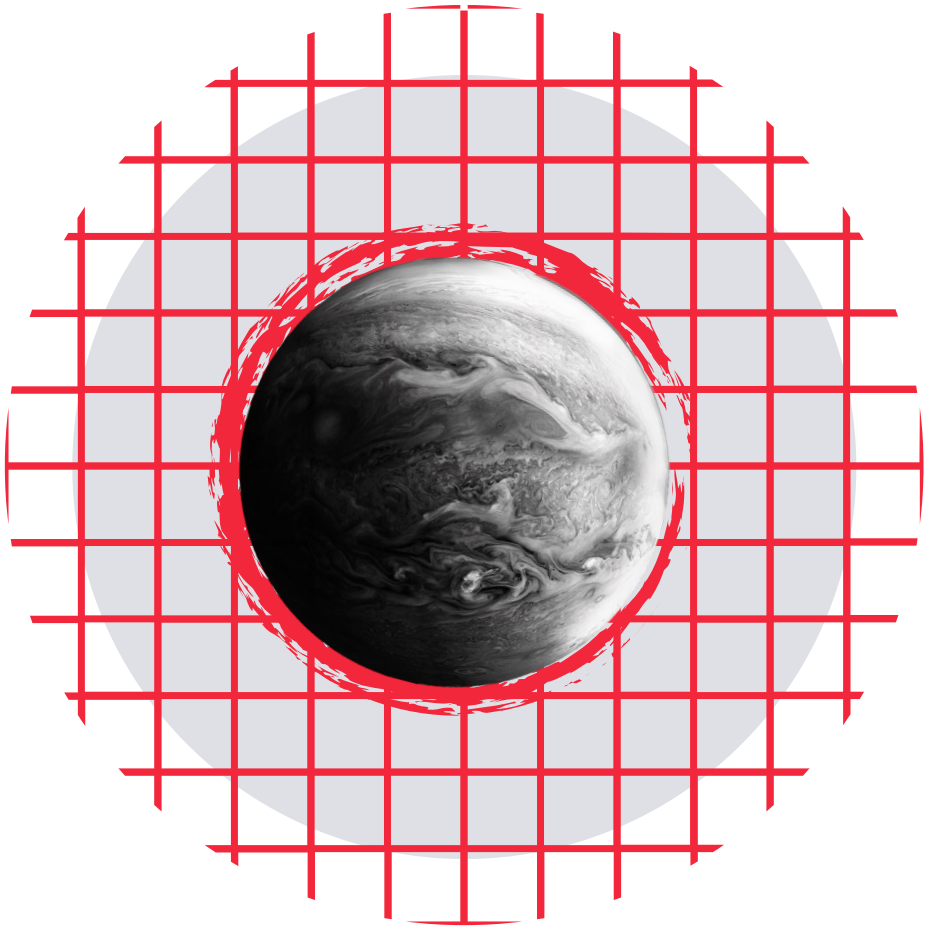
ENTHEC

WHITEPAPER

CIBERSEGURIDAD EXTENDIDA:

Cuando la estrategia construye el concepto



ÍNDICE

INTRODUCCIÓN

El CISO, Chief Information Security Officer, es el responsable de liderar la estrategia de seguridad de la información en una organización, asegurando la protección de sus activos críticos y la mitigación de los riesgos relacionados con la ciberseguridad.

En teoría, este liderazgo no implica que la ciberseguridad corporativa sea solo responsabilidad suya. Sin embargo, en la práctica, el CISO se enfrenta a una serie de desafíos que dificultan su capacidad para proteger con eficacia a la organización y que tienen que ver con factores complementarios a su actividad, como son el alcance de la estrategia, la nula implicación del resto de la organización y los recursos corporativos destinados al diseño de una estrategia efectiva de ciberseguridad. Desafíos que son consecuencia de un concepto equivocado de la Ciberseguridad corporativa que provoca que se perciba dentro de la organización como una actividad restringida al sistema interno, que es responsabilidad exclusiva del CISO y que supone un gasto para la organización desligado de su actividad principal, en lugar de considerarse una inversión, a pesar de ser crucial para la sostenibilidad del negocio a corto, medio y largo plazo.

