

JORNADA STIC

CAPÍTULO COLOMBIA

La Prevención Proactiva como elemento diferenciador...



En colaboración con:

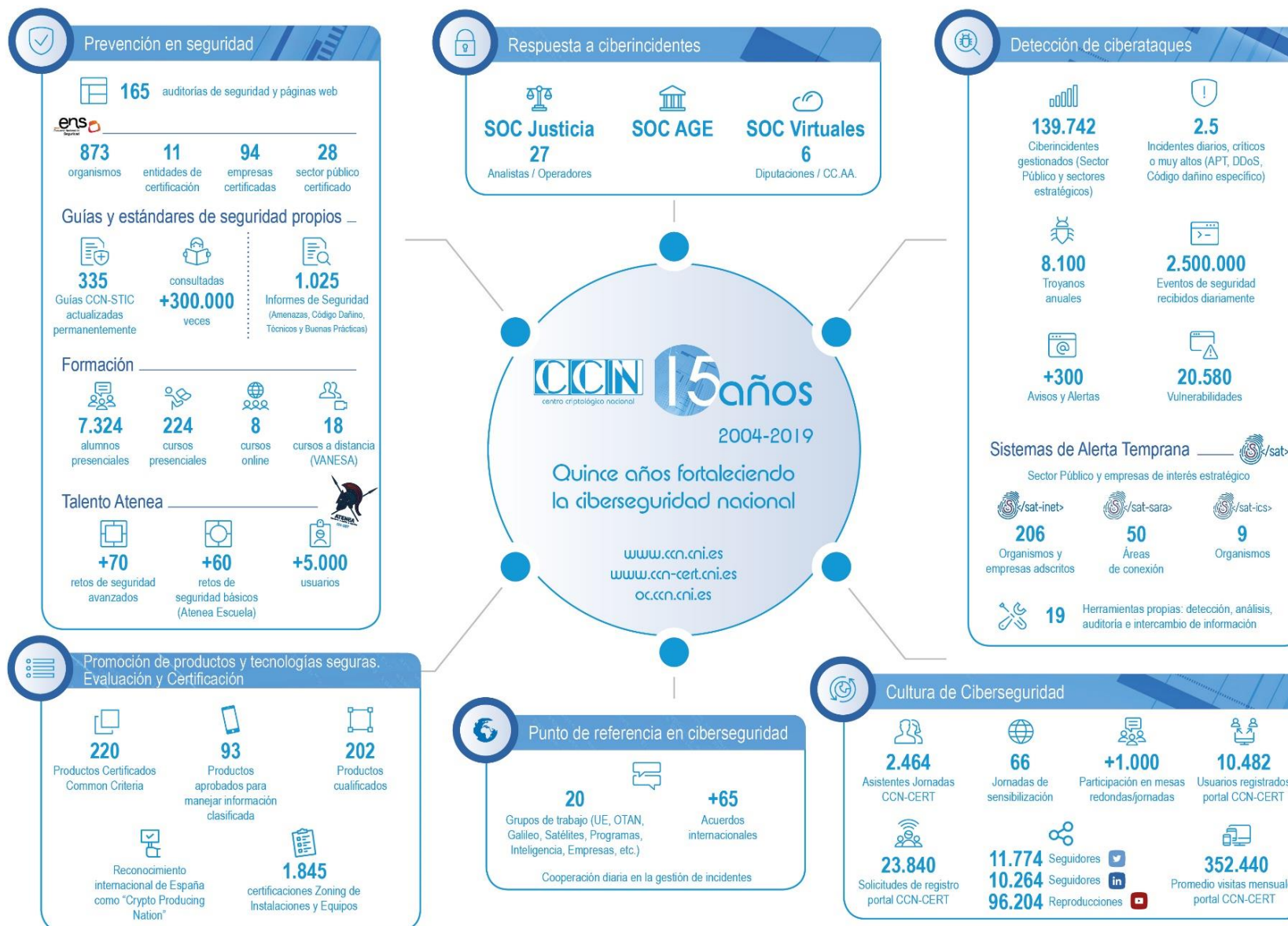




Pablo López

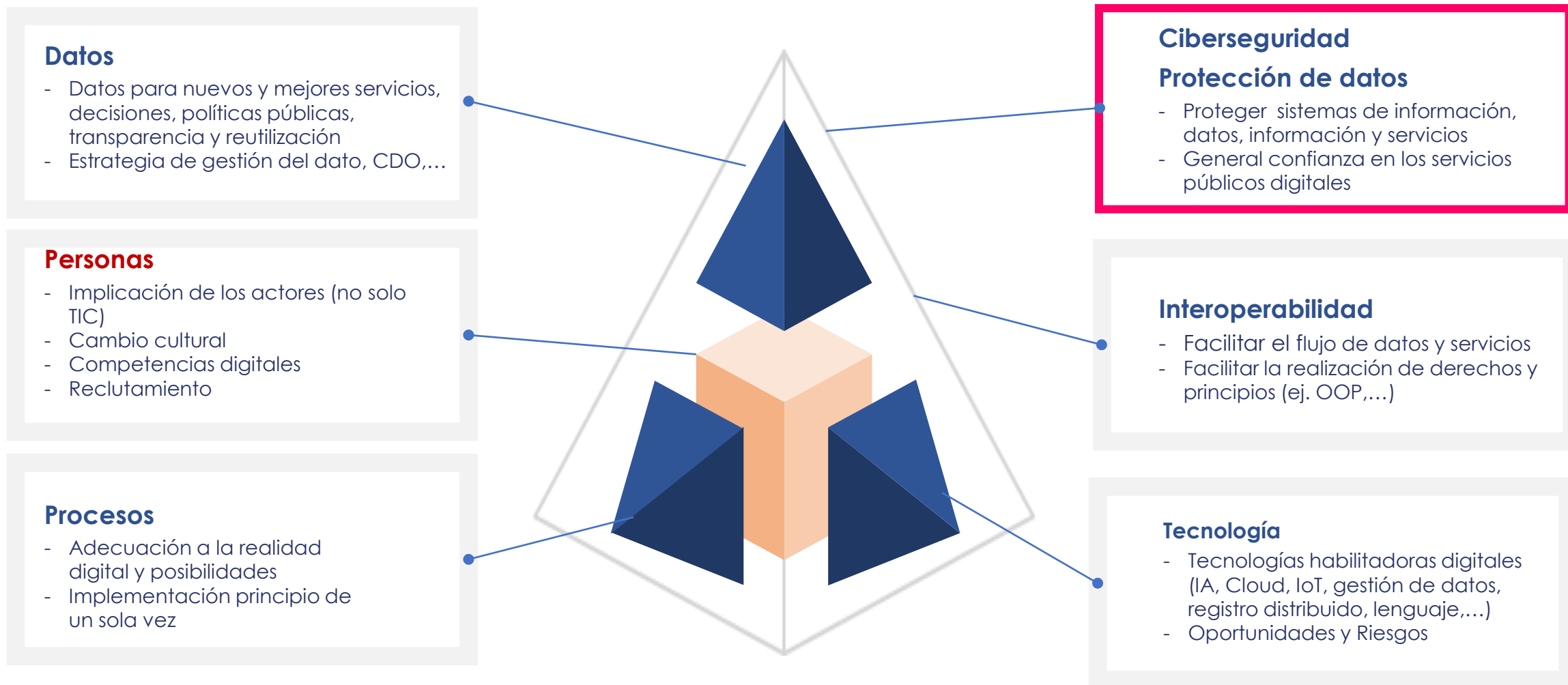
Centro Criptológico Nacional

*Jefe Área Normativa y Servicios
Ciberseguridad*



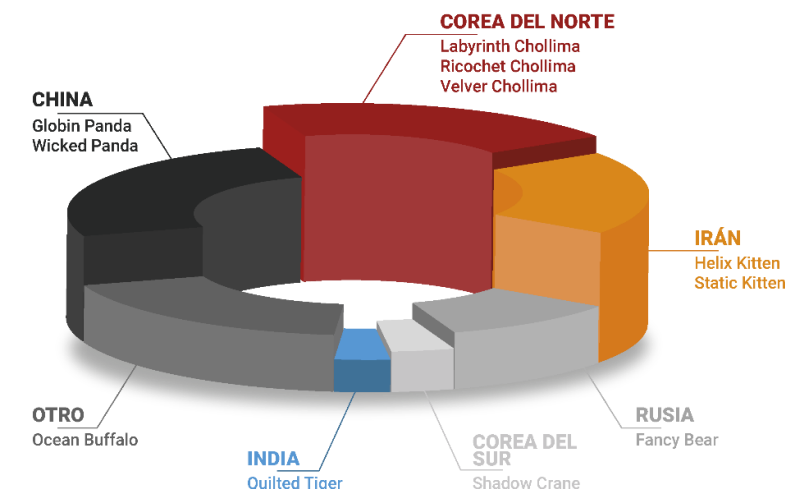
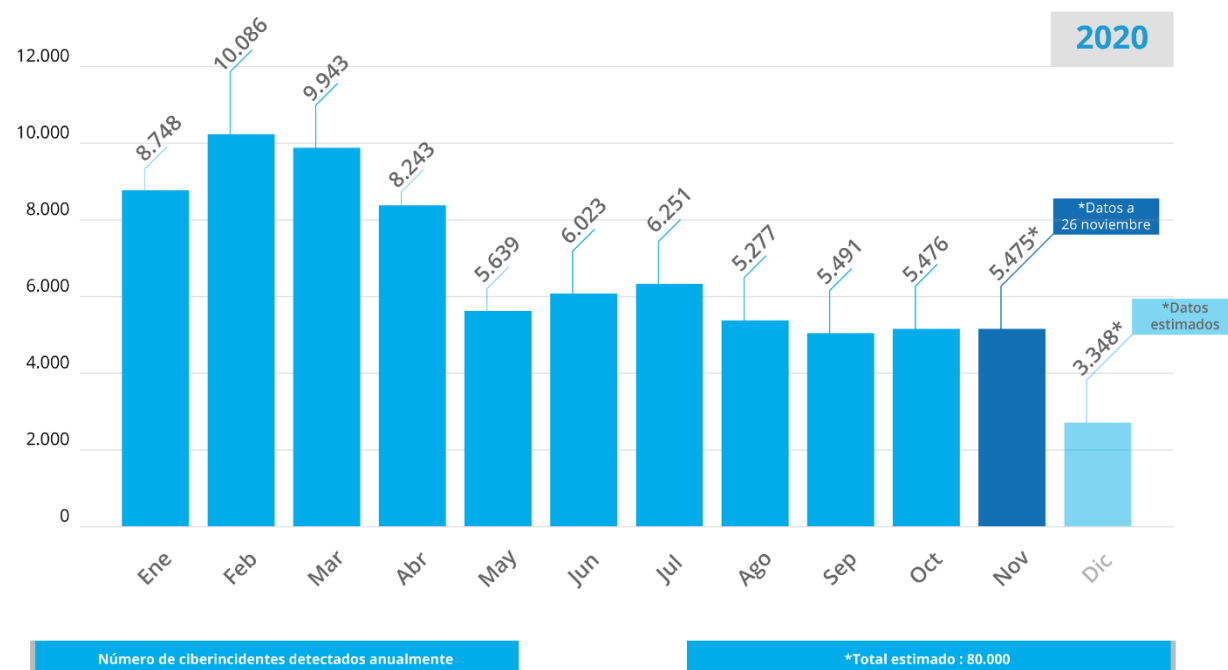
Transformación digital y ciberseguridad

Personas, procesos, tecnología, datos y ciberseguridad



La amenaza en el ciberespacio

- Complejidad y sofisticación de los ataques.
- Deficiencias en la configuración/bastionado de seguridad.
- Falta de adopción de buenas prácticas.
- Carencia de procedimientos de mejora continua.



CIBERAMENAZAS Y ACCIONES QUE USAN EL CIBERESPACIO CON FINES MALICIOSOS

Disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos.
La acciones que usan el ciberespacio como medio para realizar actividades maliciosas o ilícitas.



