¿Quién responde cuando roban o filtran datos a tu cooperativa?

cooperativas agro-alimentarias Castilla-La Mancha

Faten Facilities

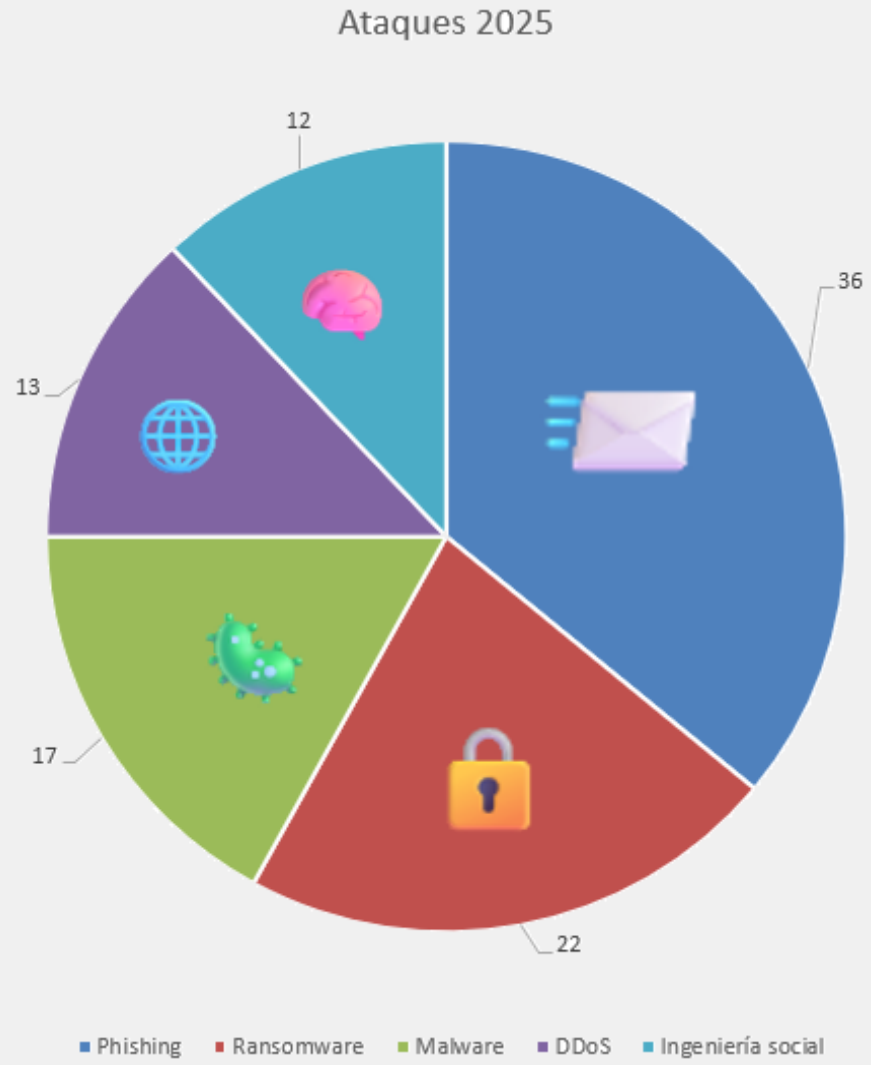
Comunitelia

FORTINET

Principales ataques

Roberto López
Fortinet Team Leader SE Region Centro

Situación en España



Datos 2025

- Cerca de 35000 casos de ataques cibernéticos a empresas (por 31540 casos en 2024).
- El 70% a empresas con menos de 250 empleados.
- Por sector:
  - Transporte – 24,6%
  - Financiero – 23,8 %
  - TIC – 14,1 %
  - Energia – 8,8%
  - Agua – 5%
  - Resto – 23,7%

