesta a disposición por Enresa, y accesible vía web por el contratista, que será el encargado de la operación para el servicio.

- Enresa, dependiendo de la criticidad o tipo de incidente, solicitará al contratista un informe post-incidente, no es un análisis forense, con el detalle del proceso de detección, gestión y respuesta.

#### 3.4.1.4 N4 Respuesta especial de emergencia ante Ciberincidentes

Ante un ciberincidente, Enresa puede pedir al contratista la activación de un nivel especial de respuesta con las siguientes características:

- Asignación de un rol de gestor, encargado de gestionar el incidente hasta su finalización, siendo el punto de contacto para las comunicaciones con Enresa, así como de coordinación con los equipos y analistas implicados.
- En función de la naturaleza del incidente, se asignará un equipo multidisciplinar de expertos (malware, ramsonware, inteligencia de amenazas, hunters, etc) que realice el análisis y proporcione una **guía de contención** para detener la propagación del ataque y evitar que se produzcan más daños en los sistemas de Enresa o posibles exfiltraciones de datos.
- Una vez contenido el ataque, se propondrá una estrategia para la erradicación o mitigación definitiva del incidente, proporcionando asistencia en el proceso de recuperación de los sistemas al estado anterior al incidente y que la operación vuelva a la normalidad.
- Elaboración de informe técnico del proceso realizado en la respuesta de emergencia, desde la situación inicial hasta la finalización del incidente.
- Apoyo y asesoramiento legal sobre posibles procedimientos de respuesta al incidente respecto al cumplimiento normativo, incluyendo los relativos a la protección de datos personales.

Se estima la necesidad de disponer de 10 jornadas de trabajo de 8 horas durante la ejecución del contrato, que podrá ser activada en cualquier momento (365 días, 24x7) y que se ejecutarán a demanda según las necesidades de Enresa, sin que Enresa quede obligada a la ejecución total de las mismas.

#### 3.4.1.5 N5. Análisis forense digital

Para cualquier intento de ciberataque, exitoso o no, Enresa podrá solicitar la realización de un análisis forense digital que a incluya todos los medios técnicos y personales necesarios, para realizar las siguientes actividades:

- Análisis y validación del incidente: recopilación de evidencias preliminares, señales de ataque, acciones realizadas y contextualización de las amenazas.
- Preservar las evidencias mediante el clonado digital o las técnicas que sean necesarias, para asegurar su validez legal y la trazabilidad de la cadena de custodia.

- Análisis de las evidencias y artefactos para identificar capacidades (vectores de entrada, técnicas de ofuscación, métodos de propagación, técnicas de exfiltración, etc).
- Obtención de indicadores de compromiso (IoC) y conocimiento de contramedidas de mitigación.
- Evaluación del alcance del compromiso, establecer posibles relaciones de compromiso con otros activos, movimientos laterales, escalada de privilegios o cualquier otro indicio de presencia de actores adicionales maliciosos.
- Elaboración de un informe técnico forense, que realice una exposición detallada del análisis efectuado, describiendo la metodología, técnicas y hallazgos del análisis.

Los análisis forenses digitales realizados por el contratista deben asegurar los requisitos formales necesarios para poder ser utilizados en un procedimiento judicial ante hechos ilícitos o delictivos relacionados con el incidente de ciberseguridad.

Se estima la necesidad de disponer de 10 jornadas de trabajo de 8 horas de duración (en jornadas de lunes a viernes) durante la ejecución del contrato, que se ejecutarán a demanda según las necesidades de Enresa, sin que Enresa quede obligada a la ejecución total de las mismas.

### 3.4.2 Continuidad del servicio

El contratista deberá evitar que las amenazas que se materialicen en su entorno se trasladen a Enresa o a sus proveedores, a través del servicio contratado.

Adicionalmente, Enresa dispone de un Plan de Continuidad de Negocio o TIC, en adelante PCN, que será actualizado con la nueva arquitectura con la participación del contratista.

El Plan de Continuidad de Negocio de Enresa, incluirá:

- Un plan de respaldo, que contempla las medidas implantadas antes de que se materialice una amenaza, y entre las que se encuentra la arquitectura de comunicaciones y seguridad a implantar, mantener y operar por el servicio de alojamiento, comunicaciones y ciberseguridad.
- Un plan de crisis, que define la secuencia de actividades necesarias desde la materialización de un incidente hasta la toma de decisiones para su resolución, en el que participará activamente el contratista, como equipo de soporte y continuidad.
- Un plan de recuperación, que, en función de la naturaleza del incidente y servicios afectados, establece los escenarios de indisponibilidad y planes de recuperación asociados, donde el Centro de Operaciones y Soporte tendrá que definir, probar y llegado el caso, realizar las actividades planificadas dentro del alcance del servicio.

Una vez actualizado el PCN, el contratista:

- Colaborará en el proceso de actualización del PCN y los procedimientos técnicos asociados en base a los cambios que se puedan producir en la nueva arquitectura de comunicaciones y seguridad implantada.
- Realizará hasta un máximo de 6 simulacros durante la ejecución del contrato.
- Definirá y diseñará de al menos un escenario de indisponibilidad basados en un ciberataque durante la ejecución del contrato.
- Participará en la operación del PCN por su activación, cuantas veces sean necesarias durante la ejecución del contrato, en modalidad 24x7.

