LinkedIn TOP 2020 STARTUPS España

Tendencias en ciberseguridad

Presentación

- Juanjo Pérez Mostajo
- COO

  Wise Security Global
- Ingeniero Técnico Informática.
- Docente Máster en Ciberseguridad.

  Universidad Internacional de Valencia

2001

ESCERT

Inet Secur

2006

tb·security

CaixaBank

cesicat

2014

WISE SECURITY

CaixaBank

Fundación Bancaria "la Caixa"

vente-privee

privalia

2019

wisesecurity GLOBAL

CaixaBank

Fundación Bancaria "la Caixa"

AXA

WISE SECURITY GLOBAL

Nuestro ADN

LinkedIn TOP 2020 STARTUPS España

wisesecurity GLOBAL

CyberSECURITY & CyberTRUST

Nuestra **misión** es nuestro continuo reto: Proteger la actividad de nuestros clientes mediante la generación de ciberentornos confiables y seguros que les permitan mantener y mejorar la confianza de sus stakeholders.

CyberSecurity

Research

Ethical Hacking and Vulnerability Assessment

Managed Cybersecurity Detection and Response

CCSA Cyber Compliance&Security Assessment

Innovation

PaaS SaaS PROFESIONAL SERVICES

Drydor

HaaS
Hacking as a Service

- Pentesting
- Simulation of advanced adversaries
- Web Application Audit
- Mobile Apps Audit
- WiFi Audit
- Cloud Audit
- SecDevops
- Auditorías de código

Drydmanager

WarZone

CSOC

Net Alarm

SOPHOS

- Deployment and operation (surveillance) of multi-brand early warning systems
- Surveillance and treatment of cyber threats
- Malware Laboratory
- DRIR (in-situ response and electronic testing)
- Members of the CERT® community

Haunt Keeper

- Home networks protection
- Preventing incidents such as information leaks or ransomware

INTEGRATED CYBERSECURITY MODEL

Wise CISOaaS

Own Methodology

Reporting C-BSC

Jira

- Assessment of cyber threats.
- Strategy, model and governance of cybersecurity
- Regulatory compliance management (GDPR, NIS, PCI-DSS, ISO 27000, ENS)
- Cloud cyber security implementation
- Mobile cyber security deployment
- Awareness programmes
- User training

Main references

MULTISECTORIAL

vueling, AXA, Adeslas SegurCaixa, CaixaBank, zetes, LABORAL kutxa, wefox, BAXI, habitissimo, HomeServe, Fundació "la Caixa", markennovy, GRUPO CONSTANT, NEINVER, manfisa, MEDEMASA, FRENDISA, GINSA, antevenio, COFARES, FAES FARMA, Firmenich for good, naturally

Customer Case Study

· Monitor and deter
· Cyber security offensive
Web applications
Mobile app
Infrastructure
APIs
Biometric authentication systems
Precision tool: training fields

Own tools
Management of weaknesses
Management of weaknesses analysis
Reporting / Automatic reports
Training area

- **Monitor and deter:** Centre specialised in handling the security of our customers' problems, which range from monitoring with NetAlarm and the review of infrastructure with Drydor to the design, implementation and operation of security in multi-brand early warning networks.

- Systems, perimeter, endpoint
- Skills 24/7
- CSIRT/CERT®

Advanced advice and implementation of cybersecurity plans and construction of the Integrated Cybersecurity Model Especially in small and/or medium-sized companies that do not have mature cybersecurity frameworks and which are provided with an external in-company CISO that can implement protocols and make security an expert aspect of the company.
Optimisation of processes:
Large corporations with a proven track record in cybersecurity (banking and

