An Indra company

Tendencias de ciberseguridad 2024:
Administraciones Públicas

SOCINFO sociedad de la información digital

Toda la información contenida en el presente documento y sus anexos, tiene carácter confidencial, y sólo puede ser utilizada con el fin de ser evaluada por el destinatario (sea cliente, proveedor, colaborador, partner, etc.) de la misma y a los solos efectos de conducir los tratos comerciales, o de otra naturaleza, que motivan el envío del documento (en lo sucesivo, el “Propósito”).

La información aquí presentada es elaborada por SISTEMAS INFORMATICOS ABIERTOS, S.A.U., (en adelante SIA) sociedad perteneciente al Grupo Indra, con C.I.F. A82733262 y domicilio en Av. de Bruselas, 35, 28108 Alcobendas (Madrid), España y anula y sustituye a las anteriores, y es constitutiva de secreto empresarial (también denominado en determinadas jurisdicciones, secreto comercial), y además, puede estar protegida por derechos de autor, derechos afines, patente, modelo de utilidad y/o diseño industrial por lo que queda terminantemente prohibida su divulgación y/o transmisión a terceros sin el permiso previo, expreso y por escrito de SIA.

Se limitará al máximo el acceso a la información confidencial por parte del personal del destinatario de la misma, o del personal de aquellos terceros a los que SIA haya autorizado a acceder a la información confidencial, limitándose únicamente a aquellas personas cuyo acceso resulte estrictamente necesario, y debiendo el destinatario de la información confidencial garantizar que informa a dichas personas del carácter confidencial y propietario de la información así como del Propósito, asegurando que dicho personal trata la información confidencial única y exclusivamente para el Propósito, y absteniéndose de toda divulgación. Una vez finalizado o concluido el Propósito, el cliente debe restituir a SIA toda la información confidencial sin conservar ninguna copia de la misma, no pudiendo utilizar de ninguna manera, ni para ningún fin la información confidencial y/o propietaria facilitada por SIA salvo que haya sido autorizado para ello previa y expresamente por escrito por SIA.

El destinatario de la información confidencial, después de finalizado el Propósito, no podrá utilizar de ninguna manera ni para ningún fin la información confidencial y/o propietaria facilitada por SIA.

Índice

1. Contexto y desafíos

- Incremento del número de ciberataques, que son cada vez más sofisticados
- Aumento de la superficie a proteger
- Medidas de acceso y de identificación, mejorables
- Mecanismos de contratación muy lentos
- Tecnologías anticuadas y/o heterogéneas
- Presupuestos y recursos insuficientes
- Escasez de talento cualificado
- Nivel de formación y concienciación insuficiente
- Falta de un método de recuperación ante desastres

Un enfoque orientado sólo a detección y respuesta no es suficiente. Este se debe orquestar con un conjunto de prácticas y servicios adicionales para contar con una visión integrada y conseguir un nivel de protección óptimo

#1
AAPP es el sector con mayor nº de incidentes

#2
AAPP es el sector con mayor nº de brechas de seguridad

Fuente: Verizon DBIR 2023

El Confidencial

Por **Manuel Ángel Méndez**
29/01/2024 - 15:57

El ministro de **Transformación Digital** y Función Pública, José Luis Escrivá, ha anunciado hoy en el Congreso las que serán las líneas clave de su cartera durante la presente legislatura. No hay grandes sorpresas, pero sí dos apuestas relevantes: el anuncio de **una nueva ley de ciberseguridad y la intención de impulsar la apertura de nuevas fábricas de *chips* en nuestro país**. Según fuentes del ministerio, ya hay conversaciones en marcha con diversas multinacionales estadounidenses para negociar el establecimiento de nuevas plantas, aunque, de momento, no ha trascendido ningún nombre.

La propuesta de una nueva ley de ciberseguridad llega en el momento de mayor actividad de ciberataques en nuestro país, no solo contra grandes empresas, también contra la Administración del Estado. El Jefe del departamento de Ciberseguridad del Centro Criptológico Nacional (CCN), dependiente del CNI, reconoció recientemente que el 2023 había sido, con diferencia, **el año en el que se habían detectado mayor número de ataques críticos en España**, más de 120, frente a 75 en el 2022, un 60% de aumento.

El Ejecutivo quiere ahora plantear una ley con un "enfoque integral" que logre **aumentar los recursos y defensas del sector público y privado frente a los ciberataques**. Hasta ahora, el Gobierno había aprobado la **Ley de Ciberseguridad 5G** (agosto 2022), centrada en el marco de las telecomunicaciones, pero faltaba ampliar esa regulación a todos los ámbitos. Fuentes del ministerio de Transformación Digital aseguran que la nueva ley contará con más de 1.500 millones de euros procedentes del plan de recuperación en ciberseguridad. El Instituto Nacional de Ciberseguridad (Incibe), ofertará además más de 10.000 plazas de formación especializada en esta materia entre 2024 y 2026.