En este documento vamos a analizar las consecuencias de ese concepto erróneo y cómo cambiarlo utilizando para ello la propia estrategia de ciberseguridad corporativa basada en soluciones de ciberseguridad innovadoras.

FACTORES QUE CONDICIONAN LA CIBERSEGURIDAD CORPORATIVA

Un concepto correcto de lo que es, lo que significa y lo que implica la ciberseguridad corporativa es imprescindible no solo para diseñar una estrategia eficaz, sino para que el CISO pueda ejercer de forma efectiva su liderazgo dentro de la organización.

Con frecuencia, las organizaciones perciben la ciberseguridad como la actividad de blindar el sistema interno, una responsabilidad que solo es competencia y responsabilidad del CISO y un gasto susceptible de estar en constante revisión porque no está adscrito a la actividad principal del negocio y porque hasta que se sufre un ataque exitoso, las potenciales amenazas se confunden con alarmismo.

Alcance, implicación y recursos son factores cuya percepción ha de ser adecuada para diseñar con precisión la estrategia de ciberseguridad que necesita la organización:

ALCANCE

Amplitud de visión de campo

La ciberseguridad no solo afecta al perímetro interno de una organización, sino que se extiende al perímetro externo, incluyendo en él a la web, deep web y dark web, en donde quedan expuestas las vulnerabilidades corporativas para ser utilizadas por los ciberdelincuentes, y los terceros de la organización, cuyas vulnerabilidades suponen un riesgo de control complicado.

IMPLICACIÓN

Ser el que lidera no significa ser el único responsable

El CISO tiene la responsabilidad de liderar, diseñar, implantar y dirigir la estrategia de ciberseguridad corporativa, pero la responsabilidad de adoptarla y seguirla es responsabilidad de todos y cada uno de los miembros de la organización, empezando por el resto de los CXO con áreas que pueden verse afectadas por los riesgos.

RECURSOS

Protegerse con inteligencia es una inversión

Dedicar a la ciberseguridad los recursos necesarios es invertir en la viabilidad del negocio, pero es esencial que esta inversión no se convierta en un lastre para su crecimiento. Por eso, tanto la estrategia de ciberseguridad como las soluciones para ejecutarla han de ser inteligentes e innovadoras para proteger con la mayor eficacia sin comprometer los recursos corporativos, profesionales y económicos.

FACTOR ALCANCE

Uno de los principales desafíos que enfrentan los CISOs es el alcance de su estrategia de seguridad.

En el pasado, los CISOs se centraban principalmente en proteger el perímetro interno de la organización, es decir, la red y los sistemas informáticos, y este es el concepto de ciberseguridad que ha quedado fijado en gran parte de las organizaciones.

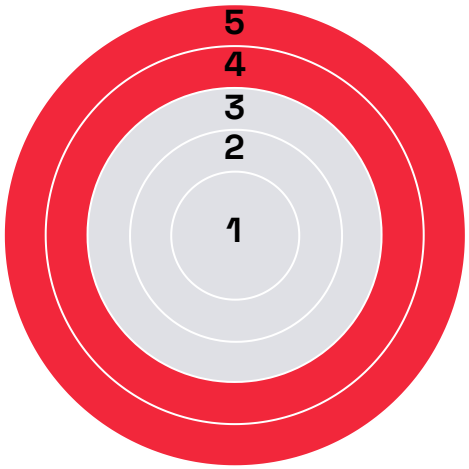
Sin embargo, con la proliferación de dispositivos móviles, la adopción de la nube, la necesaria colaboración con terceros y la existencia de un mercado donde los ciberdelincuentes filtran y exponen la información de las organizaciones, los límites del perímetro de seguridad corporativo se han ampliado y vuelto más difusos. Las organizaciones deben ahora considerar los riesgos asociados con la gestión de terceros y proveedores, los riesgos asociados con los empleados que utilizan dispositivos personales y aplicaciones de la nube para realizar sus tareas y las vulnerabilidades que representan las brechas de seguridad y la información corporativa filtrada y expuesta.