Legal Basis

ISO 27000

GDPR

ENS

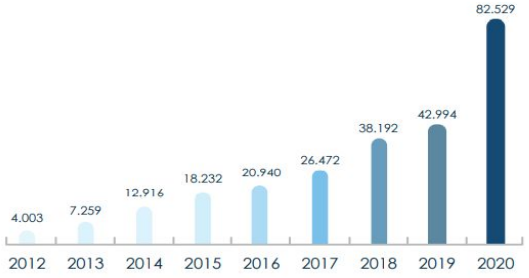
Directive NIS

PCI-DSS

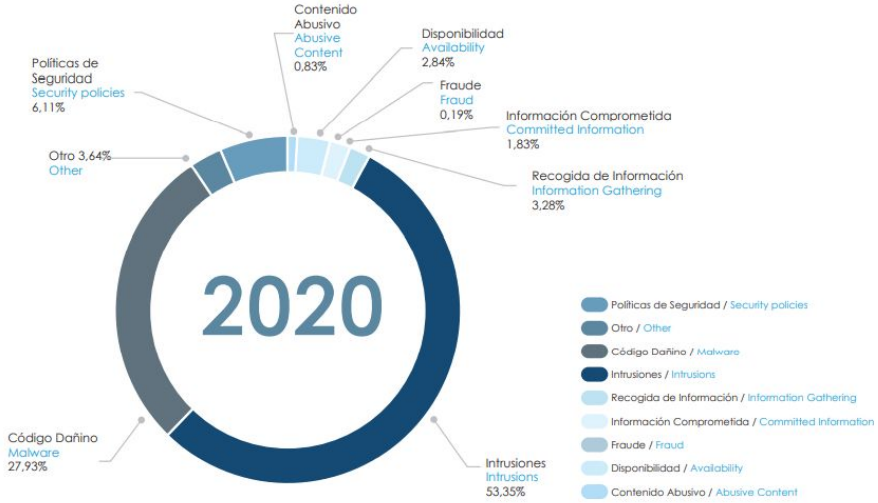
CSF – NIST

El contexto

In 2020 the CCN-CERT detected a total of 82,529 incidents, 39,535 more than in 2019.



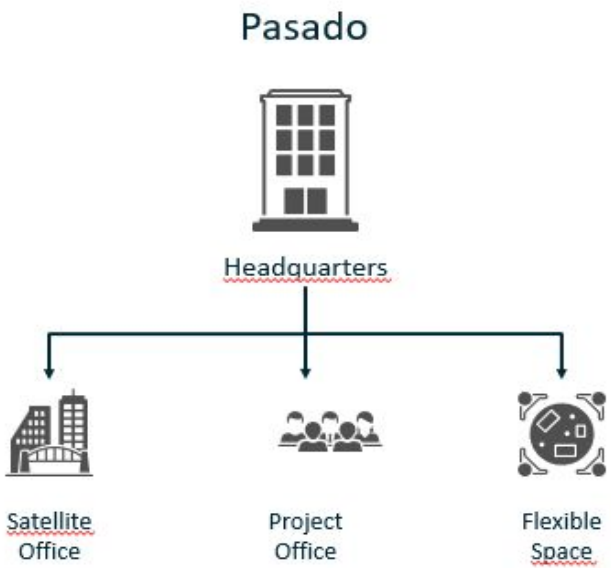
Incidentes gestionados por el CCN-CERT
Incidents managed by the CCN-CERT



Tipología de los incidentes gestionados
Types of incidents managed

Nuevas situaciones

El concepto tradicional de oficina está cambiando a gran velocidad



El contexto

¡ALERTA! CIBERATAQUES EN EL TELETRABAJO

DEFENSA CIBERSEGURIDAD

CNI advierte que el uso de redes domésticas ha multiplicado los ciberataques

“La pandemia y el teletrabajo han supuesto la multiplicación de ciberataques a empresas y organismos a través de las redes domésticas y dispositivos personales de sus trabajadores”.

“Todos somos corresponsables de la seguridad nacional y todos debemos hacer un uso responsable de las tecnologías”.

