WEBINAR 10 abril 10:00 AM

NIS2 para Entidades Locales (EE.LL.)

Urgencia, impacto & cómo prepararse

oesia grupo

oesia networks grupo oesia

tecnobit grupo oesia

cipherbit grupo oesia

UAV Navigation grupo oesia

inster grupo oesia

Rubén Vega

Key Account Manager en Grupo Oesía

01. NIS2 puntos clave

No hay período de gracia; entra en vigor de inmediato.

Aumento de las exigencias de seguridad para las EE.LL.

Gran énfasis en demostrar las acciones tomadas.

02. Ámbito de aplicación

1 Entidades Afectadas:

Públicas y Privadas
que operen en sectores críticos.

Residencia Fiscal
que operen en España, aunque tengan residencia en otro Estado de la UE.

2 Sectores Críticos:

Banca y mercados financieros

AAPP, cadena de suministro, sector sanitario y transporte

Infraestructuras digitales

3 Otros Sectores:

Servicios postales y mensajería

Gestión de residuos

Producción y distribución de alimentos y mezclas químicas

Proveedores de servicios digitales y de comunicación

Investigación científica

Seguridad privada

03. Impacto en las EE.LL.
Esenciales – Importantes

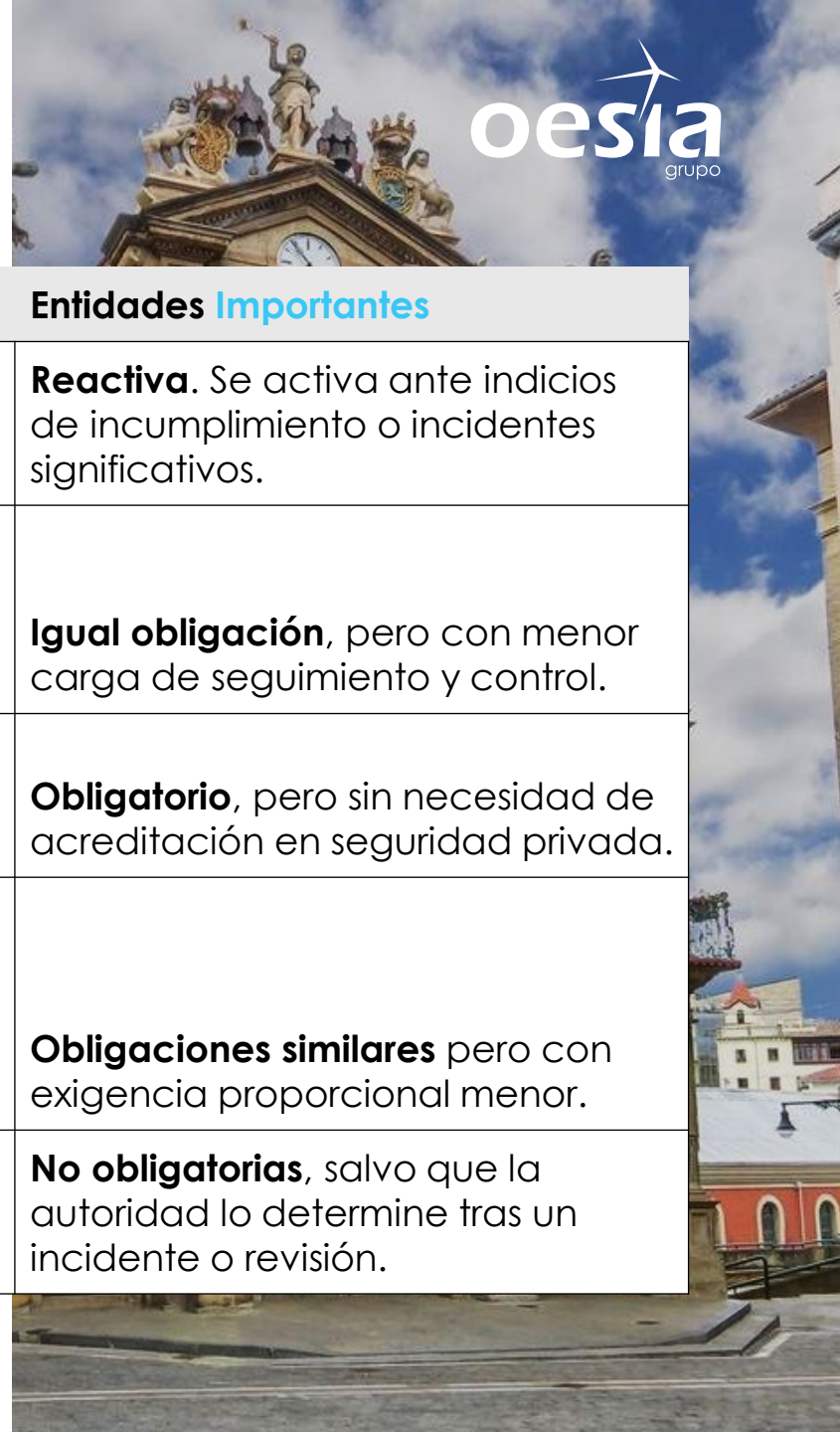
Los ayuntamientos que están clasificados como entidades **esenciales** son los siguientes:

- Los municipios cuya población supere los **250.000 habitantes**.
- Los municipios capitales de provincia cuya población sea superior a los **175.000 habitantes**.
- Los municipios que sean capitales de provincia, capitales autonómicas o sedes de las instituciones autonómicas.
- Los municipios cuya población supere los **75.000 habitantes**, que presenten circunstancias económicas, sociales, históricas o culturales especiales.

Los ayuntamientos clasificados como entidades **importantes** son:

- Los municipios cuya población supere los **20.000 habitantes** y las entidades de su sector público institucional.

03. Impacto en las EE.LL.



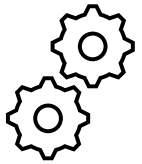
Ambas categorías deben cumplir con un catálogo común de medidas **(Art. 15)**, pero en las entidades **esenciales** **se refuerza el nivel de exigencia** y seguimiento por parte del Estado.

Esenciales estarán sujetas a un régimen de **supervisión más riguroso** y continuo, mientras que las entidades **importantes** serán supervisadas principalmente de **forma posterior a incidentes** o sospechas de incumplimiento

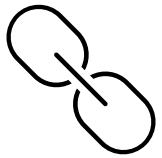
Categoría	Entidades Esenciales	Entidades Importantes
Supervisión	**Proactiva**, continua, incluye auditorías, inspecciones in situ y evaluaciones técnicas.	**Reactiva**. Se activa ante indicios de incumplimiento o incidentes significativos.
Notificación de Incidentes	**Obligatoria** e inmediata; supervisada por la autoridad competente y canalizada por la Plataforma Nacional.	**Igual obligación**, pero con menor carga de seguimiento y control.
Responsable de Seguridad	**Obligatorio**, con acreditación específica (seguridad privada).	**Obligatorio**, pero sin necesidad de acreditación en seguridad privada.
Medidas de Seguridad	**Implementación obligatoria** de medidas reforzadas (Art. 15): gestión de crisis, cifrado, respuesta a incidentes, pruebas de ciberseguridad.	**Obligaciones similares** pero con exigencia proporcional menor.
Auditorías de Seguridad	**Obligatorias y periódicas**.	**No obligatorias**, salvo que la autoridad lo determine tras un incidente o revisión.