2. Panorama de amenazas

Las amenazas de 2023 continuarán en 2024, potenciadas con IA y computación cuántica, al tiempo que el riesgo se traslada hacia nuevos vectores de ataque (móviles, cloud, IoT y redes 5G)

Principales amenazas 2023

Nuevos grupos APT
que priorizan sectores estratégicos y colaboran entre sí

Inteligencia Artificial
para ataques más precisos y difíciles de detectar

Hacktivismo
en el que prevalecen los ataques DDOS con tintes políticos y la Botnet Mirai

Campañas contra entornos cloud
que requieren una atención constante

Tácticas más avanzadas
Ransomware más avanzado. Aumento significativo de AgenTesla, Formbook, Snake Keylogger, así como el uso de archivos Onenote para los ataques

Vulnerabilidades 0-day
Principalmente, por grupos APT esponsorizados por estados, siendo especialmente críticos en productos Microsoft

Ransomware y fugas de información
Aumento de LockBit2 y LockBit3 y, en menor medida, ALPHV, Hive, Conti y Vice Society

Principales amenazas 2024

- Más ciberataques y **phishing potenciados con IA generativa**
- Aumento de Deep Fakes y de **ataques a la cadena de suministro**
- Incremento de los incidentes y brechas de seguridad en **entornos cloud**, **sistemas de control industrial**, dispositivos **IoT y redes 5G**, con una motivación política o social mayor que en años anteriores
- Tácticas y técnicas cada vez más complejas; **mayor uso de la IA y la computación cuántica para potenciar los ataques**, y **el móvil será un objetivo en ascenso**

3. Cumplimiento normativo

Existen modificaciones de normas y regulaciones que requieren un análisis GAP de qué se cumple ahora y qué es necesario adaptar (ENS, PCI, ISO). Además, se espera una avalancha legislativa en temas como la Inteligencia Artificial y NIS2.

Normas y regulaciones

Inteligencia Artificial

Borrador de Ley de IA - EU (2024)
2 años desde que se apruebe
Falta Ley de IA que recoja el régimen sancionador
No hace falta transponer

ENS 2.0

- Entró en vigor en mayo 2022. 24 meses (**mayo 2024**) para que los sistemas de información alcancen su plena adecuación al ENS
- Se introduce el principio de **Vigilancia Continua**.
- Añade medidas orientadas a servicios en nube, interconexión de sistemas y protección de la **cadena de suministro**

ISO 27001:2022

- Cambio de la norma en 2022
- Si hay que renovar, tiene sentido que se renueve con la norma actual

NIS2

- Foco en ciber resiliencia
- Foco en AARR
- Foco en la cadena de suministro
- ¿Cómo la aplicamos? Deadline transposición OCT 2024