PAZ ESTEBAN
Directora del Centro Nacional de Inteligencia

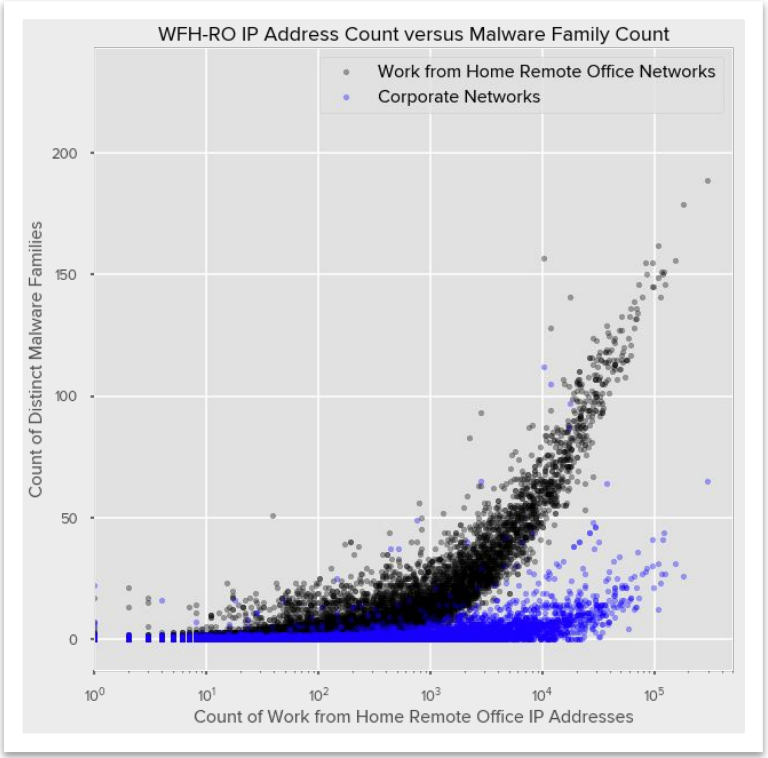
El contexto

¡ALERTA! CIBERATAQUES EN EL TELETRABAJO

LAS REDES DEL HOGAR SON INSEGURAS

”Las redes domésticas tienen una probabilidad **7,5 veces mayor** de tener cinco o más familias de malware que la red corporativa tradicional.”

“El **45% de las empresas presentan malware en las redes domésticas** utilizadas por sus empleados.”



INFORME BITSIGHT
14/04/2020

El contexto

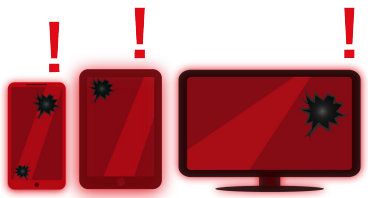
¡ALERTA! CIBERATAQUES EN EL TELETRABAJO

Las **redes domésticas** ofrecen vulnerabilidades potenciales únicas.

Los dispositivos comúnmente expuestos incluyen módems, routers, cámaras, periféricos de almacenamiento y otros **dispositivos IoT**.

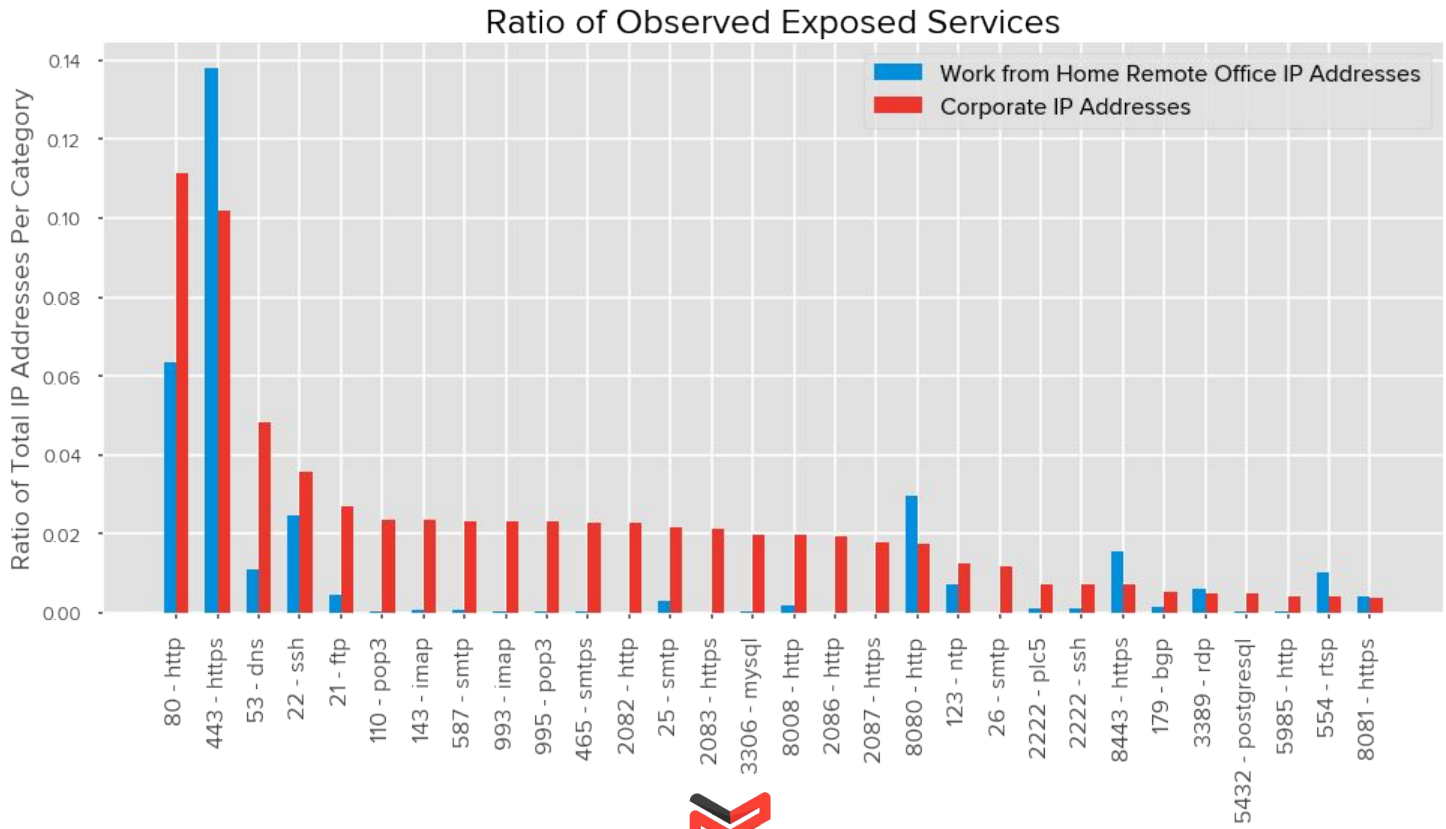
Interfaces accesibles por error y poco actualizadas