CIBERESPIONAJE

Amenazas Persistentes Avanzadas



AMAZAS HÍBRIDAS

Acciones militares
Ciberataques
Manipulación de la información



CIBERCRIMEN

Ciberterrorismo
Ciberdelito

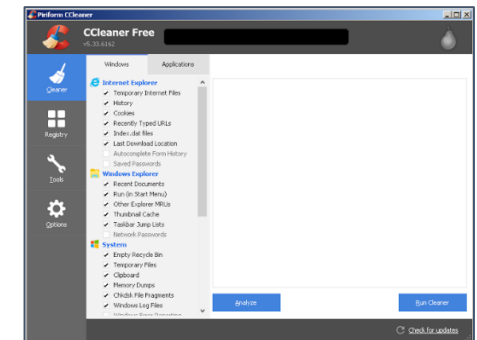
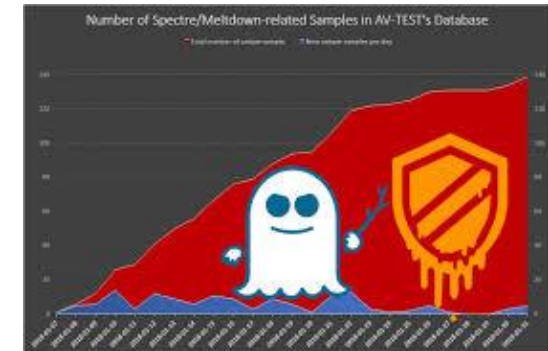


HACKTIVISMO

Ciberataques

Objetivo explotar la confianza en la tecnología

- Los ataques a la cadena de suministro se están convirtiendo en una **tendencia preocupante, forma muy efectiva de distribuir software dañino.**
- Aprovechar la **relación de confianza** entre los **proveedores de software** y los **usuarios**, beneficiándose de la confianza inherente en los archivos y servidores web utilizados para **distribuir actualizaciones.**
- Las extensiones/plugins proporcionan una funcionalidad adicional y, en última instancia, le asignan **responsabilidades al usuario.**
- Vulnerabilidades graves de procesadores Intel, AMD y ARM, que permiten en el peor de los casos **leer memoria reservada privada del kernel** desde código no privilegiado. (conocidas, al menos, desde junio 2017)
- En **tiempos recientes**: CCleaner, NotPetya (software MeDoc), distribución de Zeus mediante CrystalFinance, plataforma Orion de SolarWinds, etc...





Determinación de la Superficie de Exposición



Mejora Continua



Reducción del Tiempo de Respuesta

La adaptación a las nuevas amenazas implica **MEJORAR EL CUMPLIMIENTO** y diseñar una respuesta cada vez más eficaz frente a los ataques **INCREMENTANDO LAS CAPACIDADES DE VIGILANCIA**



Prevención Proactiva: Cumplimiento y Vigilancia

Prevención Proactiva: Cumplimiento y Vigilancia

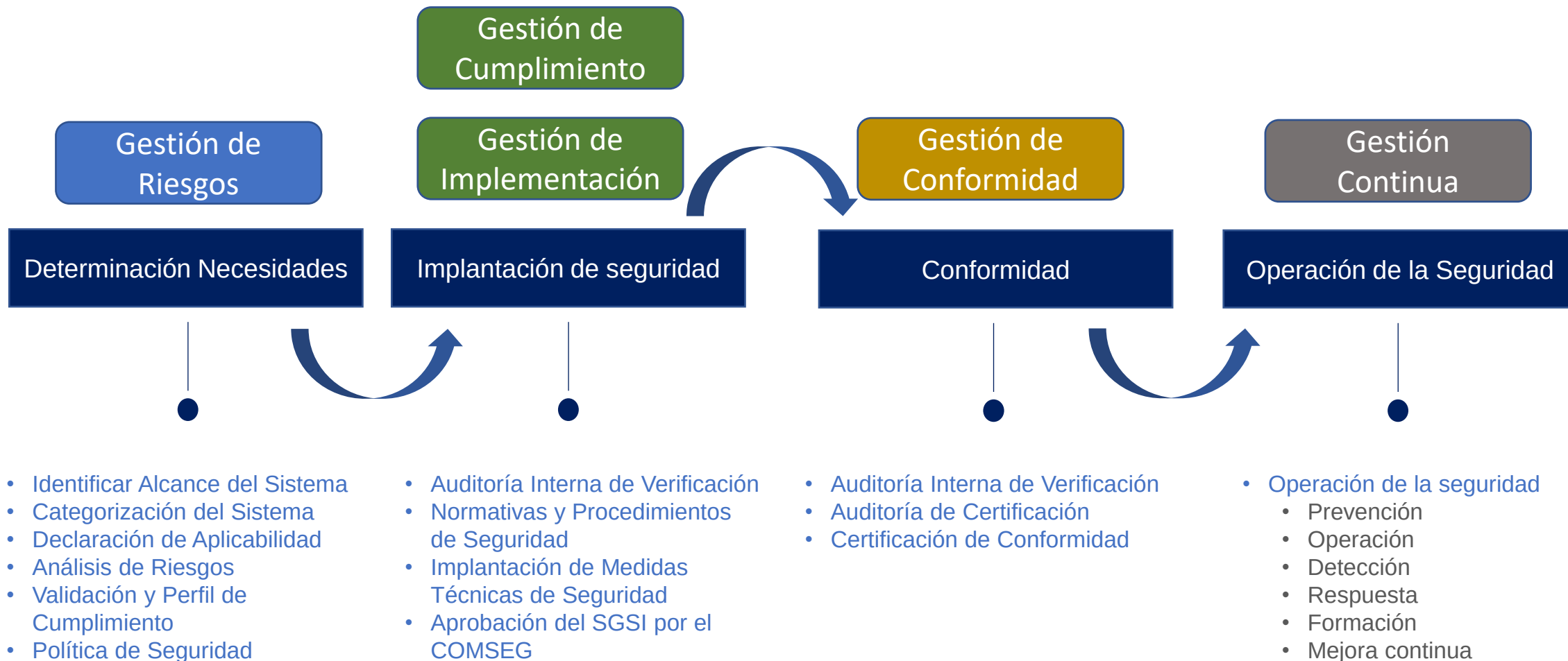
- ❖ **Establecer una hoja de ruta** que permita adelantarse al problema y, lo que es más importante, cómo poder **gestionarlo a priori** ante el menor indicio de materialización...
- ❖ Construir modelos, analizar el problema y elaborar una hipótesis fundamentada de cara a **optimizar los recursos** disponibles y **priorizar la asignación** de los mismos.
- ❖ **Predecir** el potencial ataque y **la materialización de la amenaza...** *podemos anticiparnos porque conocemos y conocemos porque medimos y medimos porque tenemos capacidades de vigilancia.*
- ❖ Al final la **mejora continua** se convierte en el elemento de **apoyo a la decisión**.