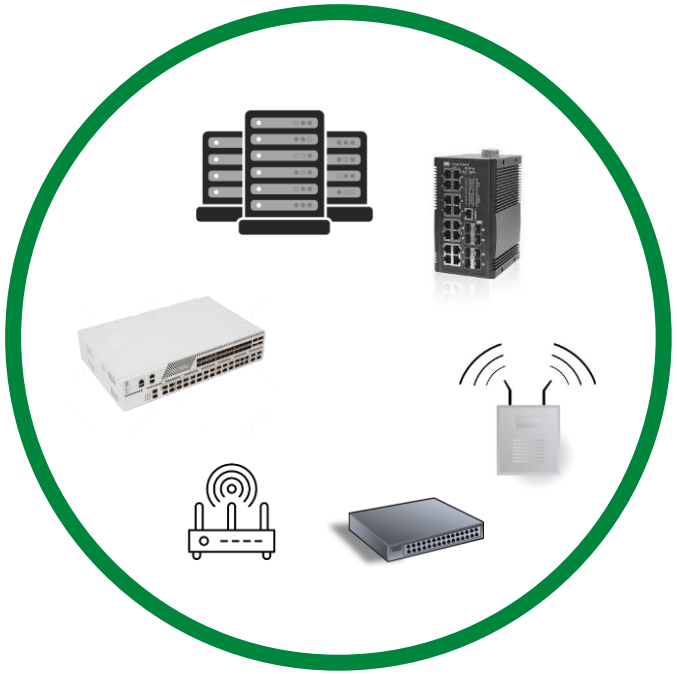
Situación en España

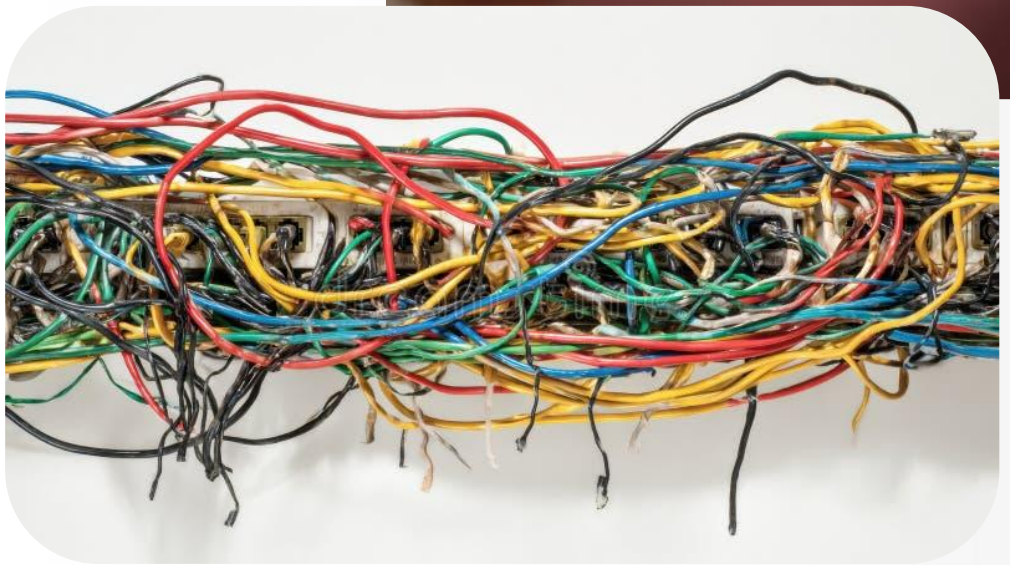
Un ciberataque paraliza Agriconsa, una de las empresas de zumos más importantes de la Comunidad Valenciana

Las ciberestafas que están proliferando a raíz de la implantación de Verifactu

Ciberataques contra pymes en Galicia: «La mitad de las que sufren un secuestro de datos cierran en menos de un año»

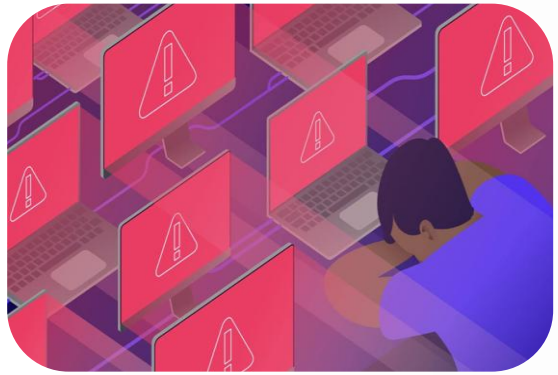
Conectividad

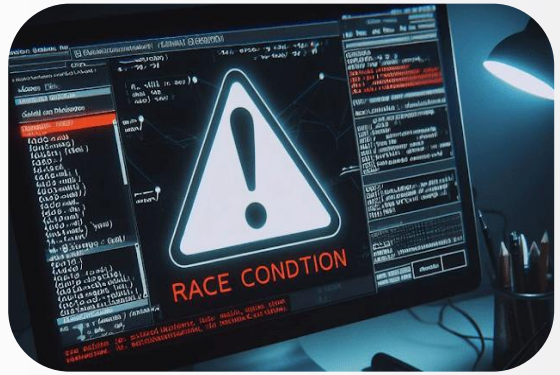




Faten Facilities

Privilegios para todos

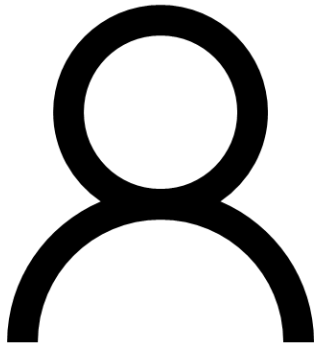


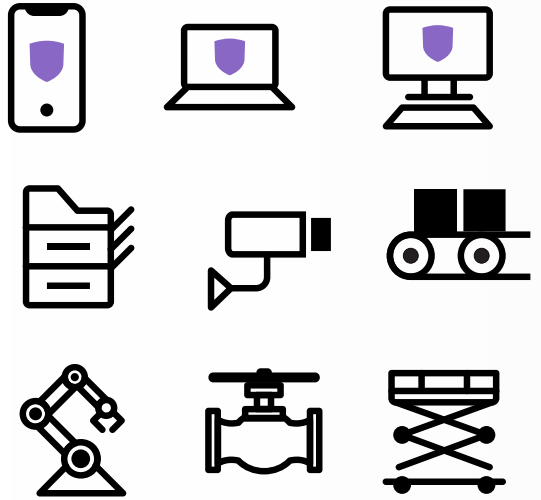


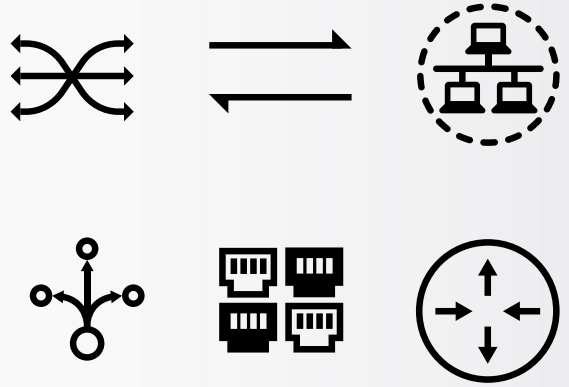
Faten Facilities

¿Qué tengo?

¿Qué tengo?



