Tendencias en ciberseguridad

Distribución de ciberinteligencia

Es un modelo basado en el **intercambio de información** entre organismos, públicos y privados, proveniente del análisis de ciberamenazas con el objetivo de mejorar y agilizar la detección y actuación ante las amenazas en ciberseguridad. Este modelo se basa en la creación de un ecosistema de información sobre amenazas colaborativo, mediante mecanismos de vigilancia y respuesta que refuercen el uso de estándares interoperables y seguros. Se requiere de **acciones coordinadas y conjuntas** a nivel nacional que sirvan a las necesidades de todos los usuarios para compartir información entre entidades públicas, sectores clave, IICC y otros stakeholders.

ORIGEN DE LA TENDENCIA

ECONÓMICO/EMPRESARIAL · DEMANDA · NORMATIVA · TECNOLOGÍA

Tan pronto como los incidentes y las vulnerabilidades son detectadas, se inicia un proceso de gestión en el que se genera un elevado volumen de información que es necesario conocer y procesar en el mínimo tiempo posible. Esta información proviene de múltiples fuentes, propias o facilitadas por otras organizaciones, públicas o privadas. Procesar y compartirla es un aspecto crítico en la gestión de la ciberseguridad de los gobiernos. La Unión Europea, a través de **la propuesta de Directiva de Seguridad en las Redes y la Información** (Directiva NIS), alineada con la Estrategia de Ciberseguridad de la UE, determina en su artículo 9 la necesidad de establecer un Sistema Seguro de compartición de información sobre amenazas entre los diferentes CERTs europeos. Por otro lado, el Senado de Estados Unidos acaba de aprobar la **Ley de Compartición de Información de Ciberseguridad** (CISA por sus siglas en inglés) con el fin de aumentar la protección gubernamental a aquellas empresas que voluntariamente decidan compartir con el Gobierno federal aquellos datos que consideren que podrían constituir ciberamenazas.

UBICACIÓN EN LA CADENA DE VALOR DE LA CIBERSEGURIDAD

Fabricación → Comercialización → **Servicios**

Los sistemas de **compartición de información de ciberamenazas** se encuadrarían en el último eslabón de la cadena, siendo prestado este servicio de intercambio principalmente por CERTs públicos pero también privados con servicios de ciberinteligencia, hacia las administraciones públicas y las infraestructuras críticas.

IMPACTO EN BENEFICIARIOS

USUARIO/PARTICULAR	EMPRESAS	ADMINISTRACIÓN PÚBLICA
Impacto en usuarios ○ ○ ○	Impacto en industria ● ● ●	Impacto en gobiernos ● ● ●
El impacto en usuarios o ciudadanos de la compartición de información sobre ciberamenazas es bajo. Sin embargo, estos sistemas redundan en una **mayor seguridad y fiabilidad** de las infraestructuras críticas del país, evitando la interrupción de servicios esenciales a la sociedad.	Los CERT de carácter privado así como las empresas de la industria de la ciberseguridad poseen bases de datos de **caracterización de ciberamenazas**, incidentes y vulnerabilidades 0-day, pudiendo suministrar esta información a las administraciones públicas para aumentar su protección.	La creación de un sistema global o red de intercambio de información tiene un alto impacto en la administración pública española y en los gobiernos de los países, ya que permite hacer frente a ataques de **ciberespionaje y ciberterrorismo** que comprometen la seguridad del país.

CLASIFICACIÓN DE LA TENDENCIA

SOLUCIONES DE PREVENCIÓN · SOLUCIONES DE CONTROL · SOLUCIONES DE MITIGACIÓN

Las redes o sistemas de intercambio de ciberinteligencia **se encuadrarían en los tres tipos**, puesto que la **caracterización completa de las ciberamenazas** implicará, por un lado, la puesta en marcha de mecanismos efectivos para prevenirlas; por otro, la disposición de herramientas de monitorización configuradas específicamente para detectarlas; y, por último, las acciones a llevar a cabo para mitigarlas en caso de que se materialicen.