Si se conoce el problema (vulnerabilidades, deficiencias y mala praxis), las carencias y potenciales amenazas se pueden **predecir y hacer prospectiva**

Si medimos, gestionamos y si gestionamos, avanzamos...

Gobernanza de la Ciberseguridad



Prevención Proactiva: Cumplimiento y Vigilancia



Servicios de Ciberseguridad

Creación de Centro de Operaciones de Ciberseguridad



Gestiona y coordina los servicios de ciberseguridad

Instalación y operación de herramientas

Se responsabilizará de la instalación y operación de Herramientas Centralizadas de Ciberseguridad

Instalación, configuración, parametrización y personalización de una serie de soluciones, en principio proporcionadas por el Centro Criptológico Nacional (CCN), que den apoyo y soporte al cumplimiento normativo y adecuación al ENS:



Cumplimiento de Esquema Nacional de Seguridad



Control de acceso a las infraestructuras de red



Monitorización de la superficie de exposición



Registro, seguimiento e Intercambio de incidentes de seguridad



Identificación de Amenazas Persistentes Avanzadas (APT)



Correlación compleja de eventos (SIEM) u otra alternativa



Sonda de control de tráfico de red

1	Adecuación al ENS – Diputación u Órgano equivalente	▼
2	Certificación del ENS – Diputación u Órgano equivalente	▼
3	Reconocimiento del Órgano de Auditoría Técnica	▼
4	Infraestructura Tecnológica EE.LL.	▼
5	Selección de las EE.LL. del MCE-ENS	▼
6	Selección muestra representativa (MR)	▼
7	Creación COMSEG	▼
8	Plan de Adecuación Conjunto	▼
9	Adecuación al ENS de la MR	▼
10	Auditoría interna	▼
11	Auditoría de Certificación	▼
12	Expedición de las APC	▼
13	Adecuación definitiva de las EE.LL. adheridas al Marco de Certificación	▼
14	Auditoría(s) de Certificación	▼

Ciclo de mejora continua de la seguridad

Las actividades 13 y 14 comprenden el Ciclo de mejora continua de la seguridad, y abarcan las siguientes tareas por parte de la **Oficina de Seguridad TIC** y el **Órgano de Auditoría Técnica (OAT)**

Oficina de Seguridad-vSOC

- Adecuación definitiva de las Entidades vinculadas o dependientes y nuevas entidades
- Mantenimiento y gestión de la seguridad de las Entidades certificadas

Órgano de Auditoría Técnica (OAT)

- Verificación de seguridad de las entidades cada 2 años
- Gestión de la certificación de conformidad