25,2% de las redes domésticas tiene servicios expuestos en Internet.



El contexto

¡ALERTA! CIBERATAQUES EN EL TELETRABAJO



El contexto

¡ALERTA! CIBERATAQUES EN EL TELETRABAJO

PROBLEMAS DERIVADOS

Redes comprometidas.

Se disparan los vectores de ataque contra equipos corporativos.

Pérdida de visibilidad de los endpoints (estaciones de trabajo, portátiles, móviles).

Las redes domésticas requieren evolucionar a un espacio con mayor madurez en ciberseguridad, dado que suponen un riesgo para los activos de información tanto del hogar como los derivados del teletrabajo.

Ciberamenazas

CCN-CERT estable una priorización por agentes de la amenaza, según sus motivaciones:

Ciberespionaje: Ciberataques realizados para obtener secretos de Estado, propiedad industrial, propiedad intelectual, información comercial sensible o datos de carácter personal.

Ciberdelito/cibercrimen: Actividad que emplea las redes y sistemas como medio, objetivo o lugar del delito.

Ciberactivismo: Activismo digital antisocial. Persiguen el control de redes o sistemas (sitios web) para promover su causa o defender su posicionamiento político o social.

Ciberterrorismo: Actividades dirigidas a causar pánico o catástrofes en las redes y sistemas o utilizando éstas como medio.

Figura 6 Importancia de las amenazas según el CCN-CERT.

¿Que hacer si me pasa?