CICLO DE VIDA DE LA TENDENCIA

DESARROLLO · **INTRODUCCIÓN** · CRECIMIENTO · MADUREZ

Estos sistemas están siendo desarrollados por empresas y CERTs con el fin de proteger infraestructuras críticas y entidades privadas (como el servicio Cyber Threat Intelligence Sharing de CyberSOC); asimismo, el CERTSI participa en una plataforma de reciente creación, para el intercambio de información de ciberamenazas con otros CERTs europeos y socios internacionales.

Sin embargo, es necesario establecer un marco regulatorio estricto, así como unos **estándares y protocolos** de intercambio de información seguros, con el fin de eliminar las barreras relacionadas con las reticencias y suspicacias a la hora de compartir información de **carácter crítico y estratégico** a nivel gubernamental.

Tendencias en ciberseguridad

Distribución de ciberinteligencia

ÁMBITO DE APLICACION

El sector de aplicación de esta tendencia es el de las **administraciones públicas** y más concretamente aplica al control de fronteras y a los mandos de ciberdefensa del Estado. La interrupción de sistemas y el ciberespionaje constituyen las principales amenazas a los que hacen frente los gobiernos. Asimismo, este servicio es demandado por empresas consideradas infraestructuras críticas.

CARACTERIZACIÓN DEL SECTOR DESTINATARIO

El sector público Español presenta 7 Instituciones del Estado y la Administración General del Estado (AGE), está integrada por la Administración Central, la Administración Periférica (Delegaciones de Gobierno en las Comunidades Autónomas, Subdelegaciones del Gobierno en las Provincias y los Direcciones Insulares), los Organismos Públicos adscritos a los Ministerios, la Administración del Estado en el Exterior (embajadas y consulados) y las Instituciones Reguladas por normas especiales (AEAT, Banco de España); ésta a su vez se organiza en torno a 13 Ministerios.

En cuanto al gasto de la AGE en ciberseguridad en 2014:

- La **inversión en hardware de seguridad** fue de **3,48 millones de euros**.
- El **gasto en software de seguridad**, supuso una cuantía de **6,71 millones de euros**.
- En cuanto a los **servicios informáticos**, el gasto de la AGE en servicios de seguridad representó un **0,01% sobre el total** de servicios.

El **Centro de Respuesta ante incidentes del Centro Criptológico Nacional** (CCN-CERT) es el organismo competente para el **tratamiento de vulnerabilidades** y la gestión y resolución de incidentes de ciberseguridad de la **AGE**, las **administraciones** de las 17 **Comunidades Autónomas** y 2 Ciudades Autónomas y las 8.125 **entidades locales**.

PREVISIONES DE DEMANDA

CRECIMIENTO

- En el año 2014, el CCN-CERT gestionó 12.916 incidentes en las Administraciones Pública, en empresas y organizaciones de interés estratégico para el país. El incremento de incidentes de 2013 a 2014 fue de alrededor de un 78%.
- De los incidentes registrados en 2014, el **11% fueron catalogados con un nivel de riesgo entre muy alto y crítico**; afectando a los sistemas de la organización y a su información sensible. Estas cifras indican que los sistemas y comunicaciones más críticas, entre ellas las de la Administración, reciben una media de cuatro ataques diarios.

CLIENTES

- Administraciones Públicas y Gobiernos.
- Cuerpos y fuerzas de seguridad del Estado.
- Infraestructuras Críticas.

MODELOS DE NEGOCIO

DIFERENCIACIÓN EN COSTE | **DIFERENCIACIÓN EN PRESTACION DE SERVICIOS** | **DIFERENCIACIACIÓN EN VALOR AÑADIDO**

CASO DE ÉXITO

CCN-CERT centro criptológico nacional

- El CERT del Centro Criptológico Nacional ha puesto en marcha una **plataforma de intercambio de información y conocimiento de ciberamenazas**, a la que únicamente pueden acceder las organizaciones registradas en el Sistema de Alerta Temprana (SAT) del CERT Gubernamental Nacional.
- Este sistema, llamado **REYES** y basado en **la tecnología MISP** (Malware Information Sharing Platform), está configurado para ofrecer un modo de intercambio de información entre distintas organizaciones que internamente generan ciberinteligencia. El sistema ofrece una base de datos centralizada de eventos de ciberseguridad en un formato estructurado compatible con iniciativas como OpenIOC o STIX, y con funcionalidades como correlación de eventos en base a sus atributos, importación y exportación de estos eventos en distintos formatos.