Adecuación al Cumplimiento - ENS

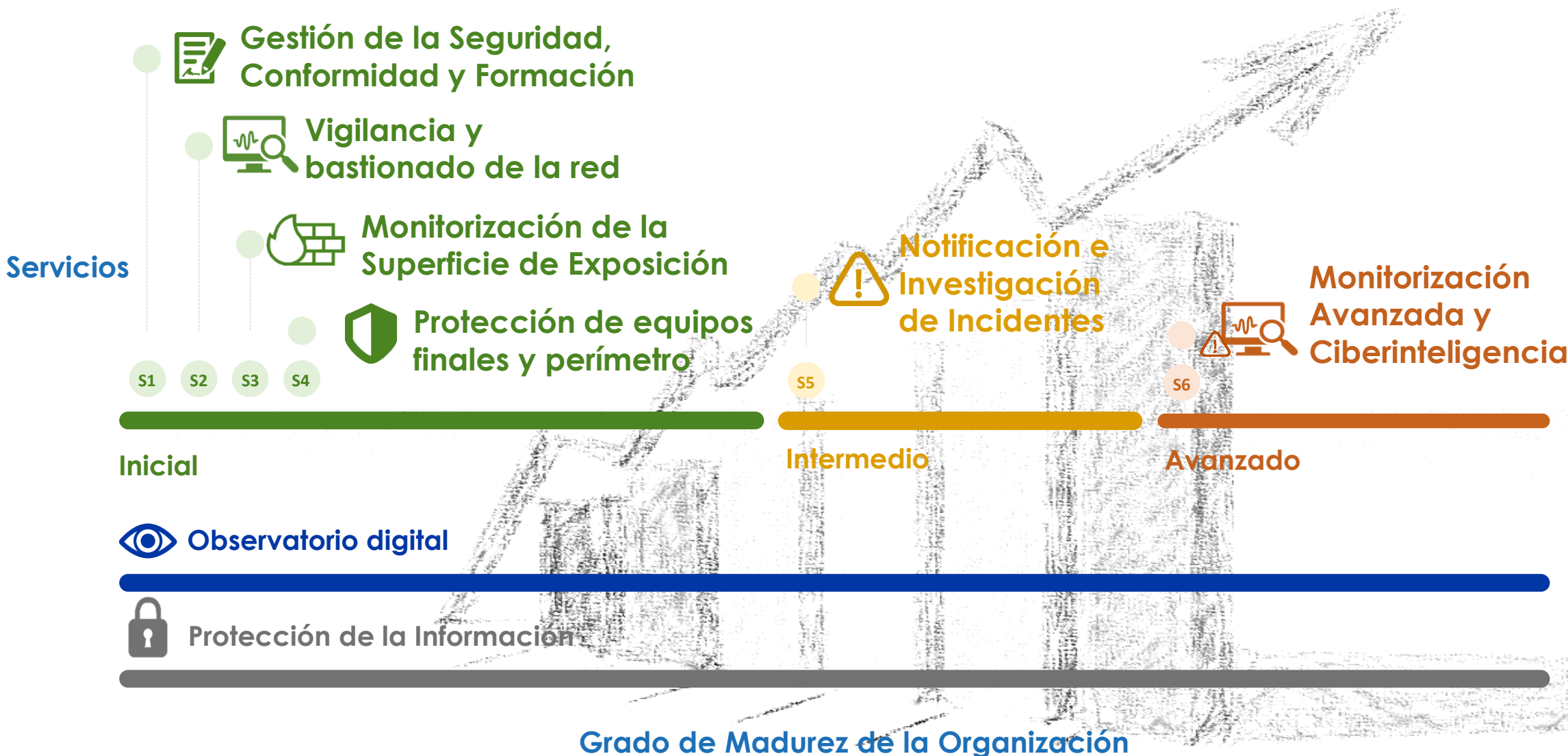


Plan de Adecuación al Sistema

Implantación de Seguridad



Hoja de Ruta – Operación de la Ciberseguridad



Hoja de Ruta – Prevención Proactiva

Servicios



Gestión de la Seguridad, Conformidad y Formación



Vigilancia y bastionado de la red



Monitorización de la Superficie de Exposición



Protección de equipos finales y perímetro

S1

S2

S3

S4

Inicial



ángeles

Formación y Talento en Ciberseguridad

evens
ENTORNO DE VALIDACIÓN ENS



Notificación e Investigación de Incidentes

S5

Intermedio



Monitorización Avanzada y Ciberinteligencia

S6

Avanzado



Observatorio digital



Protección de la Información

Grado de Madurez de la Organización

Inicial - Gestión de la Seguridad, Normativa y Formación

Marco Organizativo

Política de
Seguridad

Normativa de
Seguridad

Procedimientos
De Seguridad

Marco Operacional

Análisis de
Riesgos

Métricas e
Indicadores

Medidas de Protección

Formación

Concienciación



Gestión de la Seguridad SGSI

Conjunto de procesos, políticas, procedimientos, análisis y test, organizados de forma lógica y soportado por objetivos a nivel estratégico, basado en un modelo de evaluación y mejora continua (el ciclo PDCA).

**El ENS requiere de la implantación de un
Sistema de Gestión de Seguridad de la
Información**

Inicial - Gestión de la Seguridad, Normativa y Formación

Marco Organizativo

Política de Seguridad

Normativa de Seguridad

Procedimientos De Seguridad

Marco Operacional

Análisis de Riesgos

Métricas e Indicadores

Medidas de Protección

Formación

Concienciación

❖ Gestión de la Seguridad



Acceso Cloud



Acceso Cloud



Acceso Cloud

INES

AMPARO

PILAR

❖ Formación y Concienciación



Acceso Cloud

ÁNGELES



Acceso Cloud

VANESA

Inicial - Perfiles de personal

Perfil	Funciones
Dirección / Coordinación	• Dirección y Seguimiento • Revisión de la Planificación y Ejecución • Gestión del Equipo de Trabajo • Interlocución con Responsables
Oficina Seguridad TIC	• Análisis previo de situación en materia de ENS • Diseño y elaboración del Plan de Adecuación al ENS • Asesoramiento en materia de adecuación y cumplimiento normativo: elaboración de procedimientos específicos de adecuación (marco normativo) • Formación, capacitación y talento • Cultura ciberseguridad. Concienciación y sensibilización • Seguimiento del plan de adecuación ENS. • Elaboración de acciones correctivas (PAC)
Operación Ciberseguridad	• Ejecución de los Procesos de adecuación de las entidades al ENS • Despliegue de herramientas de Ciberseguridad centralizadas • Monitorización y administración de las herramientas de Ciberseguridad • Análisis y detección de amenazas de seguridad y desarrollo de técnicas de prevención • Mantenimiento y Soporte • Reuniones de seguimiento

Inicial - Gestión de la Seguridad, Normativa y Formación

Mínima

- Comité de Seguridad y DPO
- Plan de Adecuación (Plan Director de Seguridad)

Media

- SGSI (cumplimiento del ENS)
- Participación en órganos directivos
- Asesoramiento externo
- Campañas constantes de concienciación

Avanzada

- Oficina cumplimiento (ENS)
- Gobierno de Seguridad de la Información

**Madurez:
Gestión/Inteligencia**

**Coste Medio Año
(dedicaciones año)**

Mínima

1 hora/usuario

Media

2 horas/usuario

Avanzada

4-12 horas/usuario

Inicial - Vigilancia y bastionado de red

Marco Organizativo

Marco Operacional

Requisitos de acceso

Acceso Remoto

Inventario de activos

Configuración de seguridad

Gestión de la configuración

Detección de intrusión

Medidas de Protección

❖ Vigilancia de red y protección de comunicaciones



Instalación On-Premise

EMMA

❖ Bastionado en Equipos de Comunicaciones

Equipos de Red

Bastionado

Guías STIC

Inicial - Determinación de la Superficie de Exposición

Marco Organizativo

Marco Operacional

Requisitos de acceso

Configuración de seguridad

Inventario de activos

Gestión de la configuración

Mecanismos de autenticación

Medidas de Protección

Protección de Equipos portátiles

Protección de servicios web

❖ Monitorización de la Superficie de Exposición



Instalación On-Premise

CLARA



Instalación On-Premise

ANA

❖ Configuración y bastionado de equipos

Equipos y Servidores

Bastionado



Auditoría de Servicios Web

Ejecución en Remoto



Guías STIC



Inicial - Protección de equipos finales y perímetro

Marco Organizativo

Marco Operacional

Protección
código dañado

Detección de
intrusión

Registro actividad
de usuarios

Medidas de Protección

Protección de
Equipos portátiles

Perímetro
seguro

❖ Protección de Equipos Finales

EDR y Endpoints



CYTOMIC

Instalación On-Premise y Licenciamiento



Productos certificados

CLAUDIA

❖ Protección Perimetral

Firewall



FORTINET

SOPHOS

Check Point
SOFTWARE TECHNOLOGIES LTD

paloalto
networks

Instalación On-Premise y Licenciamiento



Productos certificados



Inicial - Protección de equipos finales y perímetro

Medidas de protección

Inicial

- Seguridad Perimetral (UTM, NGFW)
- Seguridad en el puesto de trabajo (endpoint)

Intermedio

- Capas extra en el perímetro (IPS, WAF,...)
- Capas extra (Cifrado, Navegación, DLP, MDM,...)