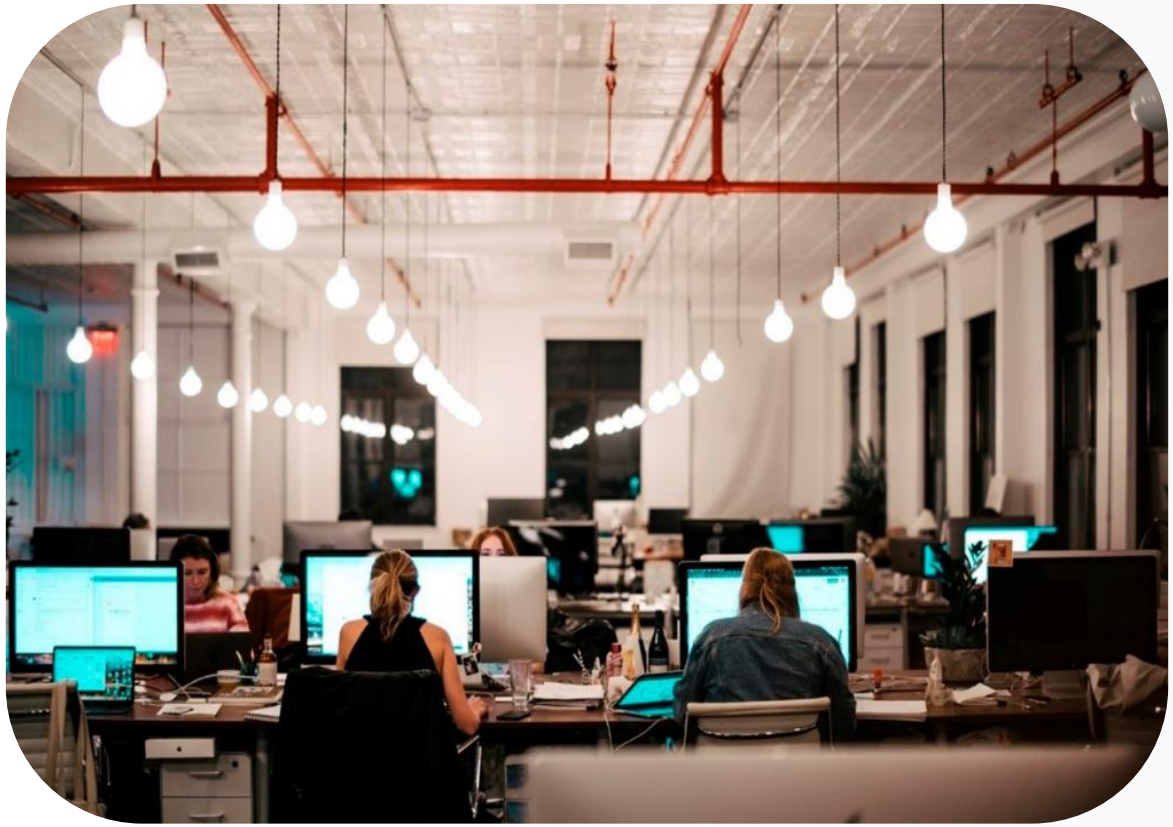




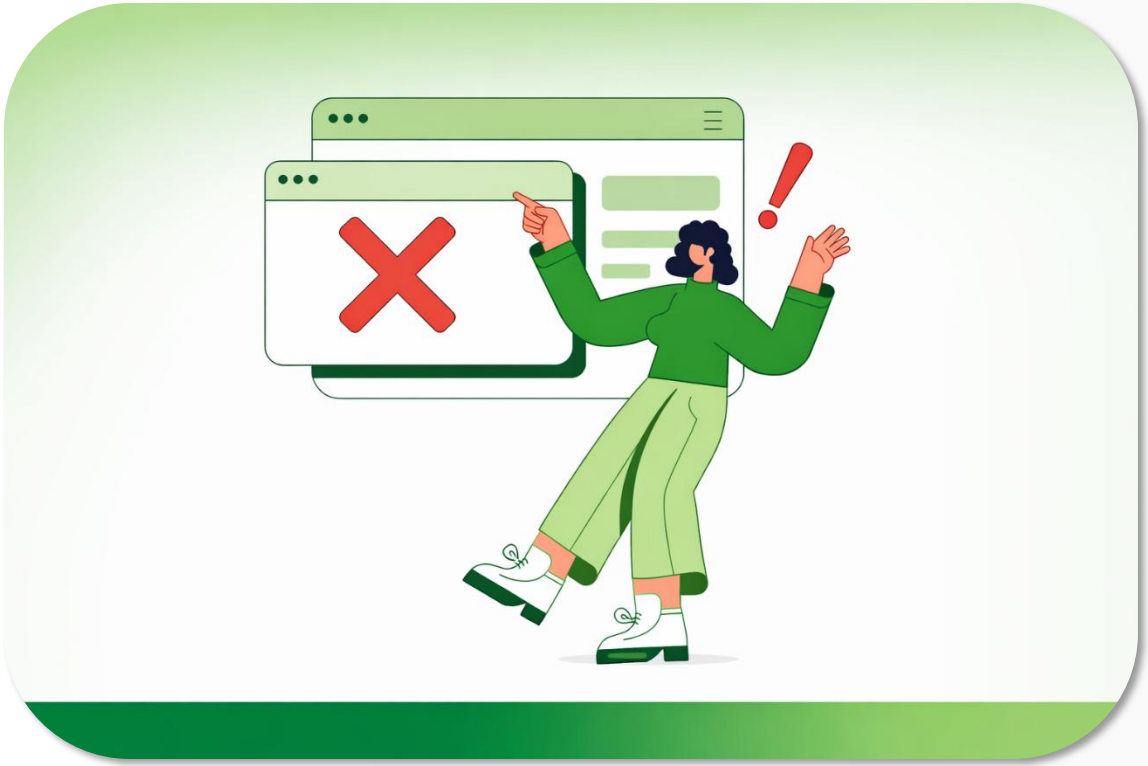
Principales errores humanos

Adrián García
Técnico especialista en Ciberseguridad

Principal foco de la ciberseguridad

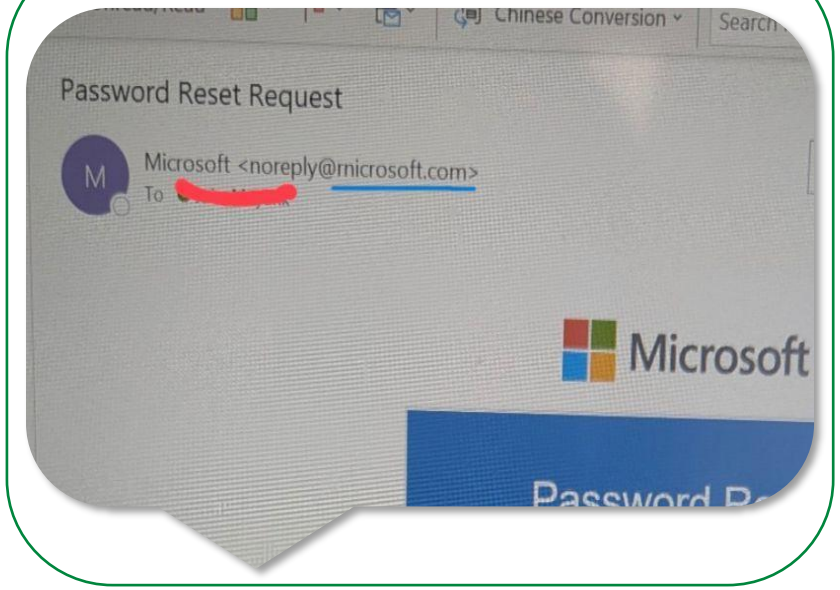


Principales errores humanos

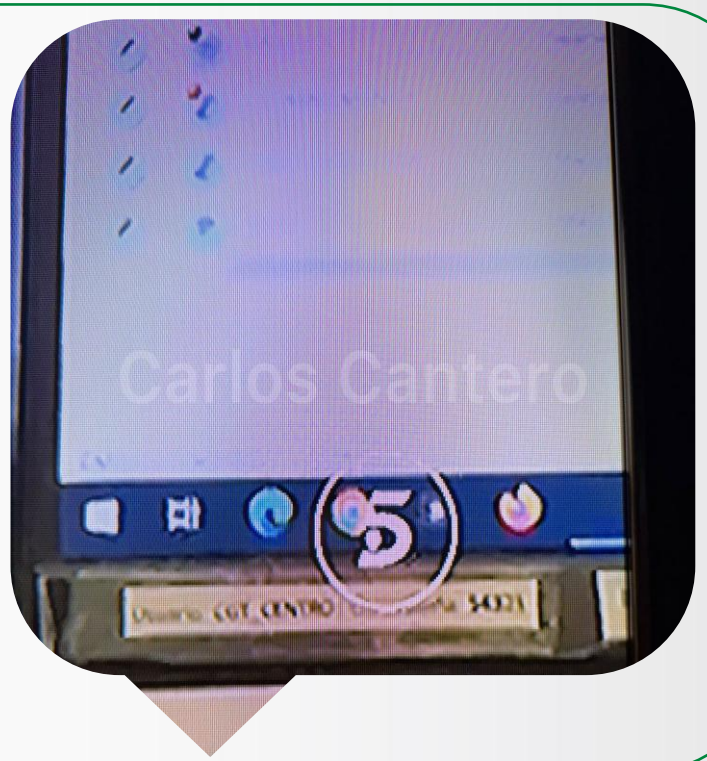


Casos REALES

Typosquatting



Filtración DGT



Faten Facilities

Casos CERCANOS

Faten Facilities

Protégete

Responsabilidades de los presidentes ante NIS2

Ángel Cantón
Director en Comunitelia-Faten

NIS y NIS2: Normativa Europea de Ciberseguridad

Directiva NIS2 (UE) 2022/2555
Nueva normativa europea que refuerza la ciberseguridad en todos los sectores estratégicos.

NIS (2016)
Aplicable a empresas esenciales: Administración Pública, Salud, Banca, Energía, Transporte, etc.

NIS2
Amplía el alcance y exige mayores medidas de prevención, control y gestión de riesgos en todas las empresas de la UE.

Protección de la Información sensible en la Cooperativa

La seguridad digital es clave para garantizar la continuidad del negocio.

Protección de datos críticos
Número de cuenta de los socios, datos fiscales, pagos, facturación y producción…

¿Qué ocurriría si, en plena campaña, un ciberataque paraliza los sistemas de la cooperativa?

¿Cómo continúa tu actividad si la empresa se detiene en plena campaña?

Suplantación de identidad