# 4 Requisitos del servicio

### 4.1.1 Arquitectura técnica de comunicaciones y seguridad

El contratista debe adecuar el diseño especificado a la siguiente arquitectura, dando respuesta a las actividades demandadas en el apartado 3 “Actividades”.

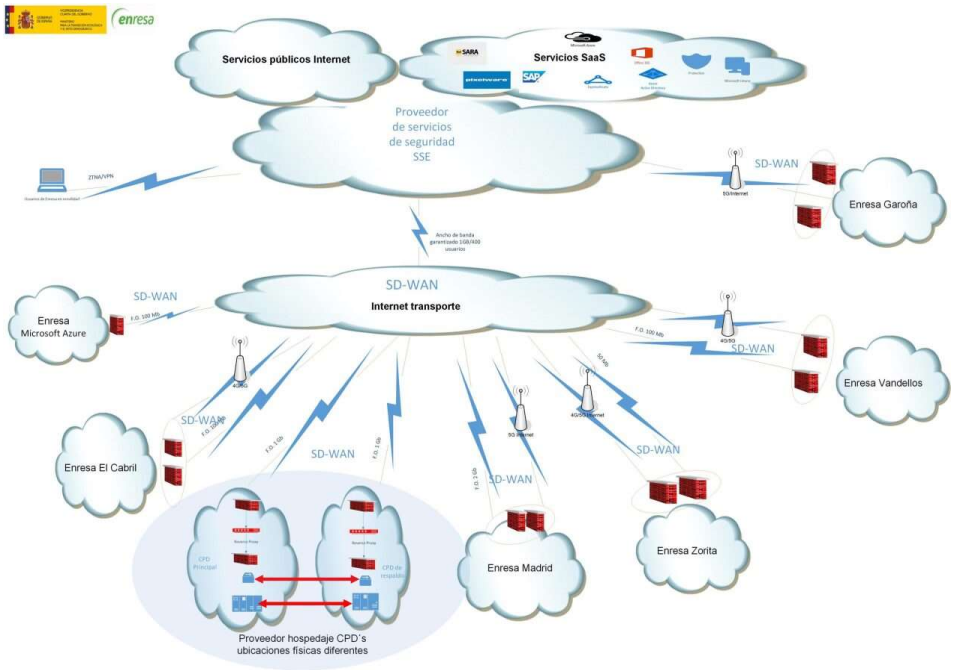



Ilustración 4: Esquema de arquitectura técnica de comunicaciones y seguridad.

La arquitectura debe garantizar la compatibilidad e integración de todos los elementos y soluciones que lo compongan. Con el objeto de garantizar que la integración sea completa y eficaz, así como permitir la reducción de los tiempos de despliegue y mantenimiento, facilitar la administración y operación, simplificar la aplicación de políticas o tareas y optimizar la respuesta automatizada en caso de incidentes, se requiere que todas las soluciones que dan soporte a los servicios que a continuación se indican formen **una única plataforma integral del mismo fabricante**:

- Apartado 3.2.3 "SD-WAN" (excepto el Reverse Proxy).
- Apartado 3.2.6 "Navegación segura"
- Apartado 3.2.7 "Protección del dato y aplicaciones en la nube"
- Apartado 3.3.1 "Detección y respuesta gestionada ante amenazas"

### 4.1.2 Traslado y acondicionamiento de equipamiento actual

El contratista deberá realizar un inventario de las conexiones existentes de los equipos de los racks de Enresa. Deberá asumir la desinstalación (quitar cables y desmontaje de los equipos) y su traslado (completamente embalados y contando con un seguro ante posibles daños) a las salas técnicas objeto del contrato desde las instalaciones actuales de Enresa, ubicadas en el área metropolitana de Madrid. Una vez en las salas técnicas objeto del contrato procederá a la instalación (montaje y alimentación), al cableado y al etiquetado de todos los equipos de acuerdo con el inventario realizado previamente. La desinstalación, traslado y montaje se planificará en la primera reunión una vez iniciado el servicio, y siempre se realizará en horario no laboral (fin de semana) para evitar cortes en el servicio.

Enresa dispone actualmente de dos racks ubicados en 2 CPD´s (uno en cada uno) en las siguientes direcciones:

- Calle Emilio Vargas 7, 28043 Madrid (en adelante CPD Sede)
- Calle de Yecora 4, 28022 Madrid (en adelante CPD GS)

El equipamiento con el origen y destino que debe de ser trasladado se encuentra en la siguiente tabla:

| Equipo | Rack origen | CPD destino |
|---|---|---|
| Cisco DN2-HW-APL | CPD Sede | CPD principal |
| Cisco HX-FI-6332-16UP | CPD Sede | CPD principal |
| Cisco HX-FI-6332-16UP | CPD Sede | CPD principal |
| Cisco HXAF240C-M5SX | CPD Sede | CPD principal |
| Cisco HXAF240C-M5SX | CPD Sede | CPD principal |
| Cisco HXAF240C-M5SX | CPD Sede | CPD principal |
| Cisco HXAF240C-M5SX | CPD Sede | CPD principal |

| Equipo | Rack origen | CPD destino |
|---|---|---|
| Cisco C9300-24P | CPD Sede | CPD principal |
| Quantum Scalar i3 + Expansión (6U) | CPD Sede | CPD secundario |
| Cisco HX-FI-6332-16UP | CPD GS | CPD secundario |
| Cisco HX-FI-6332-16UP | CPD GS | CPD secundario |
| Cisco HXAF240C-M5SX | CPD GS | CPD secundario |
| Cisco HXAF240C-M5SX | CPD GS | CPD secundario |
| Cisco HXAF240C-M5SX | CPD GS | CPD secundario |
| HP PROLIANT DL385 G7 | CPD Sede | CPD secundario |
| Cisco C9300-24P | CPD GS | CPD secundario |

### 4.1.3 Instalación y puesta en marcha del servicio

Serán responsabilidad del contratista la gestión de todas las tareas necesarias para el aprovisionamiento de todo el equipamiento técnico que se vaya a usar en la prestación del servicio, así como para su instalación y puesta en marcha, incluyendo su configuración inicial.

El contratista deberá contemplar las configuraciones, reglas, políticas y procesos existentes en los servicios y sistemas de comunicaciones y seguridad actuales de Enresa (como por ejemplo las reglas de los Firewalls), para adaptarlos a los nuevos servicios y sistemas a poner en marcha, con el objeto de evitar cualquier degradación o pérdida de funcionalidad en los servicios que se están prestando.

### 4.1.4 Administración de la solución

El contratista realizará la configuración y administración de todas las soluciones hardware y software que emplee para la prestación del servicio objeto del contrato, considerando siempre que sea posible la aplicación de las mejoras prácticas sobre seguridad recogidas en las series de documentos “CCN-STIC” disponibles en la web del CERT del Centro Criptológico Nacional, adaptándose a las instrucciones y particularidades del contexto de Enresa.

### 4.1.5 Soporte y mantenimiento

Todo el equipamiento o tecnología, tanto hardware como software y en cualquier modalidad de despliegue, que el contratista emplee para la prestación del servicio, deberá contar con un soporte y mantenimiento directo del fabricante del producto, durante toda la ejecución del contrato, con las siguientes características:

- Soporte y Mantenimiento evolutivo del fabricante en horario 8x5:

- Acceso a actualizaciones de software y parches de seguridad.
- Acceso a bases de datos de conocimiento, así como capacidad de gestionar consultas con el fabricante.
- Soporte para el despliegue e implantación.

- Soporte y Mantenimiento correctivo ante incidencia o mal funcionamiento, en horario 24x7 para incidencias de severidad crítica y de 8x5 para el resto de las incidencias.

La gestión del soporte y mantenimiento del fabricante para cada producto o tecnología será responsabilidad del contratista, siendo el único interlocutor válido para la resolución de las incidencias que se produzcan durante la ejecución del contrato.

### 4.1.6 Herramienta de gestión del servicio

El contratista proveerá una herramienta de gestión del servicio o ticketing, incluyendo todos los medios necesarios para su operación y sin que requiera ningún elemento adicional por parte de Enresa. Esta permitirá el tratamiento de todos las incidencias y peticiones relacionadas con el servicio, además deberá permitir enviar correos electrónicos con la información necesaria a los contactos que Enresa autorice.

En cualquier caso, el sistema debe permitir realizar al personal autorizado de Enresa el seguimiento de los tiques en la herramienta de gestión del servicio, así como la verificación efectiva de los Acuerdos de Nivel de Servicio relacionados con la gestión de incidencias y peticiones.

El contratista podrá proponer la integración con la herramienta de gestión de incidencias y peticiones de Enresa (JIRA Service Management de Atlassian).

### 4.1.7 Red Nacional de SOC

Con el objetivo principal la impulsar la capacidad de protección de sus miembros mediante la compartición de información sobre amenazas que se estén detectando en la Administración, el SOC (Security Operation Centre) del contratista deberá pertenecer a la RNS (Red Nacional de SOC) que a través del Centro Criptológico Nacional integra los SOC de todos los organismos públicos de la Administración Española, junto con las entidades proveedoras que prestan dichos servicios de SOC y las entidades públicas que se benefician de los mismos.

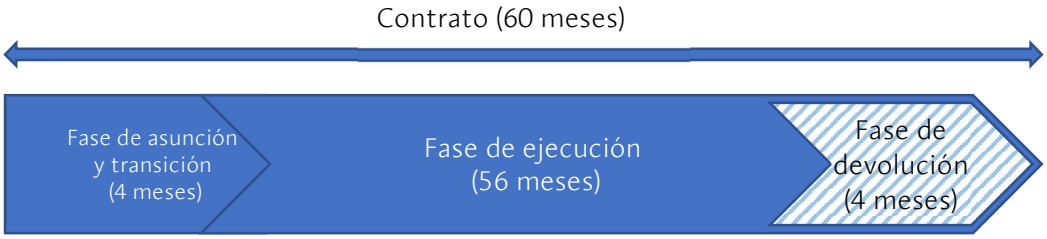
### 4.1.8 Certificaciones

- El contratista deberá disponer de la declaración o certificación de conformidad con el ENS nivel “medio” o superior, para servicios de alojamiento, comunicaciones o ciberseguridad, que cubra alguna actividad o proceso objeto del contrato que aportará en la reunión de lanzamiento del servicio como plazo máximo,y mantendrá durante la vigencia del contrato.

- El contratista deberá disponer de la certificación UNE-ISO/IEC 27001 – Seguridad de la información que deberá aportar en la reunión de lanzamiento del servicio, como plazo máximo, y mantener durante la vigencia del contrato.

# 5 Fases de prestación del servicio

Para el correcto desarrollo de los servicios objeto del presente pliego se definen las siguientes fases de prestación del servicio: asunción y transición, ejecución y devolución, que se definen a continuación.




## 5.1 Fase de asunción y transición del servicio

La asunción y transición del servicio por parte del contratista tendrá lugar durante **los primeros cuatros meses del contrato**.

Los servicios durante esta fase serán prestados por los anteriores contratistas o directamente por la Dirección de Sistemas y Documentación (en adelante DSD), por lo que el nuevo contratista deberá convivir con ellos y realizar todas las actividades necesarias para la asunción y transición a los servicios propuestos, sin pérdida de continuidad de los servicios que se prestan a Enresa.

El primer hito de esta fase de asunción y transición será la reunión de lanzamiento, en los primeros 5 días hábiles tras el inicio del contrato, en la que se planificarán todos los trabajos señalados por el contratista en su oferta para esta fase, y que generará el siguiente entregable por parte del contratista:

- E1: Presentación ejecutiva en formato PowerPoint del Plan de asunción y transición del servicio, que contenga de manera específica la planificación de las actividades a realizar y el detalle de la arquitectura técnica propuesta.

A continuación, se describe las actividades necesarias a realizar en la transición de los servicios, agrupados en hitos y su secuencia, así como sus relaciones o dependencias entre ellos:

- Hito 1: Adquisición de conocimiento: Se llevará a cabo toda la transferencia de conocimiento y se entregará al nuevo contratista toda la documentación disponible sobre la infraestructura tecnológica, procesos y procedimientos en el alcance del servicio.

  El plazo máximo para realizar este hito es de *30 días naturales* desde el inicio del contrato.

- Hito 2: Disposición de salas técnicas: Se realizarán todos los trabajos necesarios para dar cumplimiento a los requisitos del apartado 3.2.1 "Alojamiento de los sistemas de información", que permita disponer de las salas técnicas y los servicios asociados que van a componer el CPD Principal y Secundario de Enresa.

  El plazo máximo para realizar los trabajos requeridos en este hito es de *30 días naturales* desde la firma del contrato y se realizará en paralelo con las actividades del hito 1.

  El contratista deberá realizar el siguiente entregable a la finalización del hito:

  - E2: Documentación de alojamiento técnico, que incluya:
    - Información relevante de los CPD Principal y Secundario, procedimiento de acceso, zonas de uso, carga y descarga, monitorización, etc.
    - Descripción de las salas, racks y sus características técnicas, incluyendo un plano de estas.

- Hito 3: Implantación de la Arquitectura de Comunicaciones y Seguridad: Se realizarán los trabajos necesarios para dar cumplimiento a los requisitos del apartado 3.2 "Proteger" excepto los del apartado 3.2.8 "Protección de accesos privilegiados", para implantar los servicios y medidas técnicas necesarias que permitan operar una red de área amplia con los servicios de seguridad asociados y posibilite el acceso de los usuarios de Enresa desde cualquiera sea su ubicación a los servicios de Internet y las aplicaciones o sistemas de información de Enresa, así como soportar el tráfico de voz y fax.

  El plazo máximo para la realización de este hito es de *75 días naturales* desde el inicio del contrato, y se realizará en paralelo con las actividades del hito 1 y del hito 2.

  El contratista deberá realizar el siguiente entregable a la finalización del hito:
  - E3: Documentación de la arquitectura de comunicaciones y seguridad, que incluya diagramas del sistema, incluyendo equipos, líneas de defensa, redes,

interconexión con otras redes o sistemas, etc. Incluirá un anexo de diagrama de red que incluya el direccionamiento IP asociado.
- E4:Plan de pruebas conjuntamente con Enresa a realizar en el siguiente hito.

- Hito 4: Pruebas de la Arquitectura de Comunicaciones y Seguridad: Se realizarán en coordinación con Enresa y los terceros que se autoricen los trabajos necesarios para realizar todas las pruebas técnicas y funcionales necesarias que permitan verificar que la Arquitectura de Comunicaciones y Seguridad implantada cumple todos los requisitos solicitados y permite la operación efectiva de los servicios requeridos.

  El plazo máximo para la realización de este hito es de *15 días naturales* desde la finalización del hito 3.

- Hito 5: Traslado de equipamiento y puesta en producción: Se realizarán todos los trabajos necesarios para dar cumplimiento a los requisitos del apartado 4.1.2 "Traslado y acondicionamiento de equipamiento actual" que permita disponer de la infraestructura técnica de Enresa alojada en los CPD Principal y Secundarios proporcionados por el contratista, y se realizará la puesta en producción de la Arquitectura de Comunicaciones y Seguridad conforme los requisitos especificados en el hito 3.

  Para la realización de estos trabajos, será necesaria la planificación y colaboración coordinada del contratista con Enresa y con los proveedores que pueda designar.

  El plazo máximo para la realización de este hito es de 20 *días naturales* desde la finalización del hito 4.

  El contratista presentará al inicio del hito una Presentación ejecutiva en formato PowerPoint que contenga el detalle de la planificación del traslado del equipamiento.

- Hito 6 : Transición de la Detección, Respuesta y Recuperación: Se realizarán todos los trabajos necesarios para implantar las actividades requeridas en los apartados 3.3 "Detectar" y 3.4 "Respuesta y Recuperación", excepto aquellos que se identifiquen expresamente en la subfase de "optimización" cuyo detalle se describe en la siguiente fase, que permita identificar la ocurrencia de incidencias de comunicaciones y ciberseguridad, así como realizar las medidas necesarias para reducir el impacto y restablecer los servicios afectados.

  La realización de la transición de las actividades de Detección, Respuesta y Recuperación debe coincidir con la *finalización del hito 5*.

  El contratista realizará a la finalización del hito, los siguientes entregables:

  - E5: Catálogo de equipamiento técnico, que incluirá al menos:

  - Agrupación de componentes por servicio que hace uso.
  - Descripción técnica de cada componente y relaciones entre ellos.
  - Detalle de Licenciamiento o suscripción asociado al componente y/o servicio.
  - Descripción del soporte del fabricante de cada componente que lo requiera.
- E6: Procedimientos de operación y soporte, aplicables a los servicios del Centro de Operaciones y Soporte en integración con los procedimientos de Enresa.

El objetivo fundamental de esta primera fase es la adquisición de plena autonomía en la prestación de los servicios requeridos, para los que se deberá preservar la continuidad de la operación, mantenimiento y gestión de los servicios.

La finalización de la fase de asunción y transición del servicio debe ser aceptada expresamente por Enresa, mediante un acta de aceptación firmada por las partes.

## 5.2 Fase de ejecución del servicio

Durante esta fase el contratista prestará el servicio con plena autonomía y responsabilidad conforme las actividades y requisitos establecidos en la fase anterior, y deberán incorporar el resto de las actividades y requisitos solicitados en los pliegos, así como realizar los trabajos necesarios para aplicar un ciclo de mejora continua sobre los servicios prestados.

La fase de ejecución del servicio por parte del contratista tendrá lugar desde la finalización de la fase anterior y hasta la finalización del contrato.

Se distingue una subfase de "*optimización*" del servicio, en la que el contratista en el plazo máximo de ***120 días*** **naturales** desde el inicio de la fase de ejecución realizará las siguientes actividades:

- Al inicio de esta subfase de optimización, el contratista deberá realizar una presentación ejecutiva en formato PowerPoint del Plan de optimización del servicio, que contenga de manera específica la planificación de las actividades a realizar.
- Implantación de la solución o servicio de Gestión de Activos y Vulnerabilidades conforme los requisitos determinados en el apartado 3.1.3 "Gestión de Activos y Vulnerabilidades".
- Implantación de la solución de gestión de los accesos privilegiados a las infraestructuras y sistemas de información de Enresa, conforme los requisitos determinados en el apartado 3.2.8 "Protección de Accesos Privilegiados".
- Implantación del proceso iterativo de búsqueda de amenazas proactivas conforme los requisitos establecidos en el apartado 3.3.1.1 "Threat Hunting".
- Realización de las actividades de "tunning" de todos los servicios y soluciones técnicas del servicio, implementando las políticas y los casos de uso necesarios

adaptados al contexto de Enresa, con el objeto de optimizar los procesos detección y reducir los falsos positivos, mejorar la respuesta y recuperación implementando mecanismos de automatización, así como disponer de un sistema de métricas e indicadores útiles para comprobar la madurez del servicio.

Adicionalmente, el contratista deberá realizar en esta fase la implantación de las soluciones (de descubrimiento de superficie de ataque, de análisis de tráfico de red, de monitorización de experiencia de usuario) que haya asumido el compromiso de incorporar marcando *SI* en la casilla de compromiso correspondiente del Anexo 5 del PCAP.

A la finalización de la subfase de optimización, deberá entregar los siguientes entregables:

- E7: Actualización de la arquitectura de comunicaciones y seguridad, para incorporar los servicios y componentes adheridos en la subfase de optimización, incluyendo como anexos la arquitectura técnica de la solución de Gestión de activos y vulnerabilidades, y la arquitectura técnica de la solución de Protección de accesos privilegiados.
- E8: Actualización del catálogo de equipamiento técnico (E5), que incluya todos los nuevos componentes o cualquier modificación de los anteriores. Incluirá un detalle especifico de las fuentes integradas y políticas, reglas de correlación o casos de uso aplicables, para el servicio de Gestion de Información y Eventos de Seguridad, conforme los requisitos del apartado 3.3.2.
- E9: Elaboración de una propuesta de Procedimiento de Gestión de Activos y Vulnerabilidades.
- E10: Elaboración de una propuesta de Procedimiento de Gestión de accesos privilegiados para Enresa.
- E11: Elaboración de Manual de uso o Guía práctica para la gestión del servicio de accesos privilegiados para los administradores de los sistemas de información de Enresa.

## 5.3 Fase de devolución del servicio.

La fase de devolución del servicio tiene como objetivo garantizar la transferencia del conocimiento adquirido o generado durante la prestación del servicio por parte del contratista hacia Enresa, o hacia el nuevo contratista, sin que ello repercuta en una pérdida del control o del nivel de calidad del servicio.

En esta fase, el contratista estará obligado a devolver el control de los servicios objeto de contratación, simultaneándose los trabajos de devolución con los de prestación del servicio regular, sin coste adicional.

El traspaso tendrá una duración máxima de 120 días naturales desde la notificación del inicio de esta fase y en todo caso durante los últimos cuatro meses de contrato si se completa el tiempo de vigencia de este.

El compromiso de devolución del servicio incluye:

- Hacer entrega a la DSD de una versión actualizada de toda la documentación e información manejada para la prestación del servicio antes de la finalización del contrato.
- Facilitar el acceso a las ubicaciones físicas al personal de Enresa o a quién esta designe para la retirada del equipamiento técnico.
- Colaborar con el personal propio o designado por la DSD en la transferencia del conocimiento y la documentación del servicio, así como en la desinstalación y desenracado de los equipos.
- Hacer entrega de un documento de cierre del servicio, en el que se detallen todas las actividades de devolución.

En concreto, el contratista se compromete a tener preparada al comienzo de la fase de devolución del servicio toda la documentación generada en fases anteriores convenientemente actualizada.

# 6 Equipo de trabajo

El contratista designara:

- Un jefe de proyecto, que será el responsable de interlocución con Enresa y de la gestión del servicio, debe coordinar todas las actividades, los recursos humanos y la mejora en los procesos del servicio.
- Un responsable del servicio, cuya principal tarea será la interlocución y comunicación constante con el equipo directivo de Enresa.
- En aplicación del artículo 13 del Esquema Nacional de Seguridad, un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

El responsable del Servicio y el POC para la seguridad de la información, podrán ser la misma persona si el contratista así lo determina.

## 6.1 Lugar y prestación del servicio

Los trabajos se realizarán con carácter general en las oficinas del contratista, si bien y conforme los requisitos establecidos en el pliego, existen actividades del servicio, como por ejemplo la implantación del equipamiento físico y líneas de comunicaciones o las propias de los servicios de Alojamiento y el traslado del equipamiento, que requieren la prestación en los centros de procesos de datos o en las salas técnicas de los centros de trabajo de Enresa.

A estos efectos, además de los propios Centros de Procesos de Datos donde el contratista provee el alojamiento para Enresa, esta cuenta con los siguientes centros de trabajo:

| ***Nombre de Sede*** | ***Centro de trabajo*** | ***Dirección*** |
|---|---|---|
| MADRID | SEDE | Emilio Vargas, 7 – 28043 Madrid. |
| CABRIL | CENTRO DE ALMACENAMIENTO EL CABRIL | C/ Castillo, 5 – 14740 Hornachuelos. Córdoba. |
| VANDELLÓS | CENTRAL NUCLEAR VANDELLÓS I | Ctra. N-340, Km. 1123,7 – 43890 L´Hospitalet de l´Infant. Tarragona. |
| ZORITA | CENTRAL NUCLEAR JOSÉ CABRERA | Almonacid de Zorita – 19119 Guadalajara |
| GAROÑA | CENTRAL NUCLEAR SANTA MARÍA DE GAROÑA | Ctra. Trespaderne - Puentelarra s/n– 09212 Burgos |

Por otra parte, Enresa podrá solicitar:

- El desplazamiento justificado por necesidades de servicio y con carácter temporal, como por ejemplo las necesarias para reuniones de seguimiento o reuniones específicas, del Jefe de Proyecto, del Responsable del Servicio y/o del POC, a la sede de Enresa en Madrid.

- El desplazamiento puntual del personal necesario del equipo de trabajo en el caso de que alguna tarea del servicio no pueda realizarse por medios telemáticos en remoto, por razones imputables al contratista, a cualquier centro de trabajo de Enresa, especialmente las necesarias para la resolución de incidencias.

- El desplazamiento excepcional del gestor de ciberincidentess y el personal que se considere necesario por este, en el caso de requerir la respuesta de emergencia ante ciberincidentes enunciada en el apartado 3.4.1.4.

En todos los casos los gastos de desplazamiento, alojamiento y manutención correrán a cargo del contratista.

### 6.2 Horario de prestación de los servicios

Con carácter general, el servicio se prestará dentro de la franja horaria de 9:00 a 17:00 de lunes a viernes (modalidad 8x5) en el uso horario peninsular de España, excepto los trabajos a realizar por el Centro de Operaciones y Soporte en los siguientes supuestos, que comprenden las 24 horas, los 7 días de la semana y los 365 días del año (modalidad 24x7):

- En el ámbito de Incidencias clasificadas como de severidad **crítica**, conforme los requisitos determinados en el apartado 3.4 Centro de Operaciones y Soporte.
- En los simulacros y activación del Plan de Continuidad de Negocio, conforme los requisitos determinados en el apartado 3.4.2 "Continuidad del servicio".
- La puesta en producción de la arquitectura de comunicaciones y seguridad, conforme se determina en el apartado 5.1 Fase de asunción y transición del servicio.
- Aquellos cambios o actuaciones que requieran justificadamente por su impacto sobre los servicios que presta Enresa realizarse fuera del horario establecido de manera general.
- Las actividades necesarias para garantizar la correcta operación y mantenimiento de los Centros de Procesos de Datos Principal y Secundario.

## 7 Modelo de relación

Para garantizar la interlocución adecuada se crearán tres Comités permanentes (de dirección, táctico y operativo).

| Nivel | Funciones Principales | Órganos de Gestión |
|---|---|---|
| **Dirección** | Definir los objetivos estratégicos, la visión futura y evolución del servicio.<br>Aprobar las planificaciones y actuar como máximo nivel de escalado del servicio | Comité de Dirección y Estrategia |
| **Táctico** | Partiendo de los objetivos estratégicos aprobados del Comité de Dirección, generar el plan de acción que se traducirá en líneas maestras de trabajo para poder llevar a cabo la implementación de la estrategia establecida | Comité de Seguimiento |

| Nivel | Funciones Principales | Órganos de Gestión |
|---|---|---|
| **Operativo** | Los equipos de operación efectuarán la prestación del servicio siguiendo las directrices de los responsables de los equipos de trabajo | Comité Operativo. |

En la fase de asunción y transición del servicio, cada parte designará a los miembros de los comités.

### NIVEL DE DIRECCIÓN - Comité de dirección y estrategia

Periodicidad: Una reunión anual o cuando sea requerida.

Funciones principales

- Directrices de servicio y tecnología.
- Gestión de problemas detectados.
- Seguimiento económico del contrato.

Asistentes:

- Enresa: responsable de contrato, jefatura del Departamento de Sistemas y Tecnologías de Información (DSTI) y/o Dirección de Sistemas y Documentación (DSD.
- Contratista: responsable del servicio, POC para la seguridad de la Información, jefe de proyecto y Dirección del contratista.

Podrán asistir por invitacion cualquier otra persona que se considere necesario para el tratamiento de asuntos particulares.

### NIVEL TÁCTICO - Comité de Seguimiento

Periodicidad: Una reunión mensual, o cuando sea requerida

Funciones principales

- Control del cumplimiento de los Acuerdos de Nivel de Servicio.
- Seguimiento de incidencias, peticiones y cambios.
- Gestión de problemas derivados del nivel de operación.
- Propuestas de mejoras en el servicio.
- Gestión de la facturación.

Asistentes:

- Enresa: responsable de contrato.
- Contratista: responsable del servicio y jefe de proyecto.

Podrán asistir por invitacion cualquier otra persona que se considere necesario para el tratamiento de asuntos particulares.

### NIVEL OPERATIVO - Comité operativo

Periodicidad: Una reunión semanal o según necesidades del servicio

Funciones principales

- Seguimiento de la operación diaria.
- Supervisión de las tareas realizadas.
- Tratamiento de problemas específicos.
- Formulación de propuestas de posibles mejoras en el servicio.

Asistentes:

- Enresa: responsable de contrato.
- Contratista: jefe de proyecto.

Podrán asistir por invitacion cualquier otra persona que se considere necesario para el tratamiento de asuntos particulares.

Es responsabilidad del contratista convocar todas estas reuniones con una antelación suficiente. En el caso de las reuniones mensuales, estas serán agendadas como máximo en los diez primeros días del mes siguiente al periodo de referencia.

# 8 Informes

Con independencia de cualquier otro informe o entregable que se requiera en el ámbito de las actividades objeto del contrato, el contratista deberá presentar a lo largo de la vigencia del contrato los informes que se señalan a continuación, con el contenido indicado.

En caso de retraso en la entrega de informes, con respecto a los plazos requeridos, se aplicarán las penalizaciones recogidas en los ANS correspondientes.

### Informes mensuales

Deberá ser enviado por el contratista a los miembros del comité de seguimiento antes de las 14.00 horas (huso horario peninsular de España) del día 6 de cada mes o el primer día laboral si este no lo es.

El informe se estructurará en los siguientes apartados:

- Resumen: relación de los hitos o hechos más relevantes que se hayan producido durante el mes, de forma que ofrezca una visión general del servicio.

- Actividades: principales tareas realizadas durante el periodo, y las desviaciones existentes, así como los hitos siguientes a alcanzar.
- Aspectos críticos: aspectos o asuntos que puedan tener una incidencia destacada o un impacto importante, en el desarrollo del servicio en los siguientes períodos, y sobre los que habrá que prestar una especial atención.
- Seguimiento de los Acuerdos de Nivel de Servicio.
- Seguimiento económico del contrato.
- Anexo ejecutivo: presentación en powerpoint que incluya las principales métricas e indicadores del servicio.