Avanzado

- Detección de intrusos (IDS, IPS)
- Gestores de eventos (SIEM, "Machine Learning", BI,...)
- Protección especializada (corporativa, industrial, nube)

**Madurez:
(Armas/Medios)**

**Coste
Medio Año**

Inicial

20-25 €/usuario

Intermedio

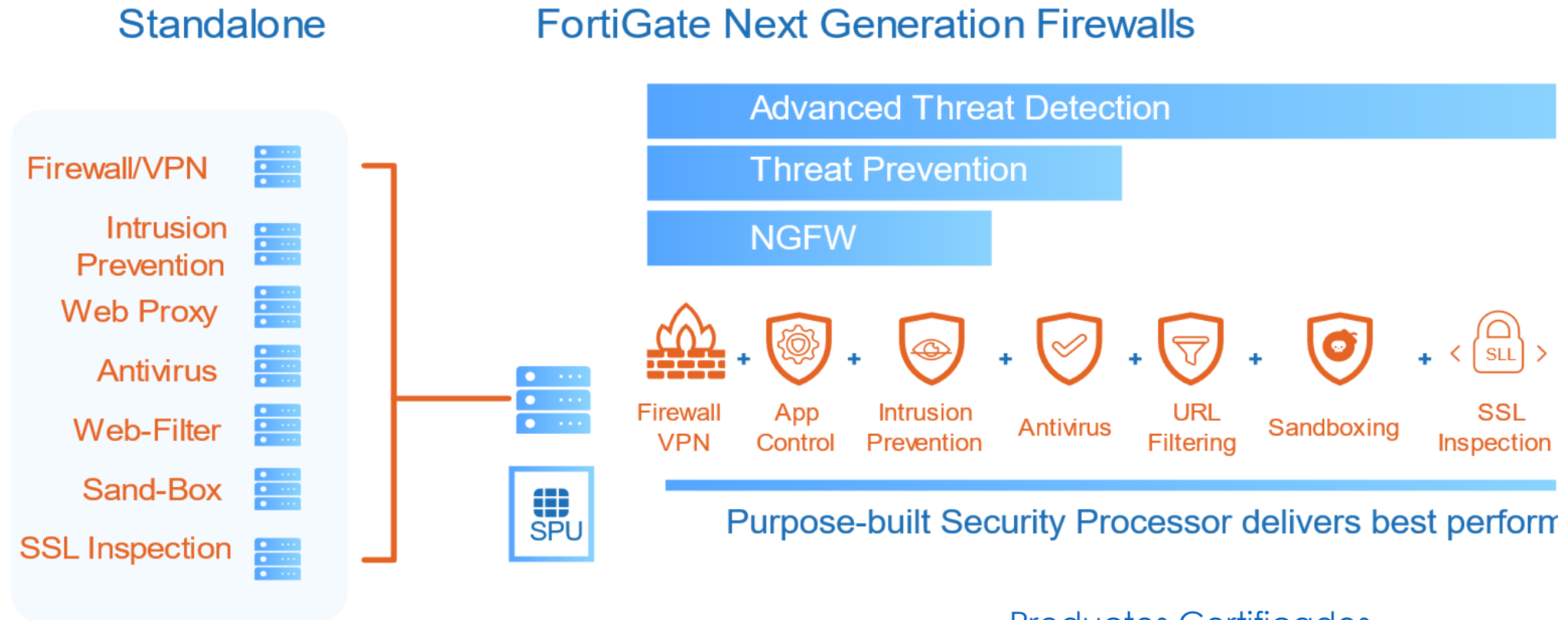
50-60 €/usuario

Avanzada

100-200 €/usuario

Inicial - Protección de equipos finales y perímetro

Capacidades según madurez

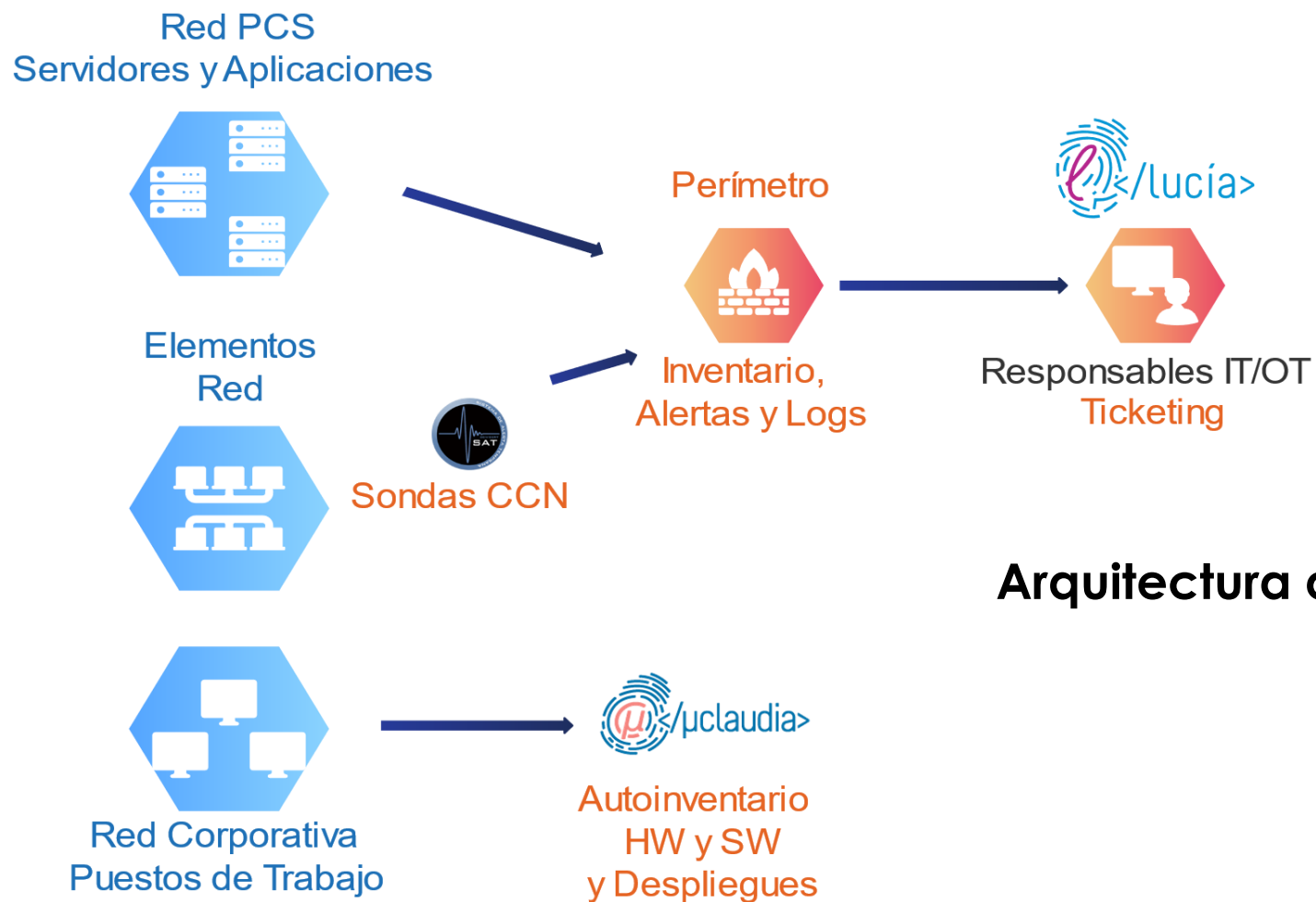


Productos Certificados

Inicial - Protección de equipos finales y perímetro

	Antivirus	Endpoint
Protección firma	✓	✓
Protección móviles (MDM)	✓	✓
Bloqueador web	✓	✓
Seguridad centralizada	X	✓
Cifrado de datos	X	✓
Acceso jerárquico datos	X	✓
Capacidad respuesta (EDR). Rollback	X	✓
Despliegue de parches	X	✓
Prevención de fuga de datos (DLP)	X	✓
Aislamiento automático	X	✓
Protección malware (0-day, Ransomware, Fileless...)	Parcial	✓
Inventario y Control de SW	X	✓
Protección especializada (Cloud, Office365, VMWare, industrial...)	Parcial	✓

Inicial - Protección de equipos finales y perímetro



Arquitectura de Seguridad Inicial