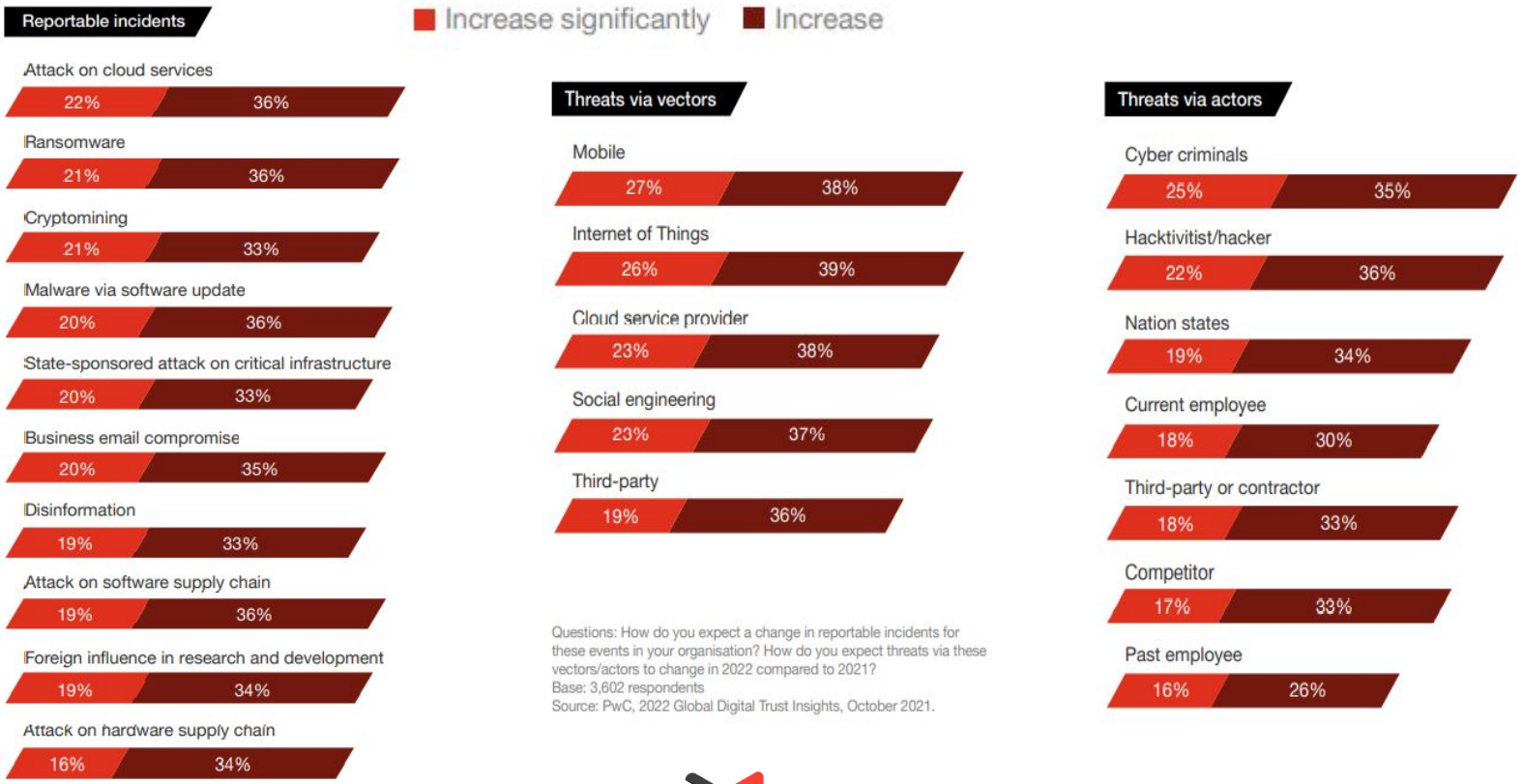
1. Contención
2. Investigación
3. Recuperación

   (el 2 y el 3 se pueden paralelizar)

4. Comunicación
   - Clientes
   - Autoridades competentes con las que tratar
   - Policía
   - Agencia española de protección de datos (más relevante)
     - Medidas previas
     - Medidas correctivas
     - Plan de acción asociado..
   - CCN, Incibe...
   - Seguro
   - Con los malos

Comité de Crisis para Gobernar las fases

Ciberamenazas



Questions: How do you expect a change in reportable incidents for these events in your organisation? How do you expect threats via these vectors/actors to change in 2022 compared to 2021?
Base: 3,602 respondents
Source: PwC, 2022 Global Digital Trust Insights, October 2021.

Y.. ¿Solución?

- Presupuestos limitados – Este problema no es nuevo.. Cuesta encontrar presupuesto

  Seguimos viendo la seguridad como un gasto y no como una inversión

- Escasez de perfiles maduros

  La necesidad va más rápido que la creación del talento. Retención del talento

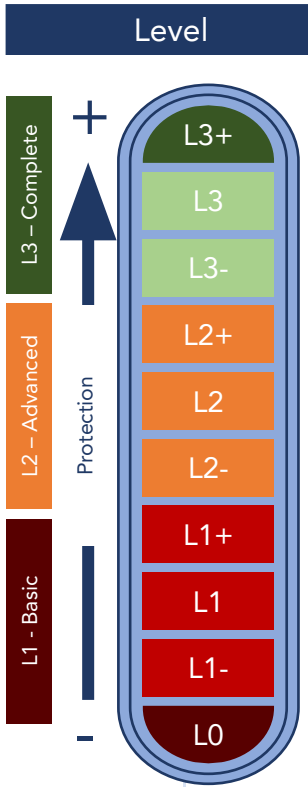
  La ciberseguridad es un servicio muy joven respecto al resto de servicios..