04. Requisitos clave: 8 de 14 total

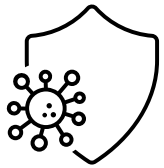
Políticas de seguridad y Gestión de Riesgos



Planes de Continuidad de Negocio y respuesta a Incidentes



Seguridad en la cadena de suministro



Seguridad de redes y gestión de vulnerabilidades

Procedimientos de evaluación de medidas y auditorías

Concienciación y formación en ciberseguridad

Autenticación multifactor y cifrado de datos

Políticas de control de acceso y gestión de activos

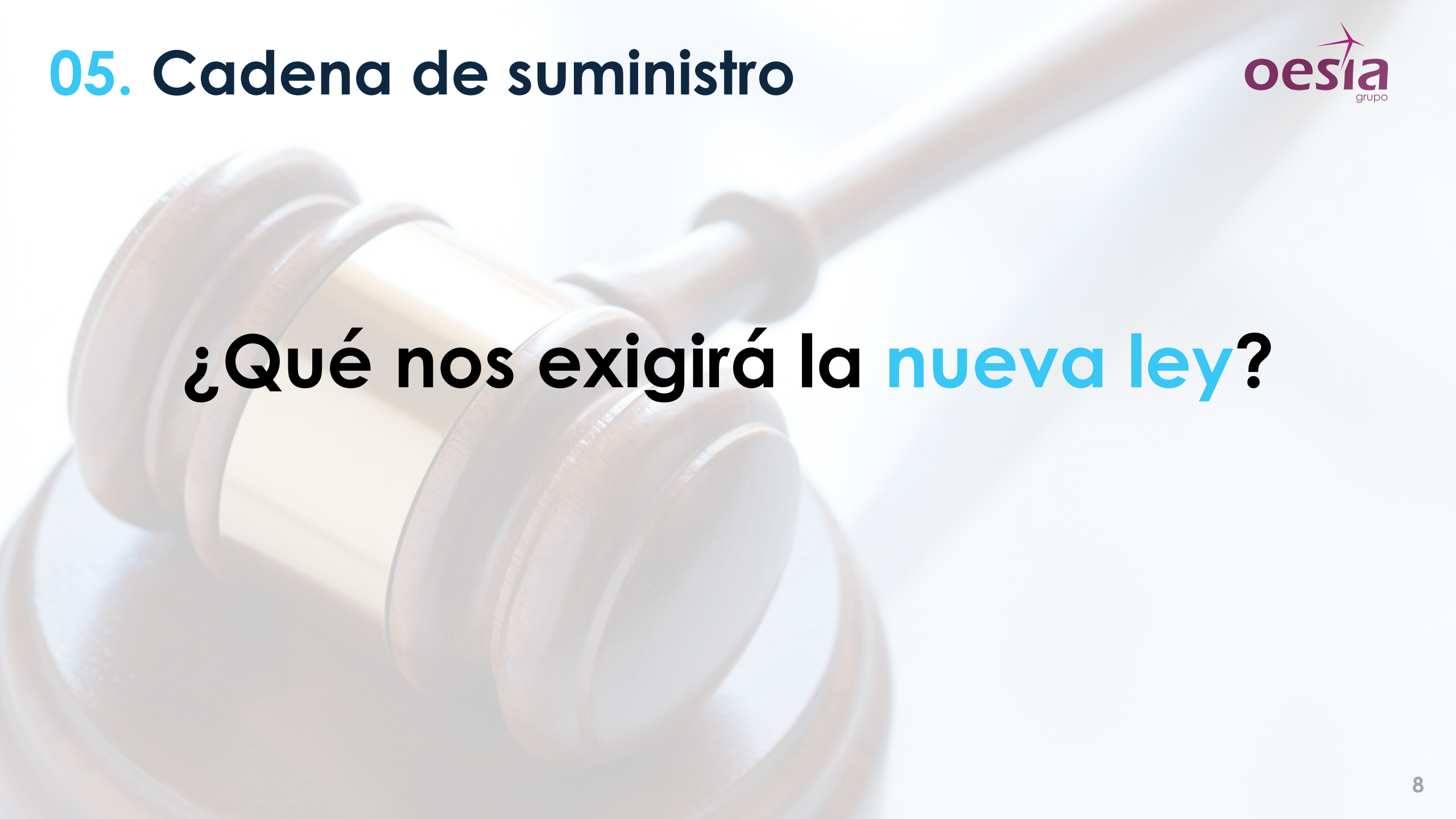
05. Gestión de activos

¿Qué nos exigirá la nueva ley?

¿Cómo se está gestionando hoy?

¿Qué podemos hacer con mínimo impacto en lo operativo?

05. Cadena de suministro



¿Qué nos exigirá la nueva ley?

Gestión de activos

- **Medida 9.3 - Gestión de Activos (Artículo 15 del Anteproyecto de Ley de Transposición de NIS2 en España)**
- **📌 Lo que las empresas deben hacer en relación con la gestión de activos según el texto oficial:**

*"Las entidades **esenciales e importantes** deberán establecer y mantener actualizado un **inventario de todos los activos de información**, incluidos aquellos activos físicos y lógicos que sean esenciales para la prestación de sus servicios o el desarrollo de sus actividades.*

*Este inventario deberá estar debidamente documentado e incluir la **asignación de responsabilidades** sobre dichos activos, así como los controles y medidas de seguridad aplicados para garantizar su protección"*

A términos prácticos:

- **Inventariado** de todos los dispositivos
- **Contexto: Asignación de Responsables**

05. Gestión de activos

¿Cómo se está gestionando hoy?

05. Gestión de activos

30%+

05. Gestión de activos

IT, IoT, OT, IoMT...

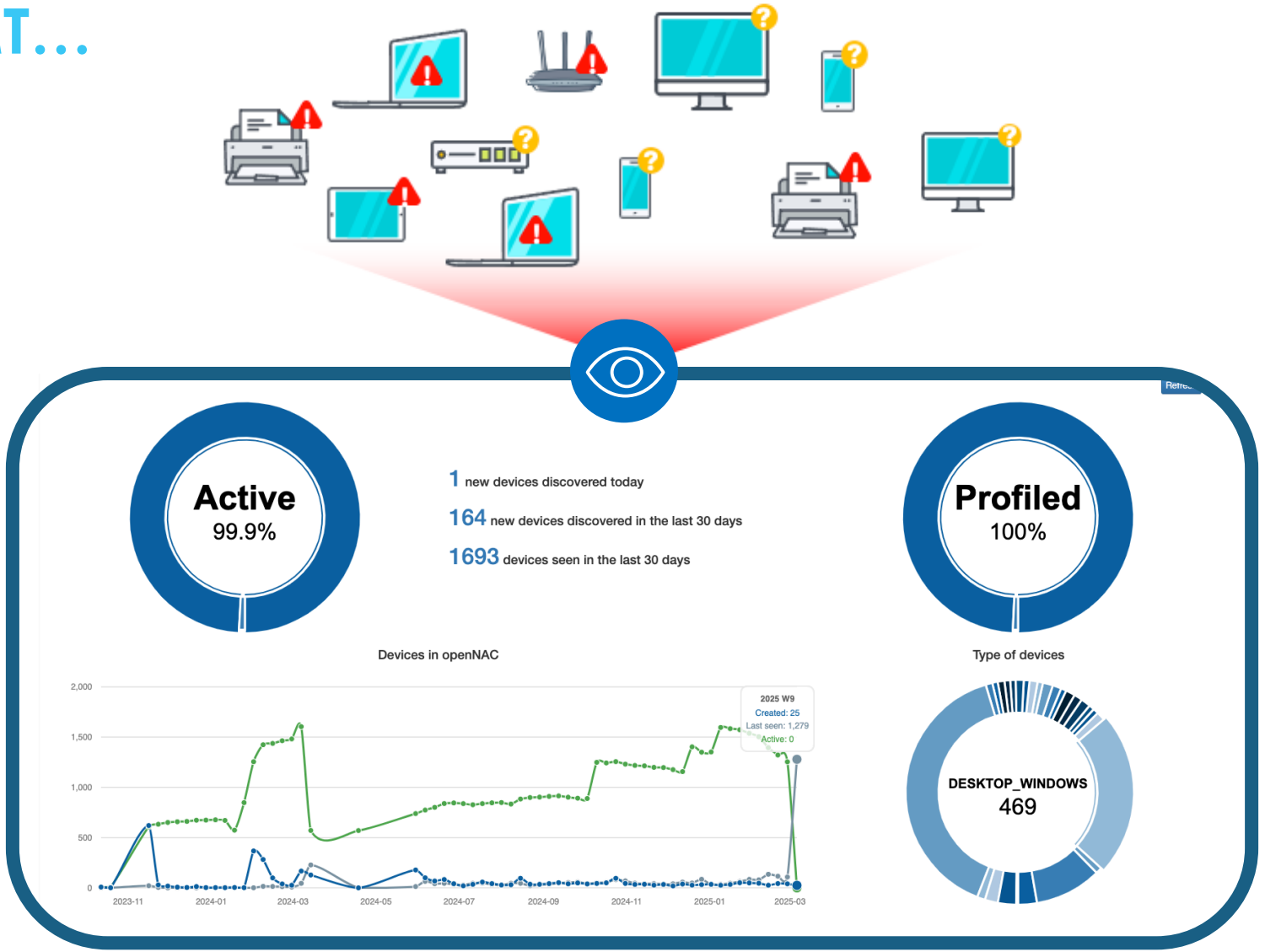


FIG 1: Todos los activos

05. Gestión de activos

Cuantificar y cualificar

Cuántos dispositivos, qué son, dónde están conectados…

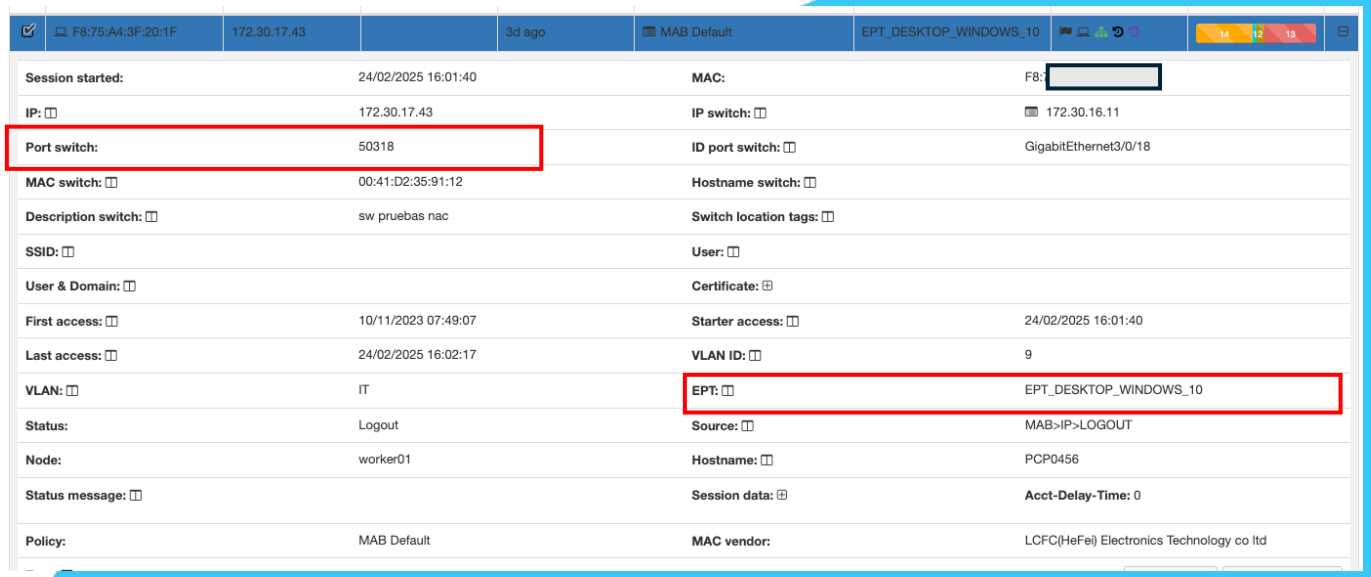


FIG 2: Un activo

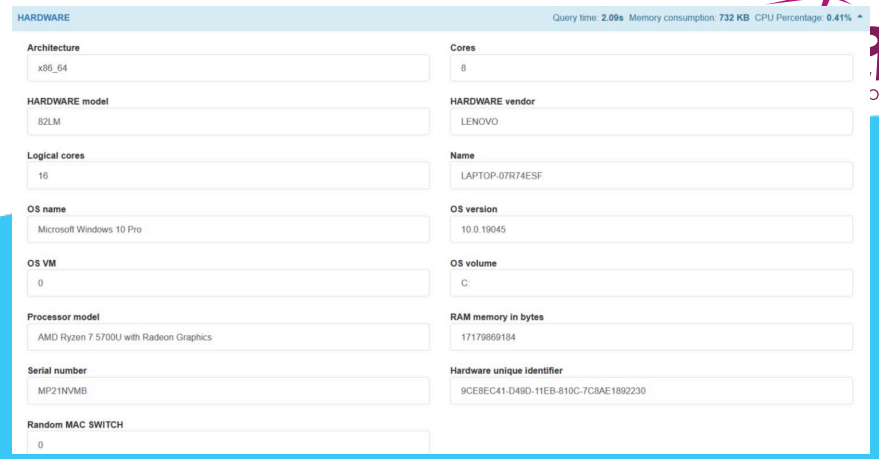


FIG 3: HW de un activo

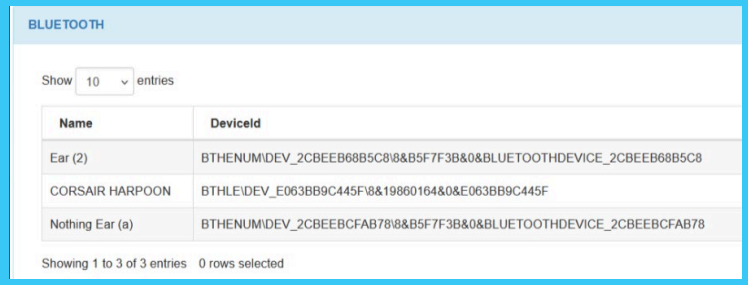


FIG 5: Bluetooth

FIG 4: Security Center

05. Gestión de activos

Contexto:

- Asignar Responsables
- Asignar criticidad (según análisis de riesgo etc., GDPR…)
- Información de ubicación física
- SLAs..

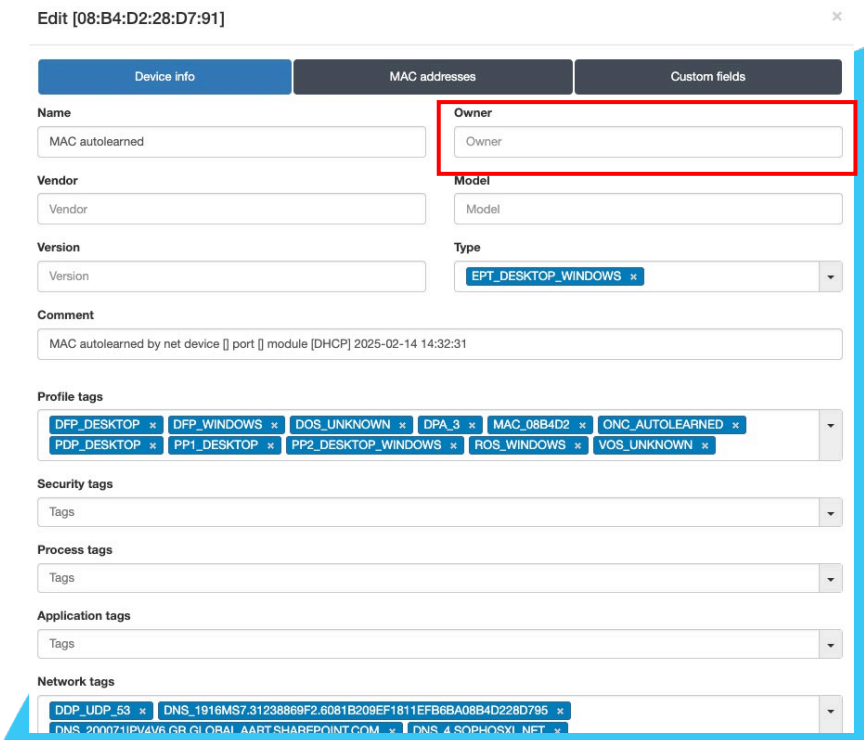


FIG 7: Contexto de un dispositivo

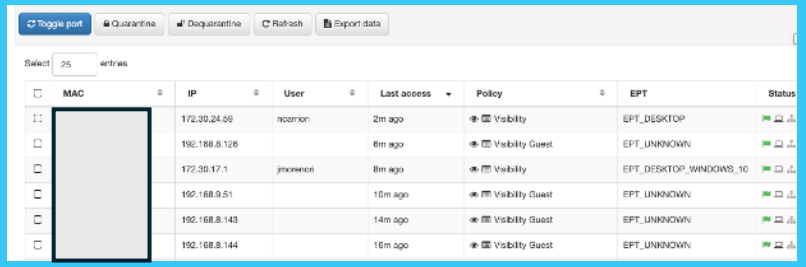


FIG 8: Múltiples activos

05. Gestión de activos

Búsqueda:

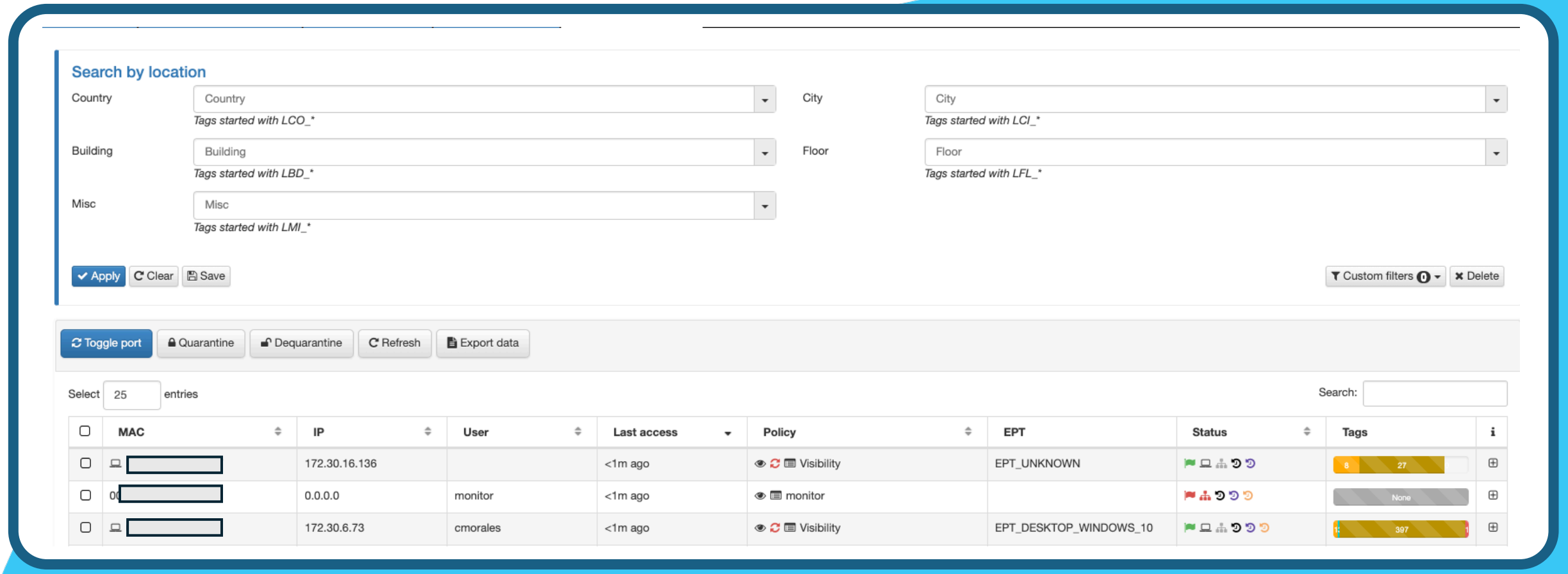


FIG 6: País, cuidad, edificio, planta…

05. Gestión de activos

Agrupaciones

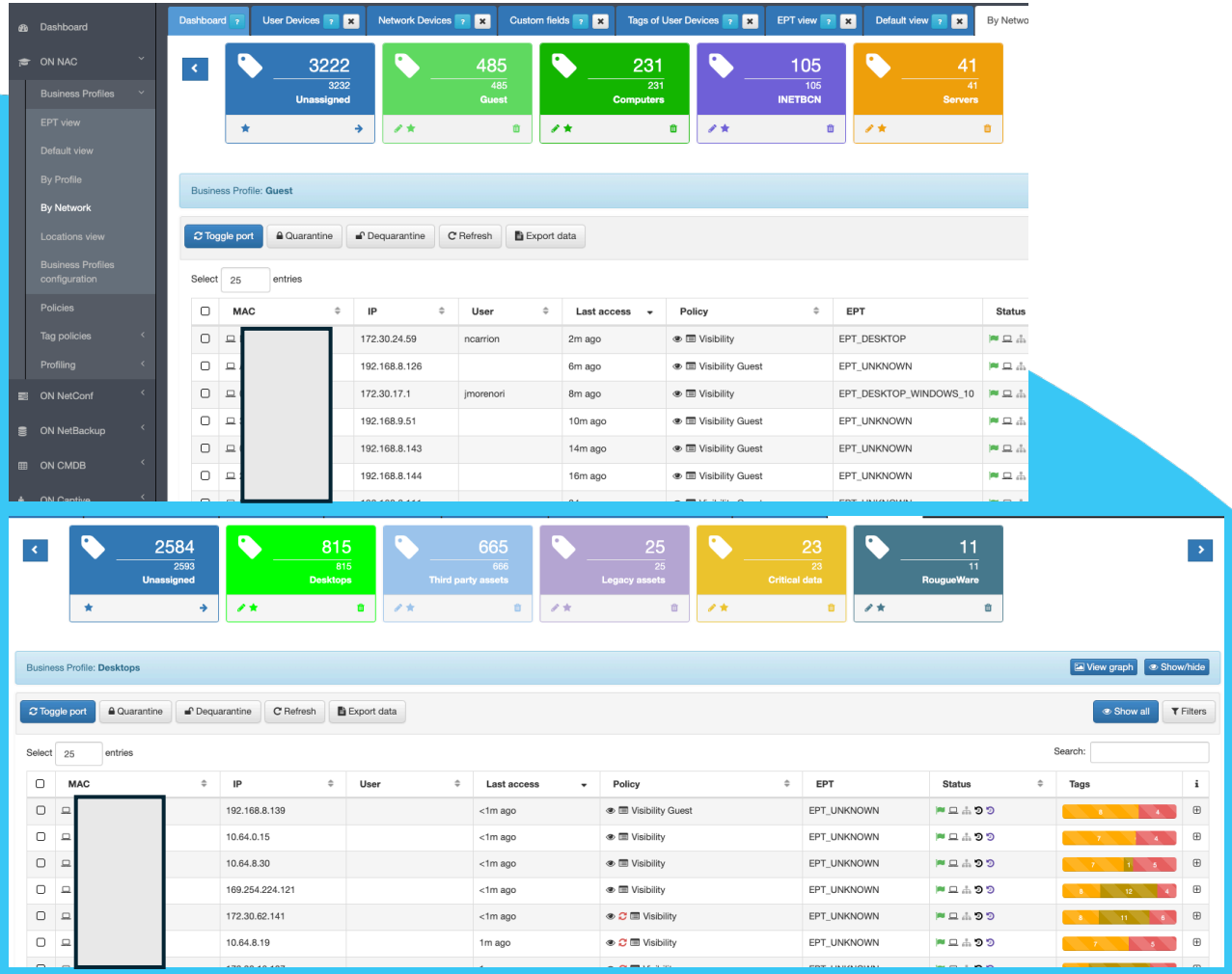


FIG 8: Ejemplos de agrupaciones con diversas lógicas según la empresa

Agrupar dispositivos por:

- Tecnología (Sobremesas, Portátiles, IoT/OT, Impresoras…)
- Ubicaciones físicas
- Plantas
- Criticidad
- Por cumplimiento de políticas de seguridad

05. Gestión de activos

Resumen:

Problema latente en el mercado – clave para la gestión del riesgo

Inventario actualizado de activos

- Todos los **activos lógicos** (IT, IoT, IoMT, OT).
- Automatizado y centralizado.
- **Cambios en tiempo real** de manera automática.

Asignación de **contexto**: Responsabilidades y criticidad…

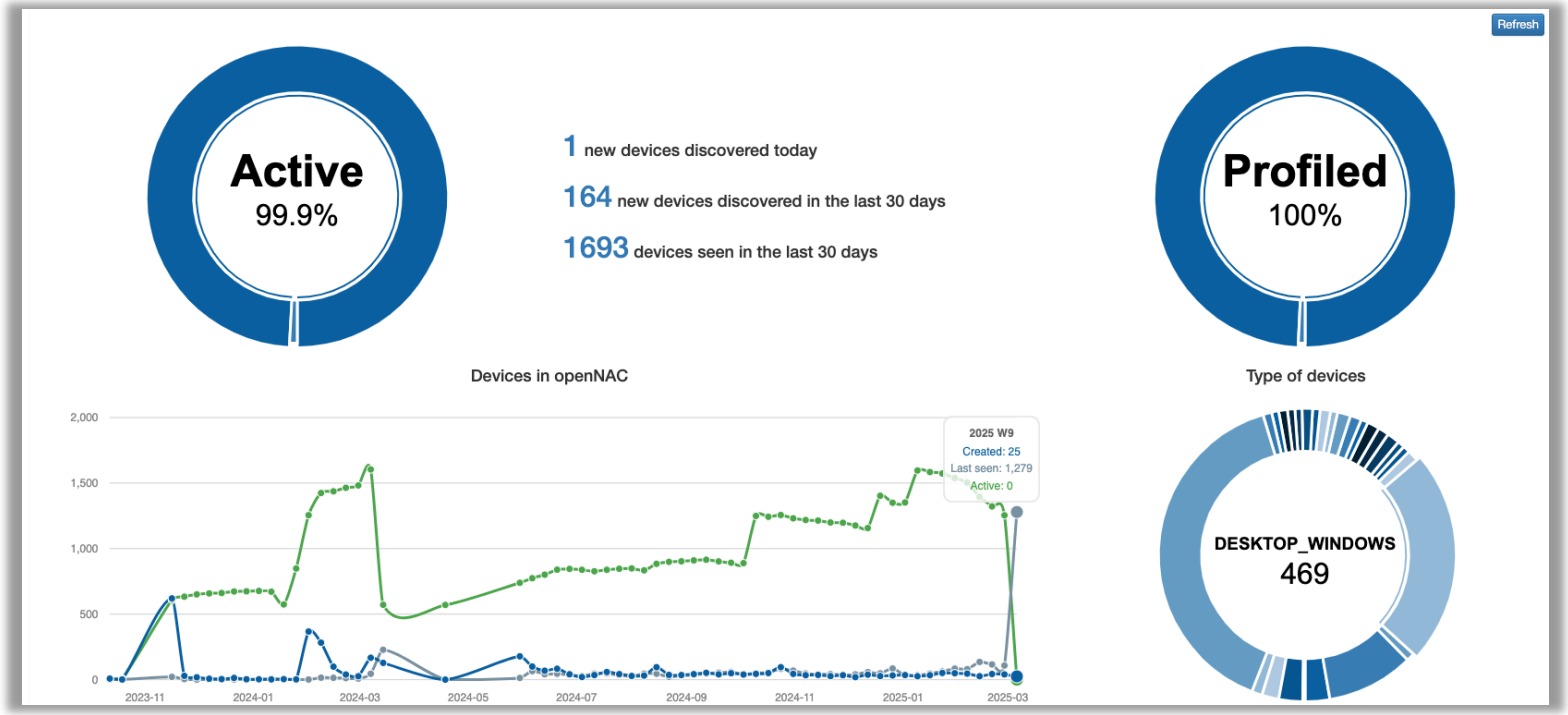


FIG 1: Todos los activos

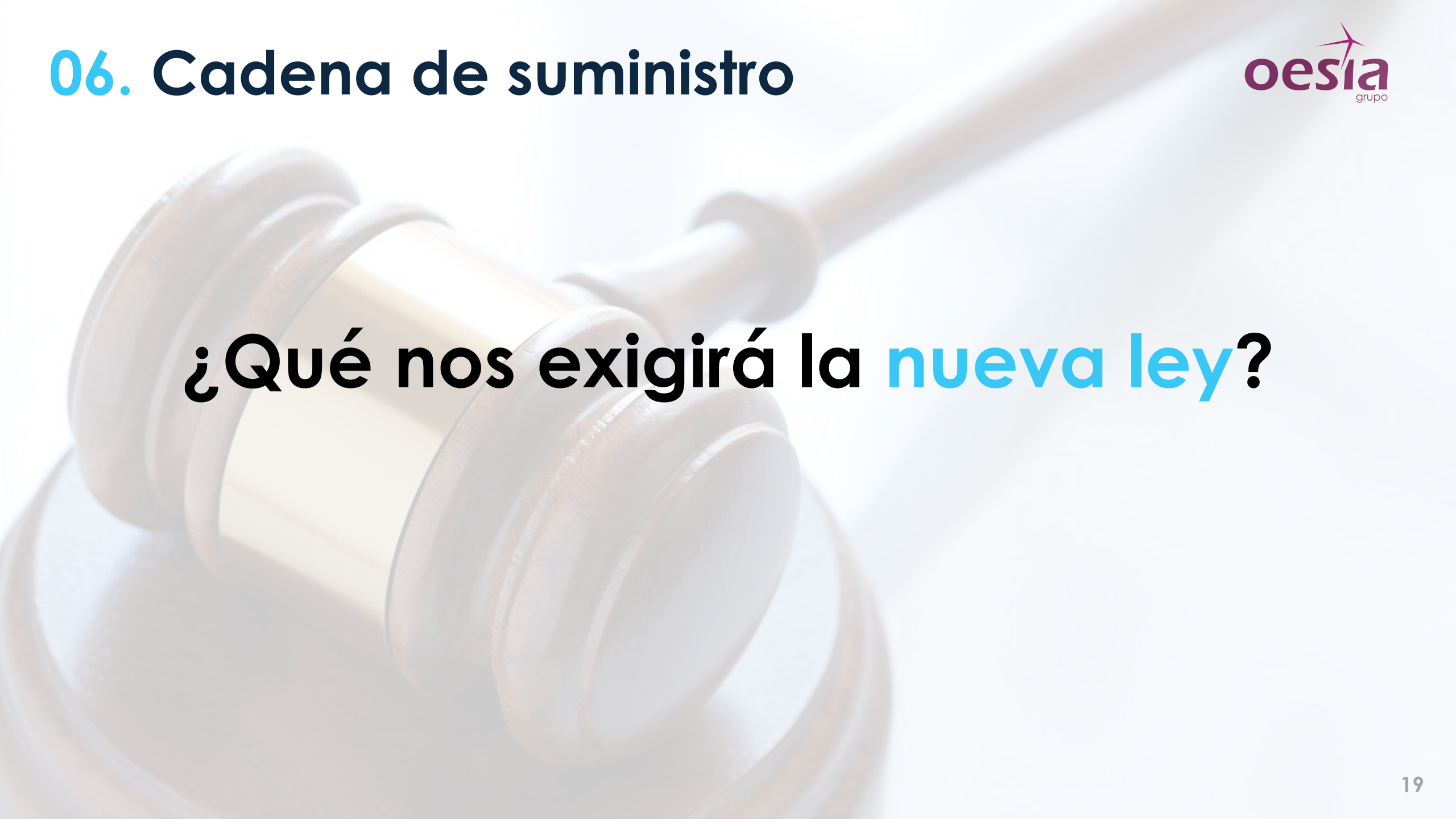
06. Cadena de suministro

¿Qué nos exigirá la nueva ley?

¿Cómo se están gestionando
los proveedores externos hoy?

¿Qué podemos hacer con
mínimo impacto en lo operativo?

06. Cadena de suministro



¿Qué nos exigirá la nueva ley?

06. Cadena de suministro

¿Qué nos exigirá la nueva ley?

Medida 4 - Seguridad de la Cadena de Suministro (Artículo 15 del Anteproyecto de Ley de Transposición de NIS2 en España)

- 📌 Lo que las empresas deben hacer en relación con la seguridad de la cadena de suministro según el texto oficial:

*"Las entidades **esenciales e importantes** deberán gestionar los riesgos de ciberseguridad que afecten a su cadena de suministro **y a sus relaciones con proveedores** y prestadores de servicios, incluidos aquellos proveedores de servicios de datos o sistemas de información en la nube.*

*Para ello, deberán establecer **requisitos de seguridad en sus acuerdos contractuales con terceros**, **asegurando** que estos proveedores apliquen medidas de seguridad adecuadas y alineadas con las exigencias de la normativa vigente."*

A términos prácticos:

- **Definir que** controles debería de aplicar el proveedor
- Articularlos en los acuerdos / contratos
- **Garantizar que se aplican**

06. Cadena de suministro > Problema real

¿Qué nos exigirá la nueva ley?

El Corte Inglés

Estimado Cliente,

Para El Corte Inglés la privacidad y la protección de sus datos personales son un compromiso constante.

En este sentido, le informamos que recientemente un proveedor externo ha sufrido un acceso no autorizado a datos personales de nuestros clientes. El incidente se identificó y se subsanó inmediatamente a través de nuestros protocolos de detección y seguridad. A su vez, requerimos a dicho proveedor la aplicación de medidas adicionales que prevengan este tipo de incidentes a futuro. Estos hechos ya han sido puestos en conocimiento de las autoridades competentes.

La información a la que se ha accedido de forma no autorizada consiste en datos identificativos y de contacto, así como números de tarjetas para compras sólo en El Corte Inglés. En cualquier caso, dicha información no permite a terceros operar ni realizar pagos con su tarjeta de El Corte Inglés. Puede usted seguir utilizando su tarjeta con total seguridad, tanto en nuestras tiendas como a través de nuestra web y app, así como en otros comercios.

Resumido:

- **Proveedor externo**
- Definir las medidas y controles
- Articularla en acuerdos/contratos
- **Hay que garantizar que se aplican**

06. Cadena de suministro

¿Cómo se están gestionando los proveedores externos hoy?

06. Cadena de suministro > Seguridad

Escenario: El dilema de los terceros (remotos)

Necesidad Operativa:

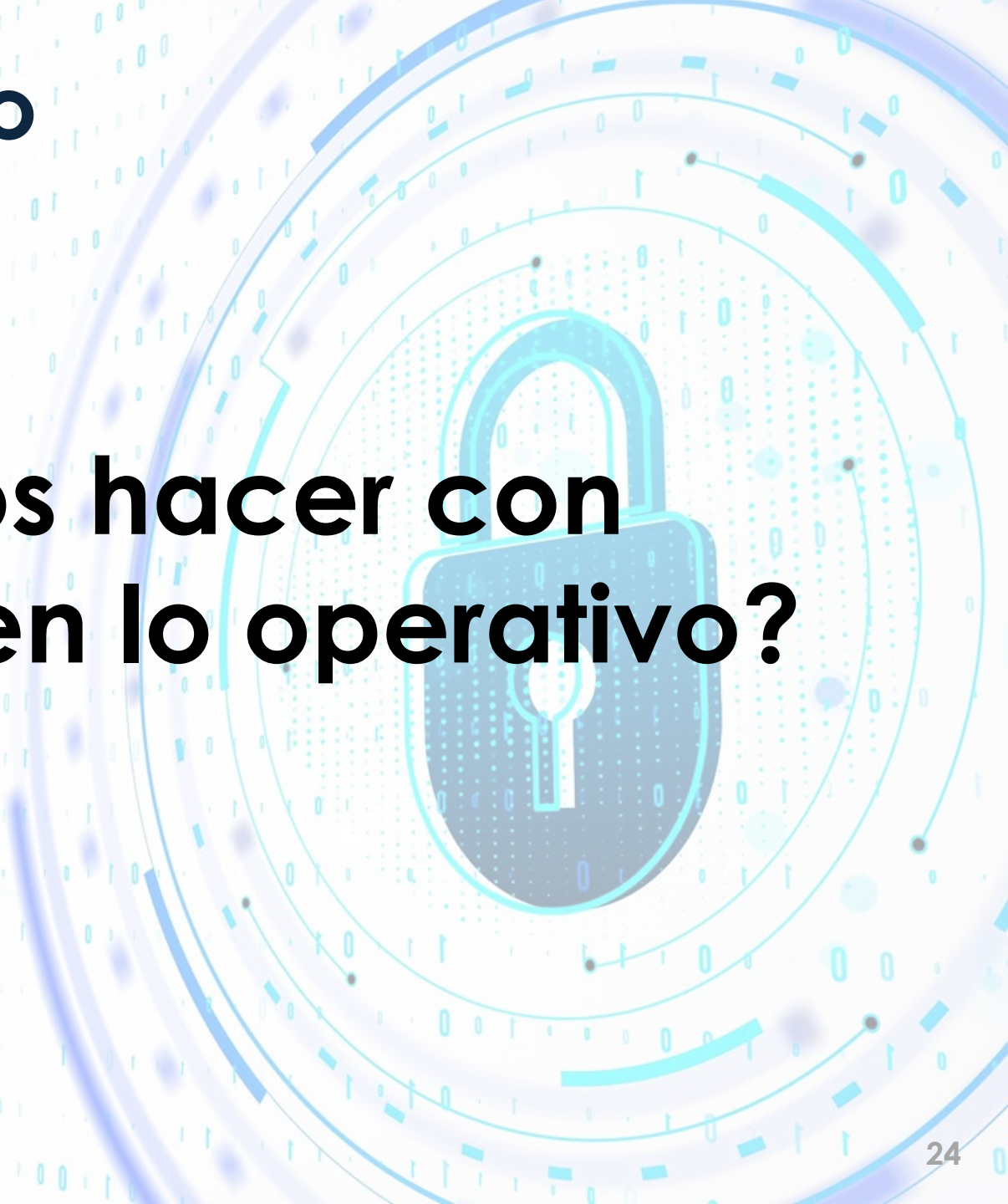
- Los terceros proporcionan servicios críticos al negocio y para ello tiene que **acceder a recursos del negocio** (acceso a bases de datos, servidores etc.).

Desafío de Seguridad:

- VPN - OK
- Dispositivos **no corporativos** comprometidos o configuraciones / comportamientos inseguros
- **Alta probabilidad de compromiso.**

06. Cadena de suministro

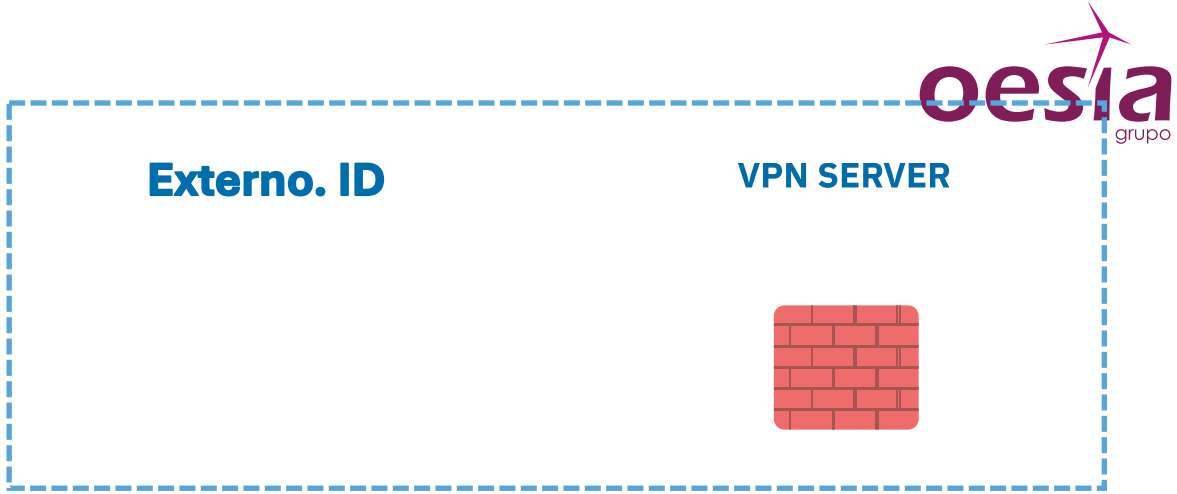
¿Qué podemos hacer con mínimo impacto en lo operativo?