PCI 4.0

A partir del 01/ABR/2024 cualquier certificación debe ser con v4.0

4. Modelos organizativos - La unión hace la fuerza

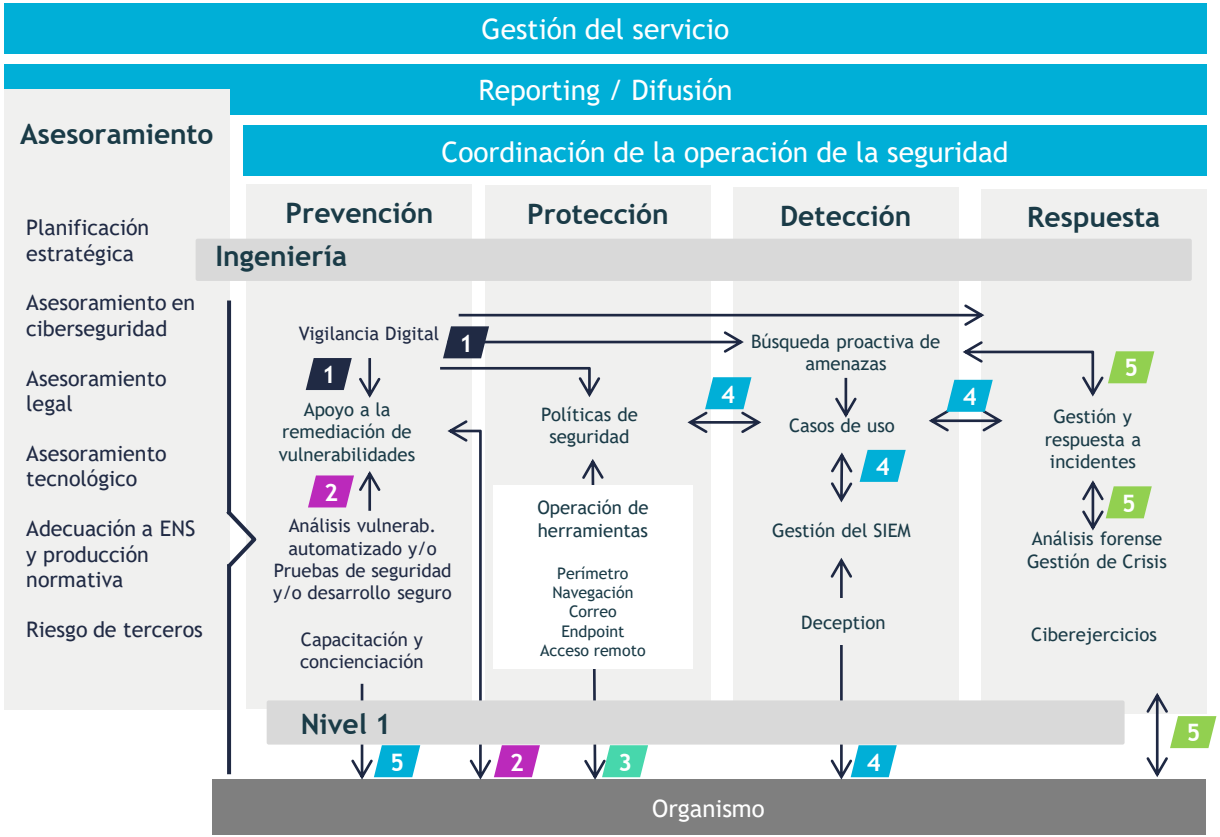
Diferentes iniciativas en marcha.
Es crítico que compartamos información y trabajemos juntos.

Es posible la complementariedad entre los servicios que presta cada organismo.

Entre todos, ayudemos a protegernos.

4. Modelos organizativos - Trabajo colaborativo entre capacidades cyber

La ciberseguridad no es un producto. Debemos evolucionar los modelos tradicionales a un modelo multicapa. Es importante que las diferentes capacidades de ciberseguridad trabajen colaborativamente entre sí, para maximizar la prevención, protección, detección y respuesta.



Algunos elementos de relación entre capacidades son:

1
- Análisis de amenazas identificadas en Internet, globales o dirigidas al organismo
- Identificación y gestión de IOCs
- Información de inteligencia de seguridad

2
- Informes de vulnerabilidades identificadas en los sistemas y aplicaciones
- Priorización de resolución de vulnerabilidades
- Controles técnicos a implementar o modificar para mejorar la postura de ciberseguridad

3
- Implementación de IOAs personalizados

4
- Identificación de eventos a generar en los sistemas y aplicaciones para la detección de amenazas e incidentes
- Gestión de integraciones con el SIEM
- Implementación y mejora de casos de uso
- Atención de alertas, triaje y enriquecimiento

5
- Investigación de amenazas que deben gestionarse
- Gestión de incidentes o amenazas detectadas
- Propuesta de nuevos casos de uso para la detección
- Identificación de políticas de seguridad a aplicar para la protección de los sistemas
- Capacitación y concienciación

5. Evolución tecnológica - Detección y respuesta

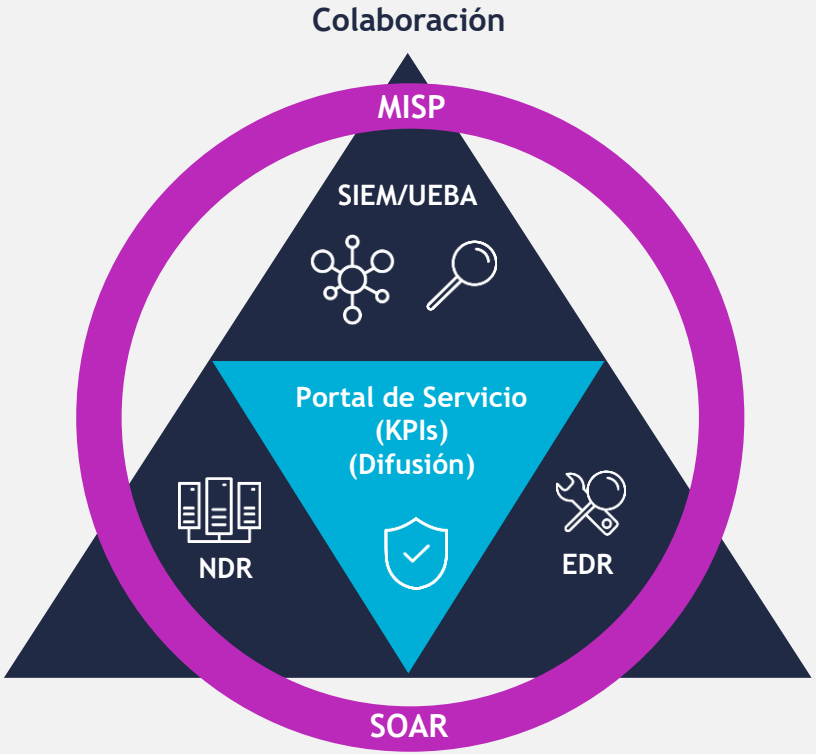
La IA tendrá un papel clave en la ciberseguridad durante los próximos años, según las tendencias pronosticadas por analistas internacionales.