2 grandes problemas…

MADUREZ

RRHH

Madurez



L1

2021

- Monitorización, vigilancia y seguimiento avanzado en la resolución de vulnerabilidades detectadas
- Auditorías de seguridad en el ciclo de vida de SIC

L1+/L2

202 - L1

- Monitorización y vigilancia
- Auditorías de seguridad SIC

L1

202

- Protección de espacio de trabajo de usuario y auditorías de verificación
- Digitalización del proceso de firma

L1+/L2

-

202 L1

- Protección de endpoints
- Formación en herramientas de seguridad

L1

202 1

- Awareness continuo y medición de nivel de cultura
- Concienciación avanzada en colectivos específicos
- Ejercicio pruebas Ing. Social

L1+/L2

-

202 L1

- Definición de la Oficina de Ciberseguridad
- Concienciación inicial
- Ejercicio inicial pruebas Ing. Social

L1

202

- Protección con proveedores TIC SIC
- Seguimiento avanzado vulnerabilidades CERT
- Diseño política actualizaciones
- Diseño política password
- Auditoría backups

L1+/L2

-

202 L1

- Estudio viabilidad firma centralizada
- Inventariado dominios
- Métricas seguridad
- Seguimiento vulnerabilidades CERT

L1

202 1

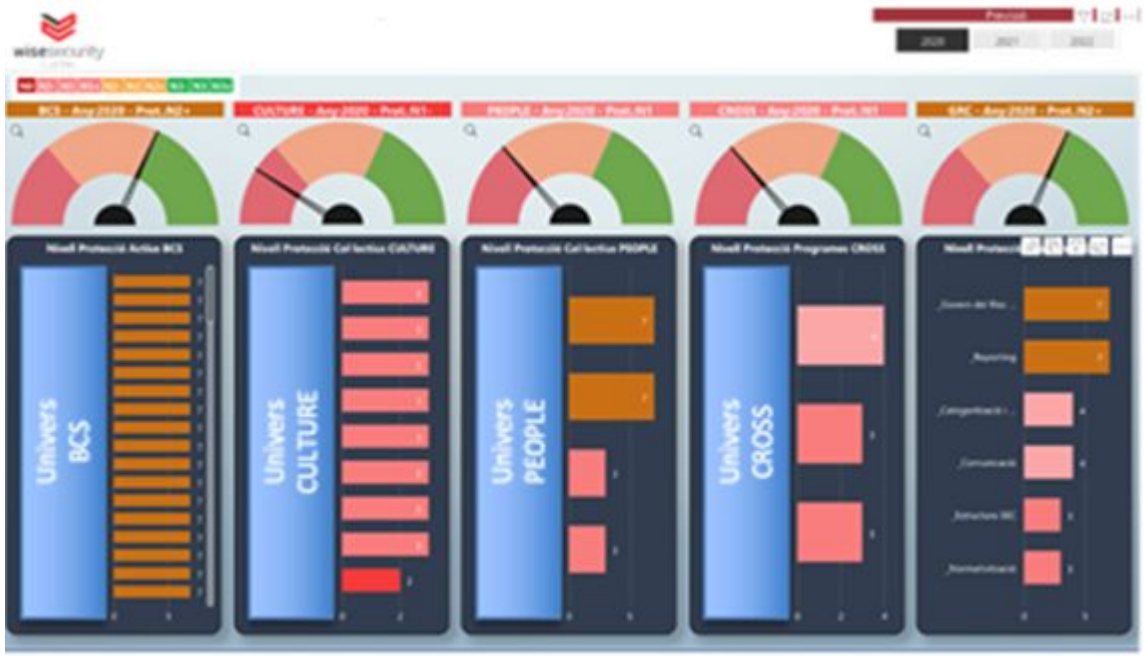
- Alineamiento compliance
- Soporte cumplimiento GDPR
- Métricas seguridad
- Desarrollo e implantación del cuerpo normativo

L1+/L2

202 - L1

- Creación procedimiento reglas de reenvío
- Clausulado proveedores
- Modelización inicial
- Elaboración procedimiento Oficina de Ciberseguridad
- Desarrollo cuerpo normativo
- Definición y ejecución plan ISO27k Delete

Madurez



RRHH

¿Quién nos ayuda? Otros sectores

Alinearnos con Negocio

EMAIL
jperez@wsg127.com

WEB
www.wsg127.com

wisesecurity
GLOBAL

¡GRACIAS!