Protección de la Información

Marco Organizativo

Marco Operacional

Requisitos de acceso

Medidas de Protección

Protección de
Confidencialidad

Autenticidad e Integridad

Etiquetado

Calificación de la
información

❖ Protección y monitorización de ficheros



Instalación On-Premise

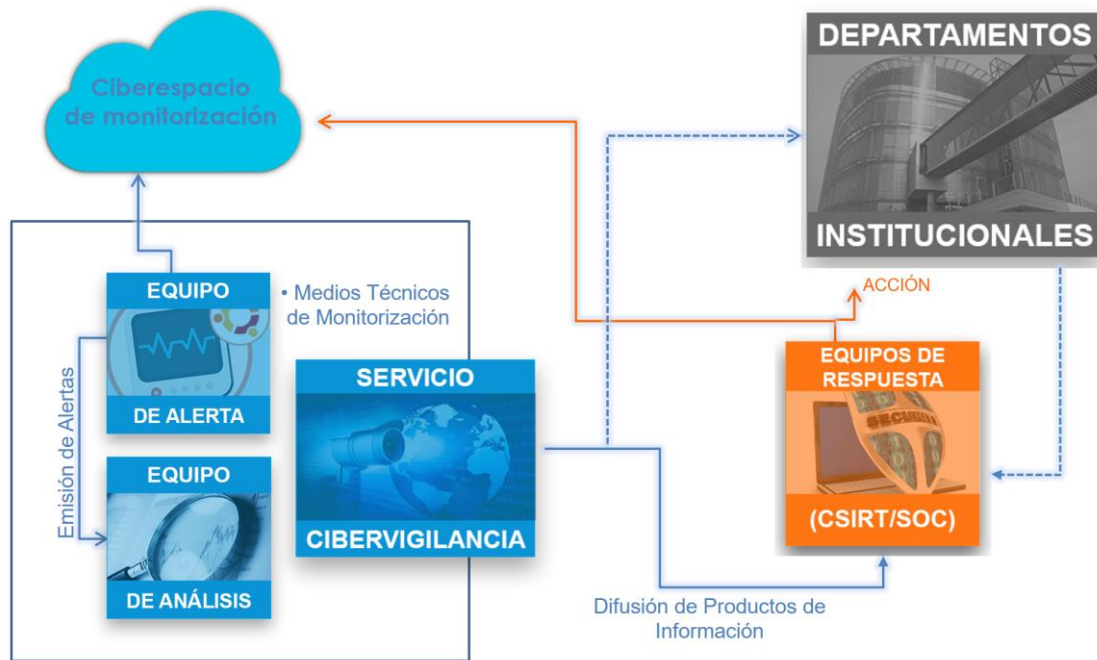


CARLA



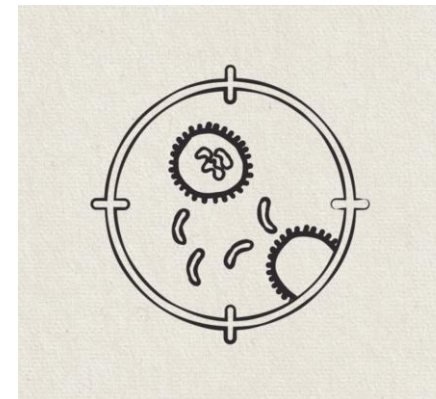
Catálogo de Productos:
Listado de Productos Cualificados

Observatorio digital

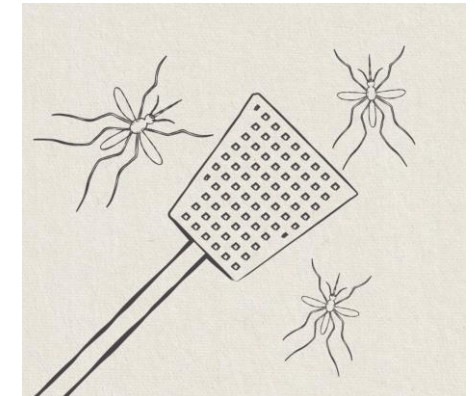


Observatorio Digital
servicio para la identificación de tendencias
maliciosas y prevención temprana en su
primera fase operativa

Prevenible



Fuera de control



Servicios a prestar



Monitorización

Monitorización y operación de las herramientas instaladas.



Coordinación

Coordinación de los servicios de ciberseguridad.

- Servicio Mitigación ataques de Denegación de Servicio.
- Servicios de gestión de Incidentes de Seguridad.
- Servicio de cibervigilancia.
- Servicio de ciberresiliencia.
- Ejercicios de ciberseguridad.
- etc.



Gestión

Gestión de incidencias de Seguridad de forma centralizada.