Superficie de ataque

1. Perímetro interno corporativo
2. Dispositivos en remoto
3. Cloud
4. Terceros
5. Web, Deep Web y Dark Web

Interna de la organización

Externa a la organización



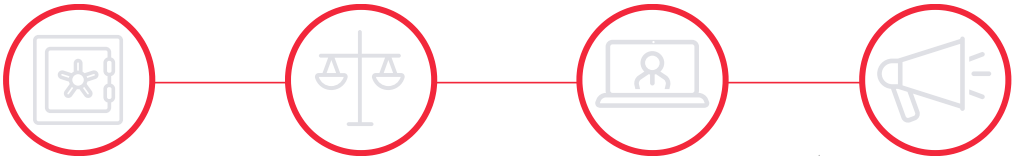
La gestión de la superficie externa de ataque (EASM) proporciona un valioso contexto de riesgo e información procesable a través del análisis continuo, para evaluar y priorizar los riesgos y vulnerabilidades localizados. La gestión de la superficie externa de ataque es una prioridad para los equipos de seguridad y los administradores de riesgos de seguridad.

Gartner, Peer Insights

FACTOR IMPLICACIÓN

Otro desafío que enfrentan los CISOs es la falta de implicación del resto de la organización en la estrategia de seguridad de la información. A menudo, la seguridad de la información se considera responsabilidad exclusiva del departamento de TI o del CISO.

Sin embargo, la seguridad de la información también es responsabilidad directa del resto de miembros de la dirección en particular. Los CISOs deben conseguir que el resto de integrantes del board participen, asuman y se hagan responsables del desarrollo de la estrategia de ciberseguridad y de fomentar una cultura de ciberseguridad en los profesionales a su cargo, además de incluirla en la toma de decisiones y el establecimiento de objetivos.



Seguridad de la información: Estrategia de ciberseguridad corporativa y protección de la información de la organización.

Legal: Cumplimiento legal y efectiva protección de los datos de terceros y de la propiedad intelectual o industrial de la organización.

IT: Correcto funcionamiento, actualizaciones y renovaciones de la infraestructura tecnológica de la organizazión.

Marketing y Comunicación: Reputación de la marca y relación con los clientes.

Operaciones: Continuidad del funcionamiento operativo de la organización.

Financiero: Valoración del riesgo de terceros y sus terceros y relación con ellos.

CEO: Responsable último del negocio.

La percepción de los CISOs españoles de falta de alineación con los consejos de administración ha aumentado, ya que sólo el 17% de los CISOs españoles declara estar muy de acuerdo con la afirmación de que su junta directiva coincide con ellos en cuestiones de ciberseguridad.

Informe Voice of the CISO 2022

FACTOR RECURSOS

Los recursos disponibles para la estrategia de seguridad de la información son limitados y constituyen una partida ajena a la oferta del negocio. Frente a esto, las soluciones de ciberseguridad tradicionales son costosas en términos de implementación y, tan importante, de mantenimiento y actualización. Esto provoca una tendencia a limitar los recursos dedicados a ciberseguridad y a que el CISO tenga que luchar en cada momento por cada partida dedicada a la estrategia de ciberseguridad. La consecuencia se traduce demasiadas veces en una protección llevada mínimos y por tanto, ineficaz ante las grandes amenazas.

Por eso, dentro de las obligaciones actuales del CISO está la de diseñar las estrategias y encontrar las soluciones de ciberseguridad más efectivas y que menos comprometan los recursos corporativos, tanto humanos como materiales. Una parte de este objetivo suele cubrirse optando por trasladar a un tercero la gestión de la seguridad corporativa, a través de un Servicio de Seguridad Gestionada. Pero ya se opte por una ciberseguridad *inhouse* o gestionada por un tercero, la clave está en la utilización de soluciones que sirvan para anular las amenazas antes de que se materialicen y cuya implantación, mantenimiento y actualizaciones no supongan un gasto inasumible a corto y medio plazo gracias a la introducción de nuevas tecnologías, como la automatización o la IA.

En 2026, más del 60% de las capacidades de detección de amenazas y respuesta a incidentes aprovecharán los datos de gestión de exposición para validar y priorizar los riesgos detectados, frente al 5% actual. A medida que las superficies de ataque de la organización se expanden por la mayor conectividad, el uso de software como servicio (SaaS) y las aplicaciones en la nube, las empresas requieren una amplia gama de visibilidad y una ubicación central para monitorear constantemente las amenazas y la exposición.