Piezas tecnológicas esenciales para maximizar la protección, detección y respuesta a incidentes

- **SIEM/UEBA**: recopilar, analizar y correlacionar la información y actividad de sistemas y usuarios en los componentes del entorno tecnológico para detectar posibles amenazas.
- **EDR**: obtener la información de ejecución de archivos, conexiones de red, actividades en memoria y otros cambios en el sistema, actividades y modificaciones a nivel de puesto de trabajo y host.
- **TIP / MISP**: centralizar datos de amenazas de numerosas fuentes y formatos. Compartir IOCs.
- **SOAR**: orquestar y automatizar acciones de respuesta con el objetivo de obtener más eficacia y eficiencia en la detección y respuesta frente a incidentes.
- **Portal del Servicio**: medición de indicadores y difusión de información.
- **NDR:** Permite identificar actividades en red sospechosas tanto en cloud como en datacenter, observando los patrones de flujo, tanto de amenazas externas como internas.

Beneficios de uso de un NDR

- No es evadible, **analiza todo el tráfico** de red
- **Detectan amenazas que han evadido el resto de sistemas**, al utilizar el aprendizaje automático para **crear modelos predictivos** de comportamiento en lugar de basarse simplemente en firmas como referencia para la detección
- Pueden encontrar **amenazas de seguridad nunca vistas** y detectar tácticas, técnicas y procedimientos de baja intensidad que los sistemas basados en firmas suelen pasar por alto



Basado en Gartner's SOC Visibility Triad

5. Evolución ¿tecnológica? - Gartner Continuous Threat Exposure Management (CTEM)

La gestión de vulnerabilidades ya no es sostenible; es crucial plantear un paradigma continuo, para tomar acciones periódicas para detectar y prevenir posibles amenazas y vulnerabilidades de manera consistente. Esto, que puede afectar a la postura de seguridad de una organización, busca reducir mejor la brecha entre la marea interminable de CVEs, configuraciones erróneas, problemas basados en identidad… y abordarlas de la manera más eficiente para reducir el riesgo de ciberataque.

CTEM no es una herramienta, es un programa…

El programa de Gestión Continua de la Exposición a Amenazas (CTEM) es un conjunto de procesos y capacidades que permiten a las empresas evaluar de forma continua y consistente la accesibilidad, exposición y explotabilidad de los activos físicos y digitales de una empresa.

… que tiene estos beneficios:

1. **Ayuda a priorizar amenazas** para su resolución de acuerdo al impacto potencial para el negocio
2. **Aporta información útil** al identificar rutas de ataque que pueden explotarse, a partir de inteligencia de amenazas, en tiempo real
3. **Gestión proactiva del riesgo** con un enfoque holístico (CVEs, configuraciones erroneas, identidades expuestas, problemas del directorio…)
4. **Aumenta la ciberresilencia** por la adaptación continua de las defensas, para proteger los activos críticos (no los callejones sin salida)
5. **Mejora la adaptabilidad** a un panorama digital que cambia rápidamente
6. **Alinea Seguridad con Negocio** al alinear la ciberseguridad con los objetivos estratégicos

6. Conclusiones

- Las AAPP pueden mejorar sus capacidades de prevención, protección, detección y respuesta a incidentes si trabajamos juntos y colaboramos entre nosotros
- Es necesario ampliar capacidades de ciberseguridad y que éstas trabajen colaborativamente
- En muchos casos, es necesario complementar las herramientas existentes para tener una visibilidad completa, ser ágiles en la detección y respuesta, y eficientes en la gestión de vulnerabilidades

An Indra company

Muchas gracias

Roberto Pérez García
Head of Cybersecurity Services & Solutions Business
rperezgar@sia.es
+34 696 982 947

BEYOND CYBERSECURITY