Un atacante puede hacerse pasar por un proveedor o un socio y desviar pagos a cuentas fraudulentas.

Responsabilidades de los presidentes y Gestores de las Cooperativas NIS2

1. Responsabilidad Legal Directiva:

"Si los **directivos** no implementan medidas adecuadas de ciberseguridad, pueden ser considerados **responsables directos** en caso de un ataque, según la directiva NIS2."

Fuente: NIS2, Artículo 18: "Los directivos deben asegurar la adopción de medidas adecuadas para garantizar la ciberseguridad y proteger la infraestructura crítica."

2. Sanciones Económicas:

"No tomar medidas de ciberseguridad adecuadas puede llevar a la **pérdida de confianza por parte de los clientes y socios**, lo que afectaría gravemente la reputación de la cooperativa."

Fuente: NIS2, Artículo 23: *"Los incidentes de seguridad pueden afectar la relación de confianza entre las empresas y sus clientes."*

3. Pérdida de confianza y daño reputacional:

"El incumplimiento de las normativas de NIS2 puede resultar en **sanciones** de **hasta 10 millones de euros o el 2% de la facturación anual** de la cooperativa, lo que pone en riesgo la estabilidad financiera de la organización."

Fuente: NIS2, Artículo 26: "Las autoridades competentes pueden imponer sanciones económicas a las organizaciones que no cumplan con los requisitos de seguridad establecidos."

Faten Facilities

4. Responsabilidad Penal:

"En caso de negligencia, los directivos pueden ser sujetos a responsabilidades penales si no toman las medidas necesarias para proteger los sistemas de la cooperativa."

Fuente: Fuente: Leyes nacionales basadas en NIS2: "Los directivos pueden ser penalizados si se demuestra que no han implementado las medidas de seguridad adecuadas para proteger los datos y sistemas críticos."

5. Parálisis de la Operación y Costos de Recuperación

"Un ataque cibernético puede paralizar las operaciones de la cooperativa, causando días o semanas de inactividad, lo que implicaría pérdidas económicas significativas y altos costos de recuperación."

Fuente: Informe "Cost of a Data Breach Report 2021" de IBM: "El costo promedio de una violación de datos es de 4,24 millones de dólares, y las empresas sin medidas de seguridad adecuadas enfrentan mayores costos de recuperación."

6. Inspecciones y Auditorías de Cumplimiento:

"Si la cooperativa es auditada y no puede demostrar el cumplimiento con los estándares de NIS2, los directivos podrían enfrentar **sanciones administrativas y la pérdida de contratos clave**."

Fuente: NIS2, Artículo 17: "Los Estados miembros deben llevar a cabo auditorías para verificar el cumplimiento de las normativas de ciberseguridad."

Incibe: Referencia en Ciberseguridad en España

Organismo de referencia en España en materia de Ciberseguridad

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

Publica informes, alertas y estadísticas sobre el impacto real de los ciberataques en empresas.

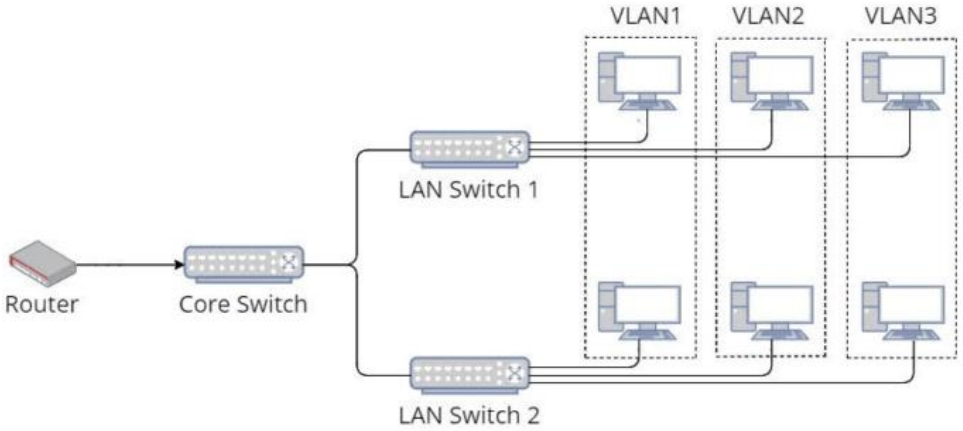
Fuente clave para conocer la evolución y riesgos actuales en España.

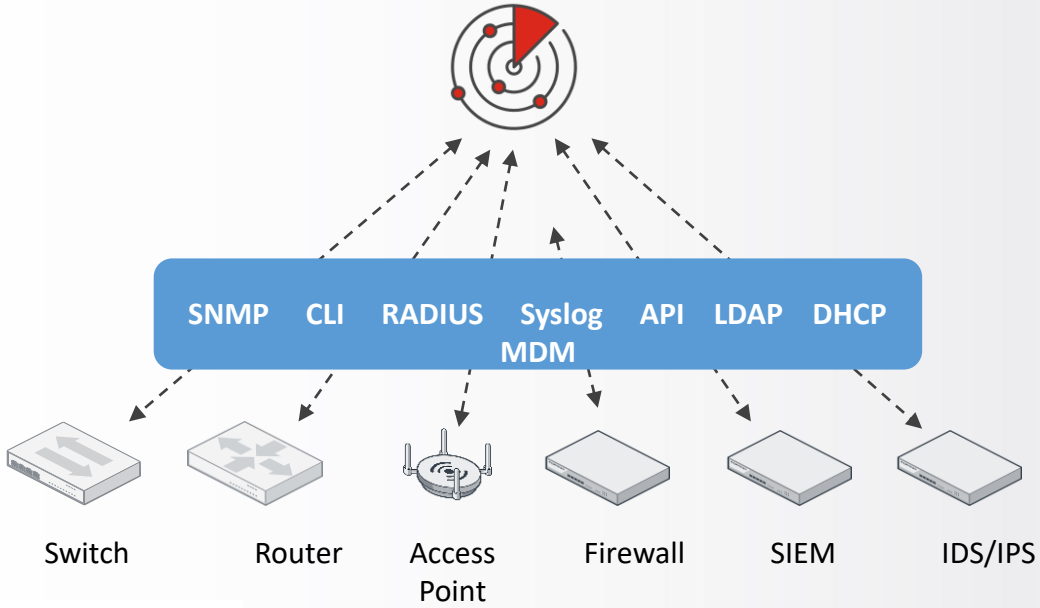
Medidas de Protección

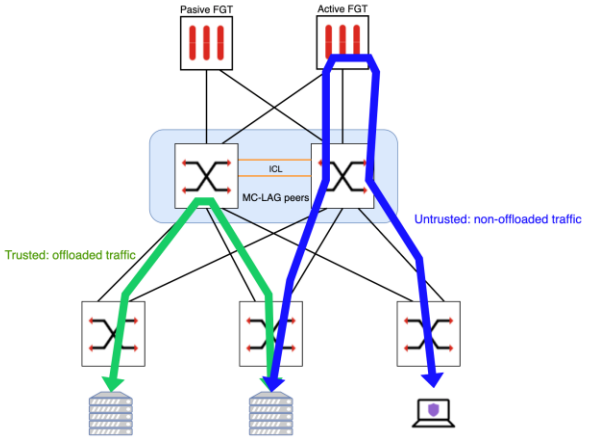
Roberto López
Fortinet Team Leader SE Region Centro

Faten Facilities

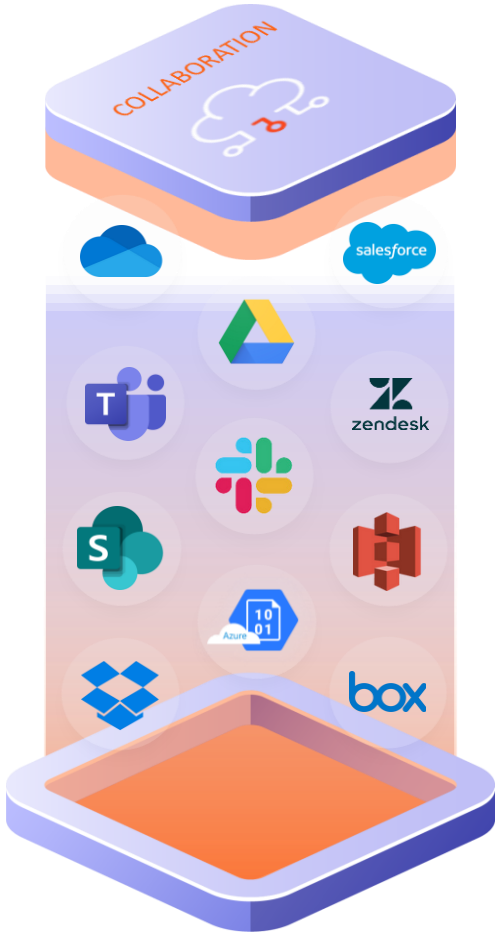
Conectividad segura y controlada







Correo/Teams seguro



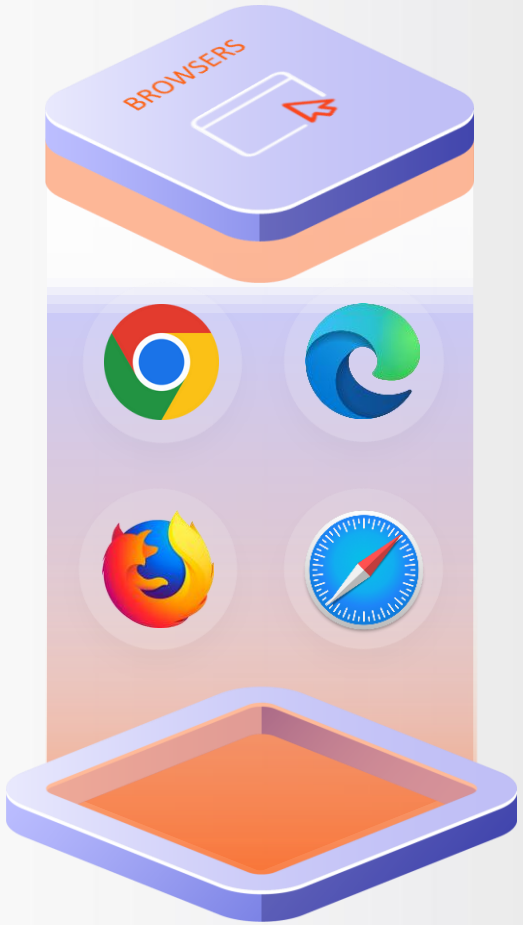
Recursive Unpacker
Anti-Evasion

Spam Filter
Anti-Spam (email)

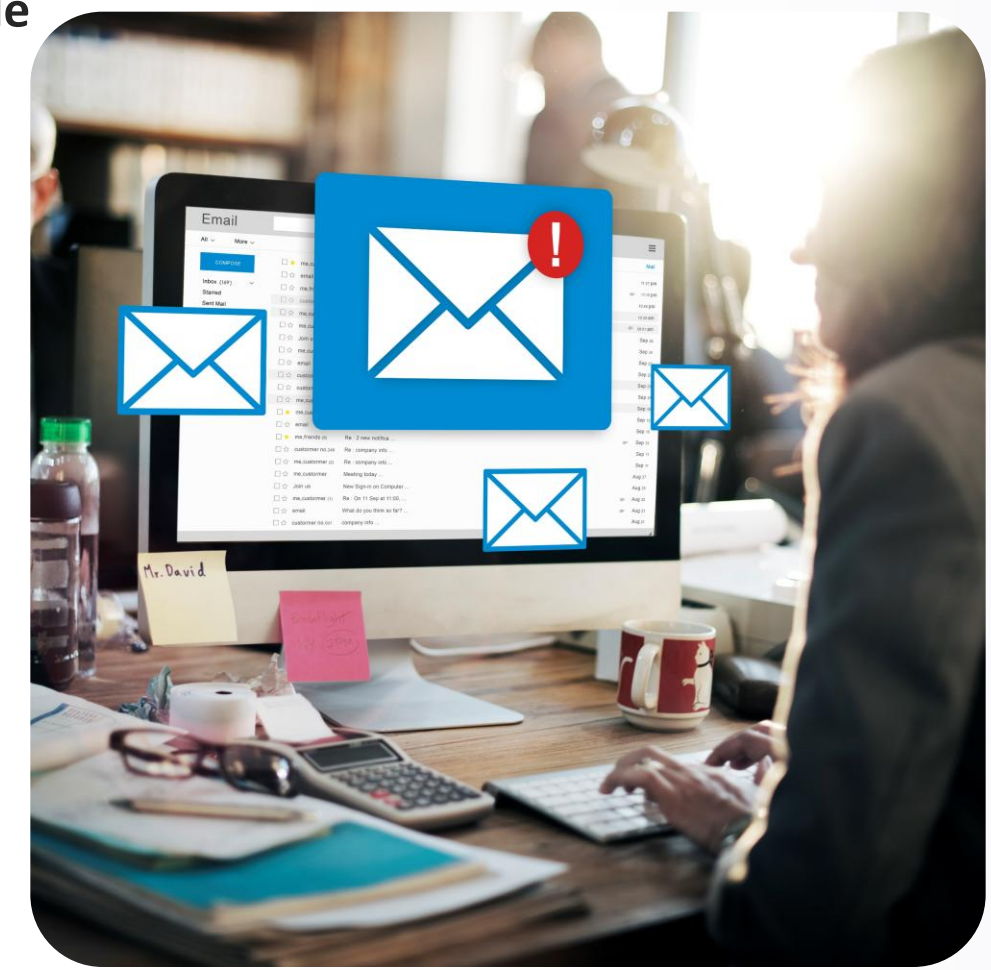
Anti-BEC & ATO
Payload-less Threats & Account Takeover

Anti-Phishing
URL analysis, AI & Image Recognition

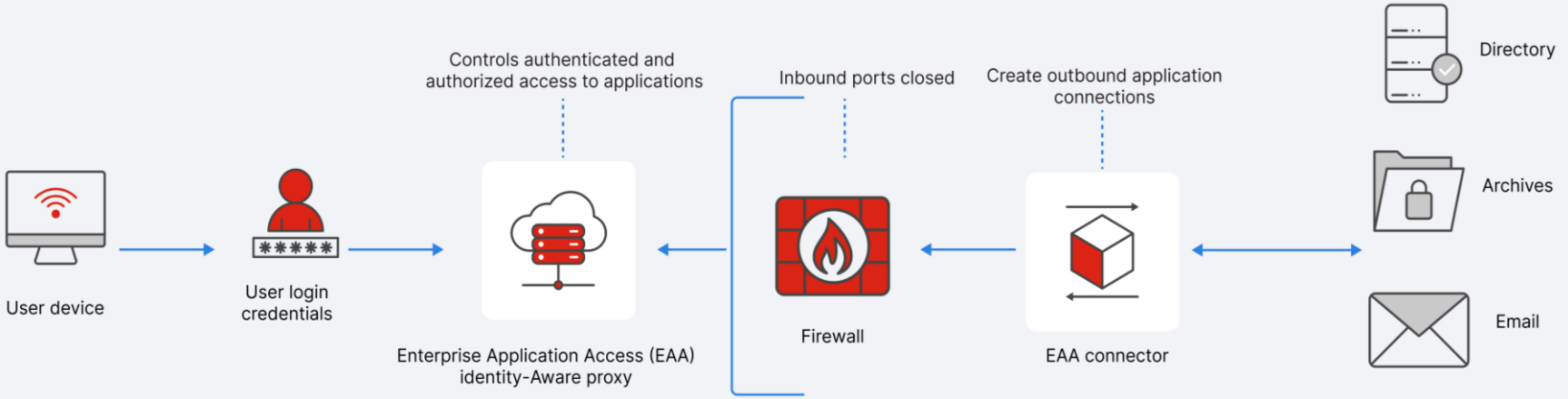
HAP™
Dynamic Analysis Zero-days & Unknown Attacks