Gartner, Cumbre sobre Seguridad y Gestión de Riesgos 2023

CIBERSEGURIDAD EXTENDIDA: LA ESTRATEGIA XTI

La cibervigilancia XTI es una estrategia de ciberseguridad basada en la **monitorización y el análisis de la Web, la Deep Web y la Dark Web de forma continuada para detectar en tiempo real la información filtrada y expuesta de las organizaciones y las brechas de seguridad que han propiciado dicha filtración.** De esta forma, una organización puede conocer en tiempo real qué información corporativa está al alcance de cualquier ciberdelincuente para así controlar y neutralizar su capacidad de ataque.

Alcance

- La Cibervigilancia XTI permite a la organización y al CISO alcanzar el perímetro externo corporativo y conocer y controlar las vulnerabilidades de seguridad más allá del perímetro interno y el nivel de Ciberseguridad de terceros relacionados con la organización.

Implicación

- La monitorización continua en tiempo real permite la emisión alarmas por vulnerabilidades y asignarlas a los diferentes directivos y profesionales de los departamentos potencialmente afectados por dicha amenaza. De esta forma, pasan a tener información del riesgo a la vez que el CISO.

Recursos

- Conocer de forma continua y en tiempo real las vulnerabilidades corporativas que están al alcance de cualquiera reduce de forma considerable los costes en recursos de protección, minimización y remediación.

Una estrategia de enfoque outside-inside de Cibervigilancia XTI para riesgos propios y de terceros, a través de soluciones con capacidades para emitir alertas personalizadas por vulnerabilidades a diferentes miembros de la organización e informes adaptados a diferentes niveles de conocimiento en ciberseguridad, permite al CISO implantar el concepto de Ciberseguridad extendida en la organización a través de la estrategia.

VENTAJAS DE LA ESTRATEGIA XTI PARA EL CISO

1. **Protección proactiva contra amenazas externas e internas:** La cibervigilancia XTI proporciona al CISO una visión más amplia de los ciber riesgos que amenazan a la organización, dentro y fuera del perímetro corporativo.

2. **Identificación y gestión de riesgos digitales:** La capacidad DRPS permite a los CISO identificar los riesgos digitales asociados con la marca, la reputación, la propiedad intelectual y otros activos digitales importantes de la organización.

3. **Mejora de la ciber resiliencia corporativa:** La cibervigilancia XTI con capacidades de EASM, DRPS y SRS permite al CISO detectar, responder y minimizar cualquier amenaza, lo que mejora la ciber resiliencia corporativa a corto, medio y largo plazo

4. **Cumplimiento normativo:** La Cibervigilancia XTI y las capacidades de EASM, DRPS y SRS ayudan a la organización a cumplir con las normativas y regulaciones de seguridad de la información.

5. **Toma de decisiones basada en datos:** La capacidad SRS permite al CISO obtener una visión clara de la posición de seguridad de la organización, así como de terceros relacionados con ella, incluidos proveedores, partners y competidores.

CIBERVIGILANCIA XTI: LA CIBERSERGURIDAD EXTENDIDA

- Cibervigilancia que alcanza más allá del perímetro corporativo, incluyendo a terceros con capacidad para suponer un riesgo para la ciberseguridad corporativa.
- Cibervigilancia que emite alertas sobre vulnerabilidades configurables y personalizables para que lleguen, además de al CISO, a los directivos y departamentos afectados que deben tomar medidas para corregirlas o neutralizar sus efectos.
- Cibervigilancia que optimiza y racionaliza las partidas de recursos dedicados a la remediación y minimización de daños en Ciberseguridad corporativa.
- Cibervigilancia automatizada 24X7 con alertas en tiempo real sobre vulnerabilidades asociadas al dominio monitorizado.
- Cibervigilancia que proporciona información sobre el estado de ciberseguridad corporativo adaptada al grado de conocimiento técnico de cada receptor de la misma.
- Cibervigilancia que permite tener bajo control las vulnerabilidades asociadas a la información filtrada y expuesta de la organización en la Web, Dark Web y Deep Web.

WHITEPAPER

kartos©
XTI watchbots

Kartos XTI Watchbots: EASM + DRPS + SRS en una sola plataforma

Kartos XTI Watchbots es la plataforma de cibervigilancia desarrollada por Enthec para extender el perímetro de seguridad controlado por las organizaciones.
Concebida desde un enfoque de estrategia hacker, Kartos está en permanente proceso de I+D para incorporar categorías y capacidades adelantadas a la evolución de los ciberataques.

External Attack Surface Management

Detección de activos corporativos e información sobre sistemas, servicios en la nube y aplicaciones que están disponibles y visibles en el dominio público para cualquier ciberdelincuente.

Digital Risk Protection Services

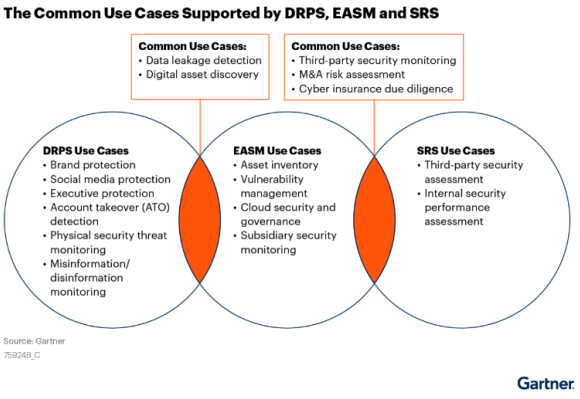
Detección de información contextual sobre posibles agentes de ataques, sus tácticas y procesos para llevar a cabo actividades maliciosas. Eliminación de actividades maliciosas en nombre de la organización.

Security Rating Services

Evaluación independiente de riesgos propios y de terceros, para una visualización amplia de la madurez en ciberseguridad de cualquier organización utilizando un enfoque externo. Ampliación y ponderación de la información proporcionada por los métodos tradicionales de evaluación de riesgos por terceros.

Análisis de 9 categorías de amenazas

- Red
- Salud de DNS / Phishing
- Gestión de Parches
- Reputación IP
- Seguridad Web
- Seguridad e-mail
- Filtración de Documentos
- Filtración de Credenciales
- Redes Sociales



WHITEPAPER

kartos©

XTI watchbots

- **Capa de IA** que permite el funcionamiento 100% automatizado sin intervención humana en ninguna parte del proceso.
- **Herramienta estrictamente no intrusiva**. La investigación se realiza en Internet, la Deep Web y la DarkWeb y no se ataca el perímetro IT de las organizaciones, por lo que su funcionamiento y la información obtenida cumplen estrictamente con los límites impuestos por la legislación.
- Única plataforma que analiza las **conversaciones en redes sociales desde la perspectiva de detección de amenazas** y ataques, más allá de la relativa a reputación y branding.
- **Funcionamiento continuo 365x24x7**, lo que permite detectar filtraciones de nueva información prácticamente en tiempo real
- **Máxima sencillez de uso**. No requiere ninguna configuración compleja. Basta con introducir el dominio en la plataforma y funciona de manera autónoma, sin necesidad de configurar parámetros de búsqueda ni de cualquier otro criterio de localización de información.
- **Monitorización automatizada, objetiva y continúa de los riesgos causados por las terceras partes** que pertenecen a la Superficie de Ataque Externa de la Administración.

Conoce más sobre nuestras licencias
Prueba de forma gratuita la Cibervigilancia XTI → hello@enthec.com
Empieza a usar Kartos

Enthec es una Deep Tech de desarrollo y fabricación de software de Ciberseguridad con enfoque hacker, para extender el alcance de las estrategias de ciberprotección de las organizaciones.

Fundada como startup en 2019 por María Rojo, Enthec ha crecido a través de rondas de financiación y del éxito de su plataforma Kartos hasta consolidarse como una de las Deep Tech con soluciones más innovadoras y eficaces en el campo de la Ciberseguridad.

Para conocer más sobre nosotros, puedes entrar en nuestra web:

www.enthec.com