Complementar el escenario típico

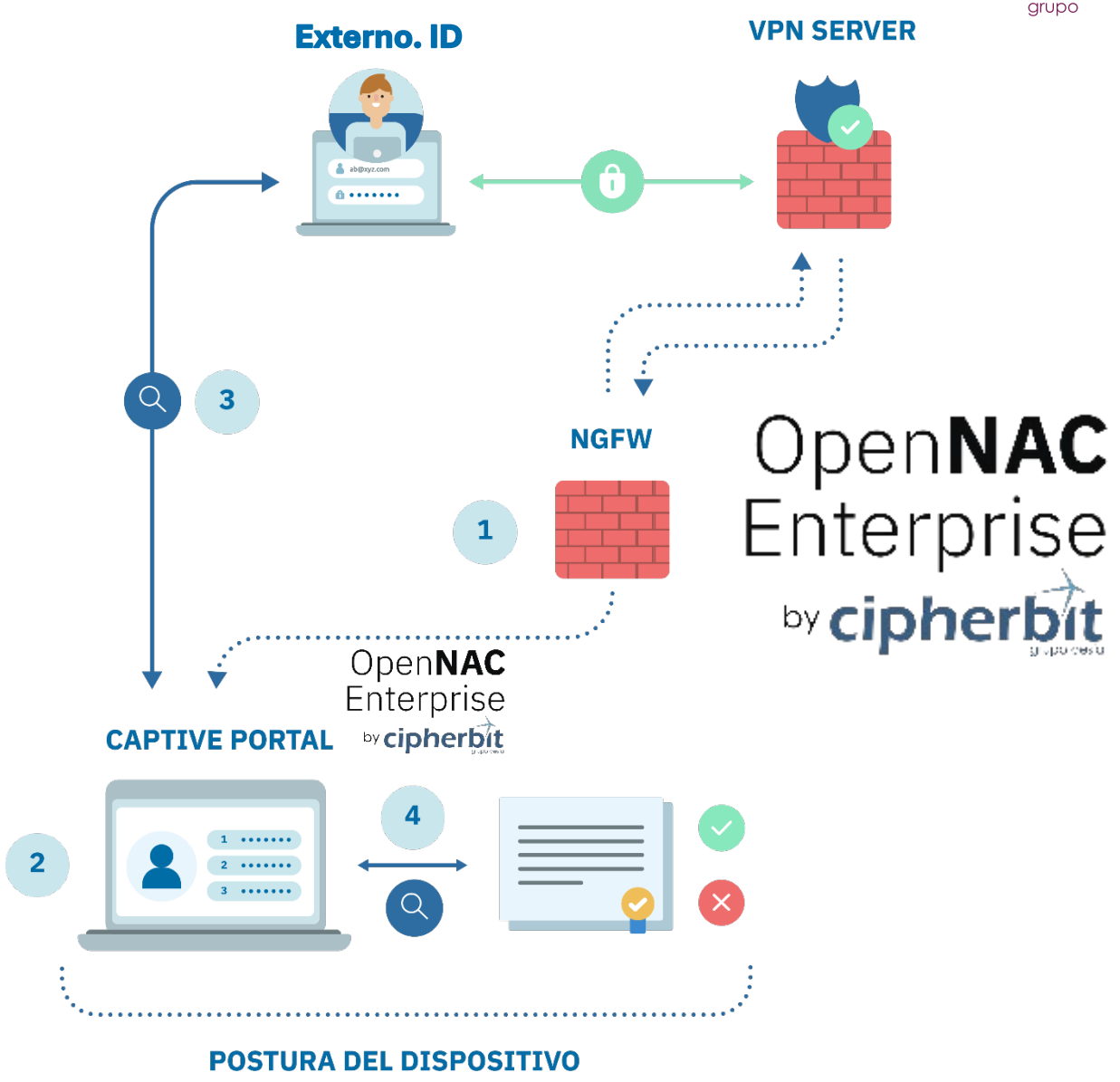
1

Las conexiones **VPN garantizan que la información que fluye hacia y desde el CPD y proveedores de servicios esté encriptada.** Estas conexiones utilizan una **identificación de usuario** para establecer un elemento de confianza en el usuario.



La solución:
OpenNAC Enterprise By Cipherbit

Si la postura del dispositivo cumple con la política del dispositivo, **OpenNAC Enterprise enviará un OK al NGFW para permitir el acceso correspondiente o un NO OK para denegar el acceso** cuando el dispositivo no cumpla.



Evidencias

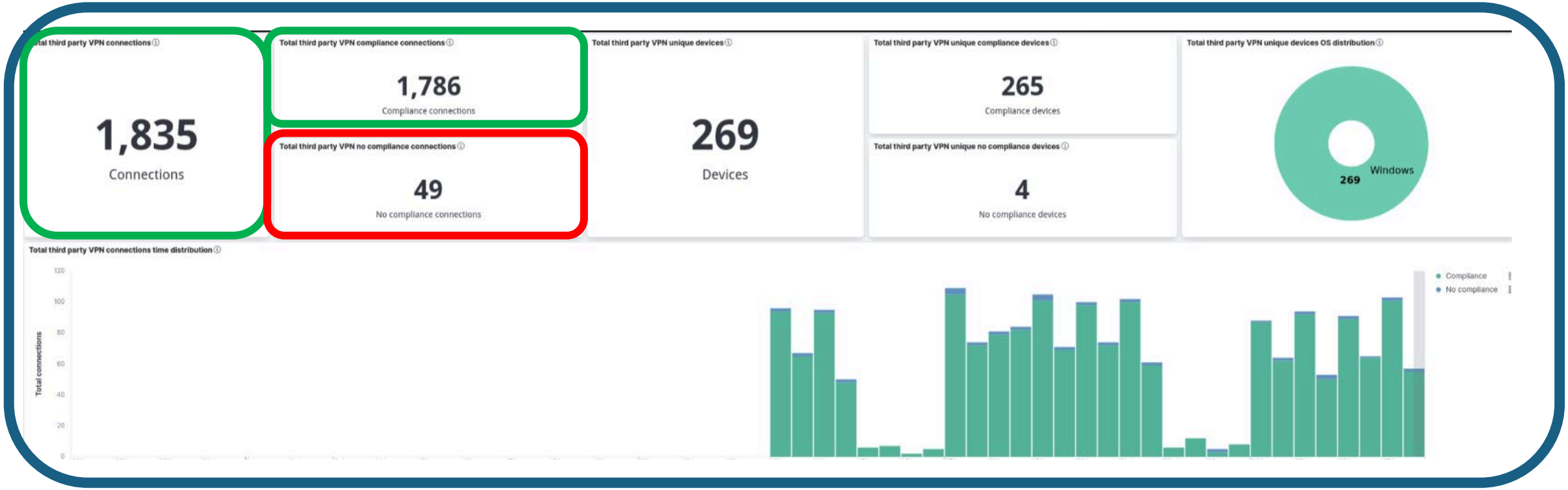


FIG 11: Dashboard de actividad de los terceros

Casos de éxito

DIPUTACIÓN DE LEÓN

Más de **4.000 conexiones VPN**

Aytos <20.000 habitantes

- Acceso Remoto
- Postura Seguridad
- 2FA

GENERALITAT VALENCIANA
Conselleria de Sanitat Universal i Salut Pública

Más de **11.000 conexiones VPN**

4-5.000 conexiones remotas diarias a los servicios centrales (desde: farmacias, hospitales, cárceles, etc.)

OpenNAC Enterprise

Reconocimiento y validación

Contrastada

Solución avalada por **más de 80 clientes**, en sectores críticos, y las certificaciones más relevantes del sector.

Diferencial

- Plataforma **nacional / europea**.
- Diseñada para la **adecuación normativa**.
- Plataforma **agnóstica y adaptable** a diversas infraestructuras.
- **Cercanía** con cliente / mercado nacional.

CONFÍAN EN NOSOTROS

Generalitat Valenciana – Conselleria de Sanitat Universal i Salut Pública

Universidad de Sevilla

Diputación de León

DSN

PORTCASTELLÓ

Generali

COLABORANDO CON

CN-CERT

PUBLICADOS POR

Gartner

Situación Geopolítica – Soberanía Nacional

CERTIFICADOS POR

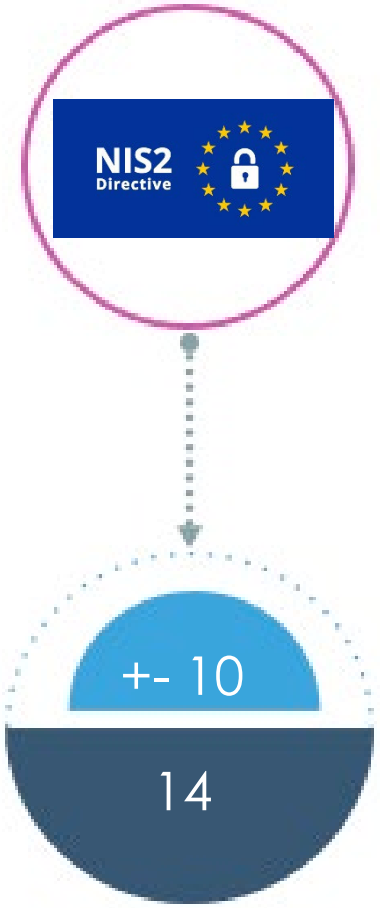
CCN-PYTEC

Incluida en Catálogo STIC-105 desde 2018

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

OpenNAC Enterprise
Aporte al cumplimiento de NIS2

Aporte al cumplimiento de NIS2



¿Cómo se cumple?

Implementando medidas de gestión de riesgo de ciberseguridad entre las cuales están (Artículo 15):

10/14 requerimientos con OpenNAC Enterprise

- **Seguridad en la Cadena de Suministro**
- **Gestión de activos**
- Políticas de control de acceso
- Seguridad de redes
- ..

oesia grupo

Crear un mundo mejor, más eficiente, seguro y sostenible

oesia networks grupo oesía

tecnobit grupo oesía

cipherbit grupo oesía

UAV Navigation grupo oesía

inster grupo oesía

rvegag@oesia.com