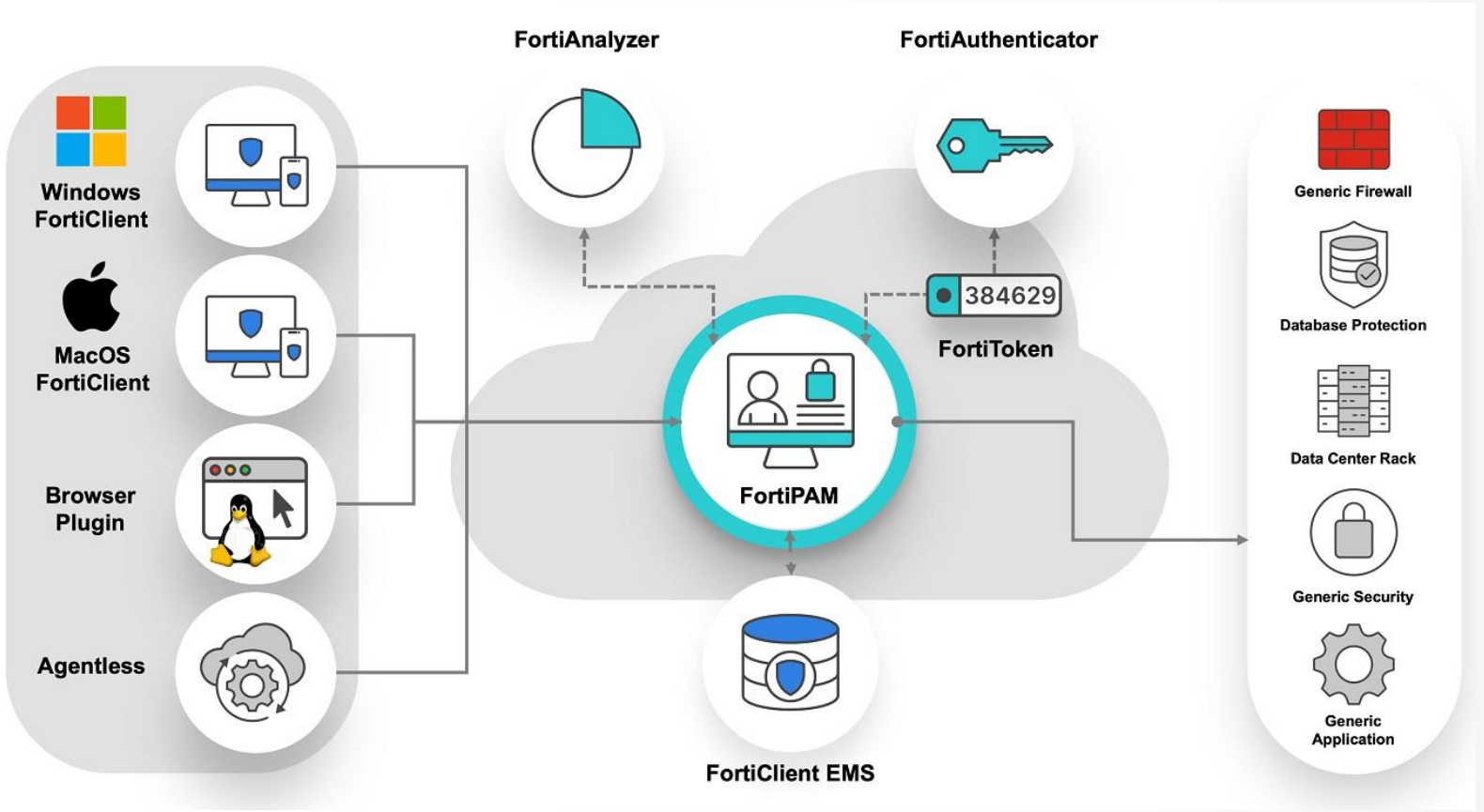
Correo/Teams seguro simple



Sólo quien debe acceder



Privilegios controlados



Faten Facilities

Privilegios controlados

Logging

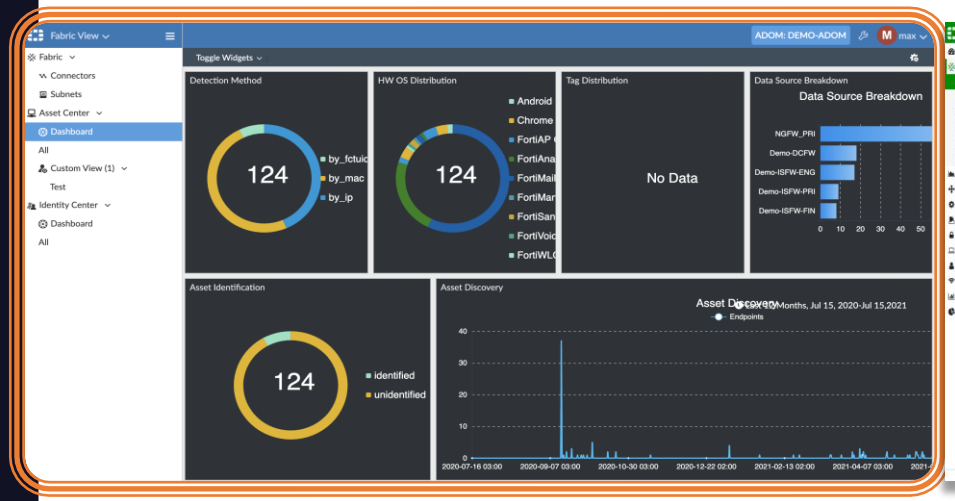
Network Visibility

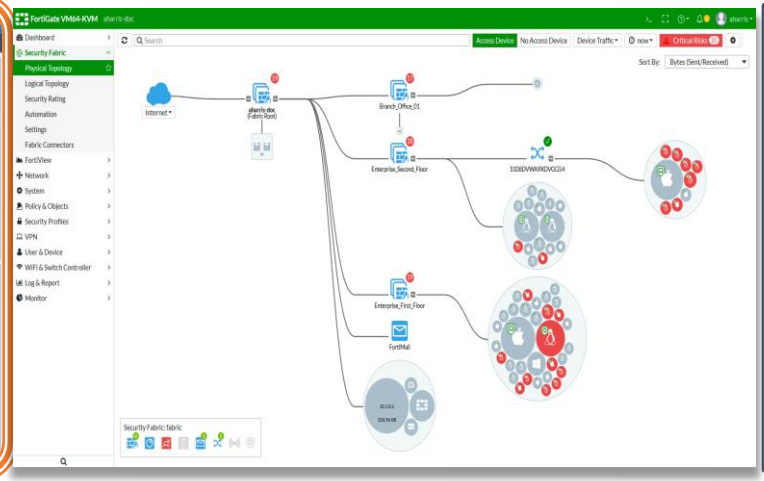
Security Analytics

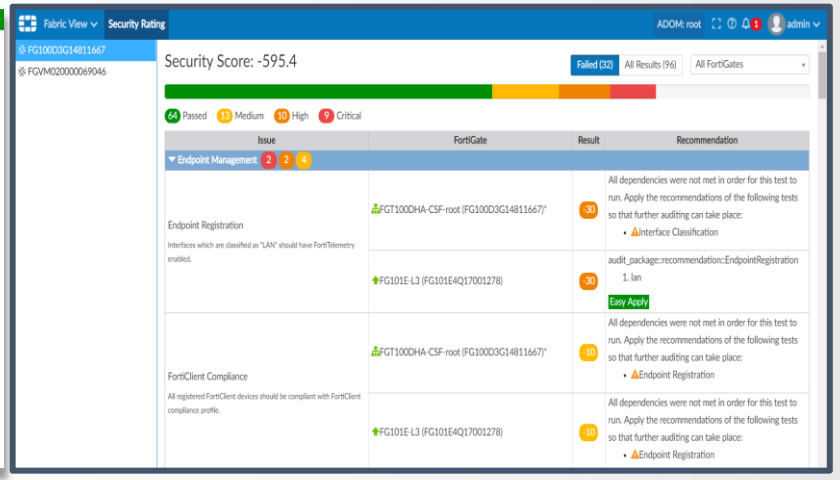
Threat Detection

Automation

Incident Response







Faten Facilities

Autoevaluación de seguridad:

https://forms.gle/YVQb62UNmNUkB7fe9

926 16 11 14

unioncoop@comunitelia.com

cooperativas agro-alimentarias Castilla-La Mancha

Comunitelia

FORTINET