En caso de que el informe no incluya toda la información requerida se dispondrá de un plazo de cuatro días hábiles, improrrogable, para su entrega una vez subsanadas las deficiencias.

Este informe servirá de base para la reunión del seguimiento mensual de la que se levantará acta que se firmará con certificado electrónico por el responsable de contrato de Enresa y por el responsable de servicio del contratista.

### Informe anual

El objeto de este informe es comunicar los resultados alcanzados cada anualidad en la prestación de los servicios en sus aspectos técnicos y operativos. Además de estos aspectos, podrá contener las propuestas para las modificaciones de alto nivel desde el punto de vista de organización, equipo, indicadores de mejora del servicio, alcances, etc.

El informe se enviará a los miembros del comité correspondiente acompañando a la convocatoria de reunión, con 10 días de antelación a la fecha de la convocatoria y contendrá la siguiente información mínima:

- Informe Técnico. Recoge, de manera sucinta:
  - Un resumen de los hitos y hechos más significativos del periodo.
  - Principales actividades realizadas en el periodo.
  - Actividades programadas para el próximo periodo.
- Seguimiento de los Acuerdos de Nivel de Servicio.
- Seguimiento económico del contrato.

Servirá de base para la reunión de seguimiento anual de la que se levantará acta que se firmará con certificado electrónico por el responsable de contrato de Enresa y por el responsable del servicio del contratista.

En caso de que el informe no incluya toda la información requerida se dispondrá de un plazo de cuatro días hábiles, improrrogable, para su entrega una vez subsanadas las deficiencias.

### Informes especiales

La Dirección de Sistemas y Documentación, podrá solicitar que se elaboren informes específicos relacionados con la ejecución del contrato, que el contratista presentará en el plazo de una semana desde la solicitud, salvo que se pacte un plazo mayor.

En caso de que los informes no incluyan toda la información requerida se dispondrá de un nuevo plazo de entrega de cuatro días hábiles, improrrogable, para su entrega una vez subsanadas las deficiencias.

# 9 Propiedad intelectual

Los derechos de explotación de las configuraciones y parametrizaciones desarrollados en el marco de este contrato corresponden en exclusiva a Enresa.

El contratista entregará toda la documentación relacionada con la gestión del servicio.

Durante la ejecución de los trabajos objeto del contrato el contratista se compromete, en todo momento, a facilitar a las personas designadas por la DSD, la información y documentación que soliciten para tener pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos.

Toda la documentación generada durante la ejecución del contrato será propiedad exclusiva de Enresa, sin que el contratista pueda conservarla, ni obtener copia o facilitarla a terceros sin la autorización expresa y por escrito de Enresa.

# 10 Seguridad

Enresa tiene establecida una Política de Seguridad que regula la gestión de la Seguridad de la Información en la organización, fundamentada en un Sistema de Gestión de la Seguridad de la Información (en adelante, SGSI), cuyo propósito es garantizar que los riesgos de la seguridad de la información son conocidos y gestionados por la organización, y en el cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS).

Las medidas de seguridad a aplicar en los servicios objeto de este contrato y en los posibles sistemas de información desplegados serán las que correspondan del Anexo II del Esquema Nacional de Seguridad, en función de la categorización del sistema MEDIO, así como el Reglamento General de Protección de Datos (RGPD) y su normativa de desarrollo vigente, según la tipología de los datos e información gestionada.

El contratista dotará de todas las herramientas informáticas y de comunicaciones necesarias para el desarrollo de todas las actividades a todos los recursos asignados al servicio sean o no presenciales. Si se requiere acceso a los sistemas de información de Enresa, sólo está permitido previa solicitud y autorización por el Departamento de Sistemas y Tecnologías de la Información (DSTI), quien en función de las necesidades evaluará el método de acceso, que con carácter general exigirá un mecanismo de doble factor de autenticación para iniciar sesión en los sistemas.

Para los supuestos en los que se usen aplicaciones web para la prestación de los servicios, estás deberán implementar protocolos seguros cifrados de comunicación (https/ssl) asegurando la corrección de vulnerabilidades publicadas sobre los mismos.

El contratista, será responsable de que las soluciones y servicios que se presten a Enresa cumplen los requisitos de seguridad. Los daños y perjuicios causados a Enresa y a terceros, por las consecuencias derivadas en el entorno de la seguridad de los trabajos realizados en el ámbito de este contrato, serán responsabilidad del contratista.

# 11 Auditorías técnicas

Enresa podrá planificar y realizar revisiones o auditorías técnicas de seguridad sobre los sistemas que se operan dentro del alcance de los servicios contratados, que podrán ser ejecutadas por Enresa o por terceros colaboradores.

De requerirse, el contratista deberá proporcionar todo el apoyo, soporte y documentación necesarios para la realización de auditorías, así como proceder a la corrección de las deficiencias detectadas y a la aplicación de las conclusiones de estas.