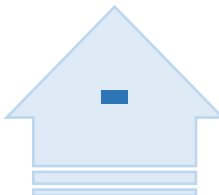
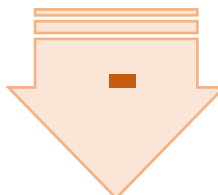
Soporte

Soporte en el día a día en materia de ciberseguridad.

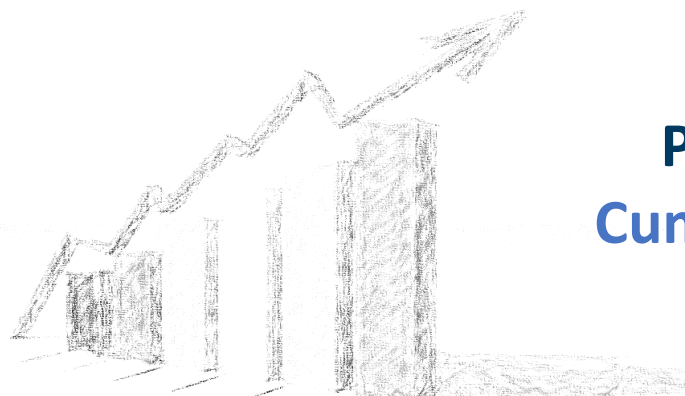
- Apoyo en el soporte al uso de las herramientas.
- Resolución incidencias en operación o uso de herramientas.
- Apoyo en la gestión de incidentes de seguridad.
- Monitorización de los sistemas para detectar actividades inusuales o accesos a información no autorizados.
- Analizar las medidas de seguridad implementada.
- Protección de la información.
- Adopción de medidas de control y supervisión.
- Ejecución de diagnósticos ante cambios en las infraestructuras.

Mejora Continua

(Hoja de Ruta)

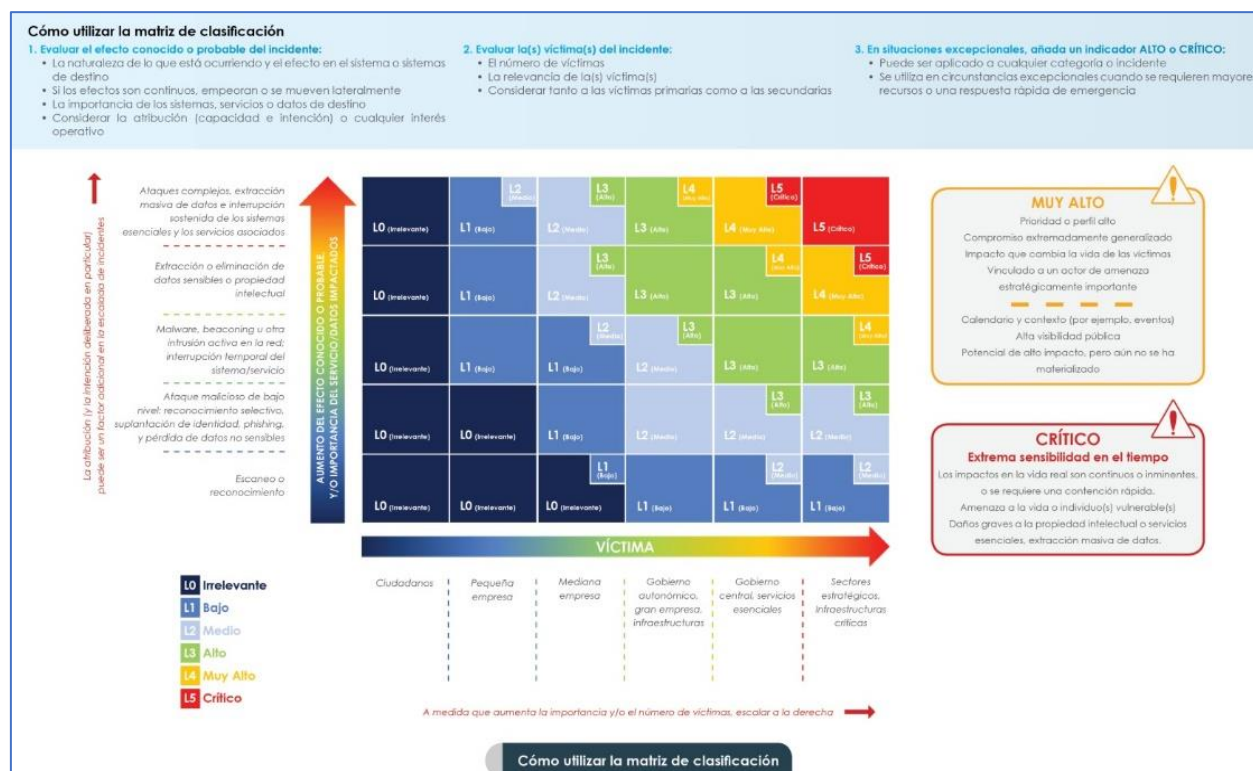
	Madurez	Coste Preventivo	Coste Reactivo	Coste Cumplimiento	Total	
	Inicial	20-25 €/usuario	2 horas/usuario	1 hora/usuario	20-25 €/usuario 3 horas/usuario	
Madurez	Intermedio	50-60 €/usuario	6 horas/usuario	2 horas/usuario	50-60 €/usuario 8 horas/usuario	Riesgo
	Avanzado	100-200 €/usuario	12-20 horas/usuario	4-12 horas/usuario	100-200 €/usuario 4-12 horas/usuario	

Prevención Proactiva
Cumplimiento y Vigilancia



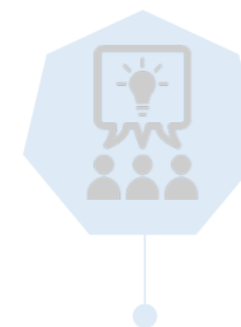
Prevención Proactiva

El reto está en conseguir que el cumplimiento y la vigilancia vayan de la mano adaptadas al nivel de madurez y recursos disponibles de las entidades



Ventajas

- Gestionar servicios de ciberseguridad
- Medición superficie de exposición
- Adaptación a la amenaza
- Mejora en la notificación de incidentes
- Eficiencia de los recursos disponibles



Más información de ataques



Mayor visibilidad sobre incidentes

JORNADA STIC

CAPÍTULO COLOMBIA

GRACIAS



En colaboración con:

