Capítulo cuarto

El intercambio de información de ciberamenazas

Miguel Rego Fernández
Director General del Instituto Nacional de Ciberseguridad (INCIBE)

Pedro Pablo Pérez García
Global Security VP en Telefónica & CEO 11paths

Resumen

Las amenazas cibernéticas son cada vez más complejas y por lo tanto más difíciles de gestionar. La compartición de información y el trabajo conjunto entre equipos de respuesta de distintos CERT/CSIRT facilitan la generación de una Inteligencia Global que mejora la capacidad de actuar de forma preventiva. Para ello, es necesario que los agentes públicos y privados se sientan implicados con la ciberseguridad, se establezcan mecanismos que faciliten la coordinación entre los distintos actores públicos y privados y la cooperación, facilitando el intercambio de información

El objetivo principal del *Information Sharing* es la recopilación, el almacenamiento y la distribución de la información necesaria para actuar de forma homogénea, rápida y eficaz contra las ciberamenazas, generando un conocimiento común y compartido. Aunque la regulación presente y futura impone la necesidad de compartir información y de notificar las brechas de seguridad es necesario armonizar a nivel internacional la legislación, superar la desconfianza de facilitar información, frecuentemente considerada de alta sensibilidad y establecer y adoptar estándares para la homogeneización de los formatos.

Abstrac

Cyber threats are becoming more complex and therefore more difficult to manage. Information sharing between different CERT/CSIRT facilitates the creation of a Global Intelligence and improves the ability to act preventively. Therefore, it is necessary to facilitate coordination between public and private actors involved in cybersecurity in order to foster cooperation and the exchange of information.

The main objective of the Information Sharing is the collection, storage and distribution of information necessary to act quickly and effectively against cyber threats, creating a common and shared knowledge. Although the present and future regulation imposes the need to share information and to notify security breaches, it is necessary to harmonize international law, overcome mistrust to provide information, often considered highly sensitive, and establish and adopt standards for homogenization formats.

Palabras clave

CERT, CSIRT, incidente, amenaza, vulnerabilidades, plataforma, formato, regulación, barreras, beneficios, inteligencia, respuesta, mitigación, estándares, cooperación, conocimiento.

Keywords

CERT, CSIRT, incident, threats, vulnerabilities, platform, format, regulation, barriers, benefits, intelligence, response, mitigation, standards, cooperation, knowledge.

Situación actual

Necesidad de intercambiar información de amenazas e incidentes

Ante la creciente complejidad en los ciberataques se requiere un mayor nivel de colaboración entre los actores públicos y privados relacionados con la gestión de las ciberamenazas. La identificación y caracterización de las amenazas del ciberespacio y la detección de incidentes, que realiza localmente un Equipo de Respuesta ante Incidentes (*Computer Emergency Response Team*, *CERT*), cuando se intercambia de forma controlada mediante servicios de compartición de información, facilita la prevención global de los ciberataques. De esta forma la identificación, análisis y compartición de información por parte de un *CERT* puede facilitar que estos eventos se repitan de forma global y contribuirá a mejorar la eficiencia y al ahorro de tiempo y esfuerzo en la respuesta ante los incidentes, en los análisis forenses posincidente, incrementando las sinergias entre *CERT*/CSIRT y la adopción de prácticas y procedimientos comunes.

Con objeto de mejorar la respuesta ante incidentes y prevenir, por ejemplo, que campañas de *malware* puedan hacerse extensivas globalmente, aparecen en escena las actividades de colaboración potenciadas por organismos internacionales, compañías y multinacionales de seguridad así como *CERT* de todo el mundo. Bajo esta óptica toma forma el concepto de *Information Sharing*.

Equipos de Respuesta ante Incidentes con diferentes niveles de madurez pueden trabajar de forma activa en una respuesta ante incidentes coordinada de forma global, aportando y compartiendo información de valor y mejorando la seguridad de todo el ecosistema. Dado que la naturaleza de los ciberataques frecuentemente es global, es fundamental que la respuesta y neutralización no se limite al ámbito local o nacional sino que se actúe desde una perspectiva transfronteriza. Para que esta acción global sea posible se necesita colaborar intercambiando, de forma segura y confiable, información sobre dichos incidentes.

Sin embargo, poner en marcha y mantener un procedimiento de compartición de información no es tarea tan sencilla como en principio podría suponerse. En general, habrá que superar múltiples escollos que dificultan este proceso. Entre estas dificultades podemos citar: el establecimiento de una relación de confianza, superar el recelo a dar visibilidad a la información obtenida y llegar a un consenso para dar formato a la información y a las cuestiones relacionadas con su tratamiento, mantenimiento, clasificación y difusión. Estamos hablando del uso de estándares.

Inhibidores y habilitadores para la compartición de información de amenazas

Los aspectos técnicos son la barrera más común para el intercambio de información eficaz entre *CERT*. Estos problemas técnicos están relacionados

con la solución utilizada para facilitar el intercambio automatizado y la capacidad de interoperar con otros sistemas desplegados por los *CERT*/CSIRT locales. Otro problema muy importante está relacionado con la calidad de los datos, es decir, que la información compartida por uno de los actores sea identificada como relevante y de valor para el resto de la comunidad.

Sin embargo, los obstáculos técnicos son más fáciles de superar que los problemas legales, sobre todo con la creciente estandarización para el intercambio, almacenamiento y procesado de la información. En el intercambio de información con los *CERT* las barreras legales y los problemas de confianza son a menudo los principales obstáculos para que el intercambio se materialice.

Finalmente, a menudo los operadores miembros de la comunidad de intercambio, inmersos en la operativa del día a día, manifiestan un bajo nivel de interés tanto en compartir como en utilizar la información compartida, lo que provoca que el sistema global, poco a poco, vaya perdiendo utilidad y valor.

Barreras en el intercambio de información derivados de aspectos legales

En torno a los aspectos jurídicos y de procedimiento de intercambio de información entre los *CERT* y otras partes interesadas, los aspectos legales y procedimentales son las barreras más frecuentes. En esencia, los *CERT* y otras organizaciones similares frecuentemente tienen dudas acerca de si un conjunto particular de información puede ser compartida, con quién y en qué condiciones. Se generan dudas respecto a si la información que se intercambia presenta problemas legales en materia de protección de datos y protección de la privacidad dado que, incluso en el ámbito de la Unión Europea, se pueden encontrar diferentes interpretaciones relativas a los criterios de protección de la privacidad. Debido a estas cuestiones, a menudo el intercambio de información entre los *CERT* y otros actores se inhibe.

Entrando en detalle sobre los puntos más complicados:

- Retención de datos: la vigencia y periodo de conservación de los datos, así como el ciclo de vida de la información desde su generación, procesado, almacenado, uso y borrado/destrucción es clave para una compartición que legalmente sea viable. Normativas que homologan tratamientos en privacidad a nivel Europeo, mecanismos como Safe Harbour o Privacy Shield ayudan a establecer garantías entre las partes.
- Alojamiento de datos: La complejidad legal que supone el alojamiento *cloud* es relevante, dado que es importante conocer donde están ubicados los sistemas que almacenan los datos asi como la legislación del país y los tratados con países afines.
- Compartición de datos de carácter personal: Evidentemente, la transmisión de datos requiere los consentimientos oportunos acorde con la ley

de protección de datos del país y, además, el tener datos tan comunes como las *IP* (considerados datos de carácter personal en varias geografías) añade complejidad legal. Asimismo, siempre que aparecen datos de carácter personal tenemos la complejidad adicional de gestionar adecuadamente los derechos de los titulares, tema que debe ser tenido en cuenta en el proceso de transferencia.

Según algunas opiniones, los problemas legales en el intercambio de información no son únicamente el resultado de la falta de armonización internacional en la legislación de protección de datos sino, y especialmente dentro de la Unión Europea, de las diferentes interpretaciones de las leyes nacionales por parte de diferentes organismos.

Barreras en el intercambio de información derivados de falta de confianza

Los problemas de confianza son algunos de los obstáculos más importantes para la comunicación mejorada y eficaz entre los *CERT* y otras partes interesadas. En ciberseguridad la confianza es la característica más importante de una relación de cooperación exitosa. Además, la confianza se debilita cuando solamente una de las partes está activa en el intercambio de información, sin obtener mucho a cambio de la otra parte.

Comúnmente aparecen diferentes actores donde las fronteras del uso de la información no están claras y requieren clarificar en alto detalle el uso de la misma, así como el alcance del tratamiento. Por ejemplo, es frecuente la aparición de actores en la empresa privada que pueden usar la información para su uso o para la venta, igualmente organismos públicos pueden usar la información para su protección o ayudar a otras administraciones.

	PÚBLICO	PRIVADO
CONSUMIDOR INFO	AAPP X + AAPP Y	ACME
PRESTADOR INFO	AAPP Y	ACME

En relación a la falta de confianza, y especialmente en los *CERT*/CSIRT de ámbito privado, se añade un nuevo problema en base a la desventaja competitiva que supone para un *CERT*/CSIRT que comparte información frente a otro que solo recibe, invirtiendo el primero en recursos humanos y técnicos de los cuales saca provecho el contrario. Esto hace a menudo que la colaboración entre *CERT*/CSIRT privados sea muy escasa.

También es habitual que la información de incidentes críticos, especialmente relacionados con los ataques de tipo APT, en los que de forma frecuente hay robo de información a la víctima no sea compartida en la comunidad con el fin de evitar los problemas reputacionales que puede suponer.

Insuficiente interés por parte de las partes

La comunicación operativa entre los *CERT*/CSIRT, es una práctica habitual y, por tanto, no es frecuente ver desinterés en el intercambio de información por parte de los mismos. Por lo general, los *CERT* no solo están dispuestos a compartir información de incidentes de seguridad, sino también a redactar informes y estudios descriptivos que se comparten con la comunidad, informes que son generalmente muy bien recibidos y apreciados entre todos los actores. Sin embargo, debido a las carga de trabajo, a menudo esta información de alto valor se demora excesivamente en el tiempo. Cuando los *CERT* están gestionando un incidente los expertos se centran en aspectos muy operativos como la mitigación y la coordinación y a veces no tienen tiempo para compartir informes detallados con el resto de los *CERT*. La descripción de incidentes de alto impacto, a gran escala, son un ejemplo típico de una situación que generaría un informe a intercambiar. La cultura de compartir y la demanda de información no es sin duda un problema, pero las cargas de trabajo son, a menudo, un inhibidor importante.

Barreras de carácter técnico

Muchos *CERT* agradecerían recibir entradas de información automáticas de otros Equipos de Respuesta ante Incidentes para utilizar esa información dentro de su comunidad y prevenir incidentes. Sin embargo, esta automatización basada en plataformas de intercambio cuenta, a menudo, con distintos problemas de índole técnico debido a:

Cambios de formato en la información.

Problemas de sincronización horaria o con el sello de tiempo del evento que se está compartiendo.

Los datos recibidos en relación con los incidentes no contienen suficiente información para iniciar una investigación.

Se necesita seguir trabajando de forma global para mejorar los formatos de información a compartir y, aunque existen muchos estándares en el campo de la seguridad, los *CERT*/CSIRT frecuentemente actúan de forma *ad hoc*.

Es muy importante, antes de convertir los *Data Lakes* donde se aloja la gran cantidad de información generada en auténticos vertederos, tener claros los procesos de conversión de los datos en información, los procesos de generación de metadatos (datos sobre datos), contextualización, etcétera, así como la agregación, correlación y demás procesados con el fin de preparar la conversión final de dicha información en inteligencia (*actionable intelligence*).

DATOS → INFORMACION → INTELIGENCIA

Beneficios y habilitadores en el Information Sharing

El objetivo principal de *Information Sharing* es el de establecer un procedimiento que permita la recopilación, el almacenamiento y distribución de la información necesaria para actuar de forma homogénea, rápida y eficaz contra las ciberamenazas. Esto, además, revertirá en un mejor conocimiento del *malware*, sus mecanismos de ataque y en facilitar las tareas de prevención y respuesta ante incidentes relacionados con actividad.

Figura 4.1. Beneficios del Intercambio de Información (Fuente: Blog de ERTS/CSIRTSI).

Los beneficios derivados del intercambio de información son:

Generar una conciencia del estado global de seguridad

La compartición de información de incidentes y amenazas entre *CERT*/CSIRT nacionales e internacionales permite construir un mapa de situación de la ciberseguridad a nivel global que aporta la visión de lo que está ocurriendo en el ciberespacio y facilita la generación de un conciencia global, en todos los estamentos de la sociedad, sobre la importancia y necesidad de proteger la información y los servicios digitales.

Un estudio realizado en 2013 por ENISE recalca que seguridad y funcionalidad son las dos causas raíz que nos obligan a una mayor compartición, destacando con menor presión rendimiento, interoperabilidad y ahorro de costes.

Las amenazas cibernéticas son cada vez más complejas y por lo tanto más difíciles de gestionar. La compartición de información y el trabajo conjunto entre equipos de respuesta de distintos *CERT*/CSIRT facilitan la generación de una Inteligencia Global que mejora la capacidad de actuar de forma preventiva y facilita la persecución y neutralización de las amenazas.

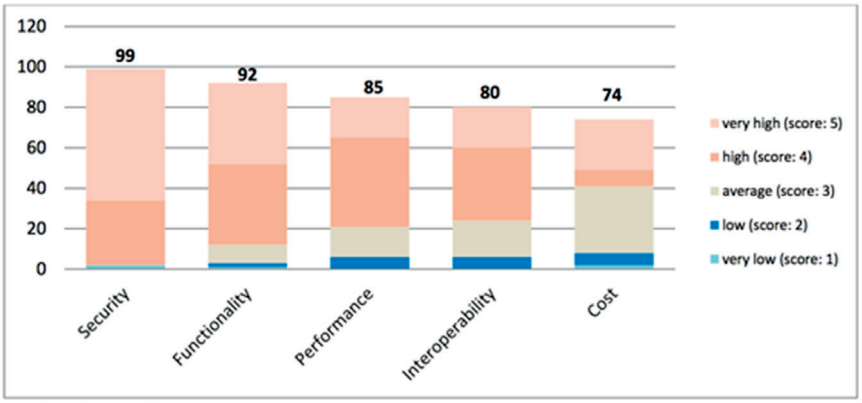

Figura 4.2. Comprensión avanzada de amenazas.

Maduración del conocimiento

Uno de los elementos de información que aportan más valor cuando se intercambian son las «lecciones aprendidas» en relación con la actuación ante una amenaza o un incidente. Esta información mejora el conocimiento colectivo y facilita a los técnicos una mejora en sus niveles de capacitación.

Prevención

Los informes generados por los *CERT* facilitan la caracterización de las amenazas y la descripción de los vectores de ataques y de las ventanas de exposición. Esta información es muy valiosa para que el resto de la comunidad pueda actuar de forma preventiva dentro de su comunidad, identificando de forma temprana situaciones de riesgo y actuando sobre las mismas.

Respuesta ágil

Al compartir información detallada sobre el procedimiento que ha aplicado un *CERT* para la mitigación de un incidente, se facilita que el resto de la comunidad pueda aplicar esas técnicas de forma inmediata, por lo que se ganará en eficacia, reducción del tiempo de mitigación y en eficiencia, aplicando solo recursos estrictamente necesarios en la actuación.

Marco normativo y legislativo aplicable en Europa y España

Europa

Un primer ejemplo en este sentido es la Directiva 2002/58/CE[1] que tiene por objeto proteger la privacidad de los datos personales en el sector de las comunicaciones electrónicas. Sobre la base de un requisito de esta directiva

[1] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sec-

los proveedores de servicios de comunicaciones electrónicas están obligados por ley en todos los Estados miembros de la Unión Europea, bajo ciertas circunstancias también sus ciudadanos, a notificar fallos de seguridad que afecten a datos de carácter personal.

En segundo lugar, la normativa europea del sector de las telecomunicaciones ha definido el deber de notificación de incidentes de seguridad. Sobre la base de la Directiva marco[2] (artículo 13 bis) (Parlamento Europeo y del Consejo, 2009), «los Estados miembros se asegurarán de que las empresas que suministran redes de comunicaciones públicas o presten servicios de comunicaciones electrónicas notifiquen a la autoridad reguladora nacional competente de una violación de seguridad o pérdida de la integridad que haya tenido un impacto significativo sobre el funcionamiento de las redes o servicios. En su caso, la Autoridad Nacional informará a las autoridades nacionales de reglamentación de otros Estados miembros y a la Agencia Europea de Seguridad de las Redes y de la Información (*ENISA*). Por otra parte, la Agencia y la Comisión Europea deben recibir un informe que resuma las medidas adoptadas para resolver los problemas detectados».

Como tercer ejemplo relacionado con la notificación de incidentes, se encuentra la Directiva NIS 2016/1148[3], aprobada por el Parlamento Europeo el pasado 6 de julio, que recoge la obligación para los operadores de los siete sectores estratégicos afectados por la directiva de notificar incidentes que tengan un impacto significativo en la seguridad, o continuidad, de los servicios principales que suministran. La Directiva NIS será traspuesta a las leyes nacionales, en el plazo máximo de veintiún meses desde su aprobación, a través de un acto legislativo (ley, decreto o de un instrumento reglamentario de otro tipo).

Un cuarto ejemplo en relación con las obligaciones de notificación se deriva de otro acto legislativo, el Reglamento de servicios de identificación y la confianza electrónicos (eIDAS) (Parlamento Europeo y del Consejo, 2014). El artículo 19 de este Reglamento establece que los proveedores de servicios fiduciarios deben informar de «cualquier violación de seguridad o pérdida de integridad que tiene un impacto significativo en el servicio de confianza proporcionado o en los datos personales» a los órganos de control pertinentes (por ejemplo, una autoridad de seguridad o de protección de datos) y, en algunos casos, a ENISA. Dado que el Reglamento es directamente aplicable en los Estados miembros sin necesidad de transposición, la regla de notifi-

tor de las comunicaciones electrónicas (directiva sobre la privacidad y las comunicaciones electrónicas).

[2] Directiva 2002/21/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas.

[3] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

cación consagrada en el presente acto legislativo (el Reglamento eIDAS) se aplica directamente a nivel nacional.

España

La primera iniciativa a analizar es la Estrategia de Ciberseguridad Nacional (ECSN), aprobada en diciembre de 2013. Incluye como uno de sus cuatro principios rectores la Responsabilidad Compartida, estableciendo que: «todos los agentes públicos y privados con responsabilidad en esta materia, incluyendo también a los propios ciudadanos, han de sentirse implicados con la ciberseguridad. Para ello, se hace precisa una intensa coordinación de los diferentes organismos de las Administraciones públicas y una adecuada cooperación público-privada capaz de compatibilizar iniciativas y propiciar el intercambio de información».

Este principio se desarrolla, posteriormente, en dos líneas de acción en las que se establece el marco estratégico que facilita el desarrollo de iniciativas para el intercambio de información. En concreto, la línea de acción 1, «Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas» establece la necesidad de garantizar la coordinación, la cooperación y el intercambio de información entre la Administración General del Estado, las Comunidades Autónomas, las Entidades Locales, el sector privado y los organismos competentes de la Unión Europea e internacionales para asegurar la permanente concienciación, formación y capacidad de respuesta a través del Sistema de Intercambio de Información y Comunicación de Incidentes. Esta aproximación se refuerza, posteriormente, a través de la línea de acción 8, «Compromiso Internacional» que, con el objetivo de promover un ciberespacio internacional seguro y confiable, en apoyo a los intereses nacionales, facilita la promoción de las mejores prácticas en el conocimiento de la situación, la alerta y la respuesta ante incidentes cibernéticos.

La ECSN fue desarrollada a través del Plan Nacional de Ciberseguridad (PNCS) aprobado en 2014 que, a su vez, se concretó en nueve «planes derivados». El plan derivado 9, «Intercambio de Información sobre Amenazas», se ha dedicado específicamente a desarrollar esta actividad, desarrollando e implantando los procedimientos, mecanismos y herramientas que permitan llevar a cabo el intercambio de información sobre ciberamenazas entre los órganos y organismos con competencia en materia de ciberseguridad de la Administración General del Estado (AGE), las Comunidades Autónomas, las Entidades Locales y el sector privado nacional, así como con los correspondientes organismos competentes de la Unión Europea, OTAN e internacionales; contribuyendo con ello a lograr una coordinación y cooperación eficaces en la ejecución de las necesarias acciones de prevención, detección, reacción y respuesta frente a las ciberamenazas.

El segundo instrumento analizado es el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), el organismo que se encarga de impulsar, coordinar y supervisar todas las actividades que tiene encomenda-

das la Secretaría de Estado de Seguridad del Ministerio del Interior en relación con la protección de las infraestructuras críticas españolas, conforme a la Ley 8/2011[4], en la que se Establecen las Medidas para la Protección de las Infraestructuras Críticas, posteriormente desarrollada a través del Real Decreto 704/2011[5]. La revisión en 2015 del *Plan Nacional para la Protección de las Infraestructuras Críticas*, de 7 de mayo de 2007, permitió incluir la obligación de que los Operadores de Infraestructura Crítica reporten al *CERT* de Seguridad e Industria (*CERT*/CSIRTSI) incidentes de ciberseguridad conforme al nivel de alerta establecida en cada momento. Para facilitar el cumplimiento de este requisito se desarrolló la *Guía de Reporte de Incidentes de Ciberseguridad*[6], que establece el procedimiento a seguir por los operadores y los niveles de atención y respuesta por parte del *CERT*/CSIRTSI en función del nivel de alerta existente.

Figura 4.3. Niveles de Alerta del PNPIC (Fuente CNPIC).

El tercer instrumento es la Ley 9/2014, General de Telecomunicaciones[7], que incluyó en una disposición adicional, la «disposición adicional novena. Ges-

[4] Ley 8/2011, de 28 de abril, por la que se Establecen Medidas para la Protección de las Infraestructuras Críticas.

[5] Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas.

[6] Instrucción pendiente de publicación.

[7] Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

tión de incidentes de ciberseguridad que afecten a la red de internet**»,** la obligación y necesidad de que los prestadores de servicios de la Sociedad de la Información, los registros de nombres de dominio y los agentes registradores que estén establecidos en España presten su colaboración con el *CERT* competente en la resolución de incidentes de ciberseguridad que afecten a la red de internet. Para el ejercicio de las funciones y obligaciones anteriores, el punto 2 de dicha disposición establece que los prestadores de servicios de la Sociedad de la información, respetando el secreto de las comunicaciones, suministrarán la información necesaria al *CERT* competente y a las autoridades competentes, para la adecuada gestión de los incidentes de ciberseguridad, incluyendo las direcciones IP que puedan hallarse comprometidas o implicadas en los mismos.

Por último, se recoge la necesidad de informar a la Agencia Española de Protección de Datos de las brechas de ciberseguridad que supongan la filtración de información de carácter personal. La Directiva 2002/58/CE [8] establece que los proveedores de servicios de comunicaciones electrónicas disponibles para el público están obligados a notificar las quiebras de seguridad que puedan afectar a datos personales a las autoridades nacionales competentes y, en algunos casos, también a los abonados y particulares afectados. El 25 de agosto de 2013 entró en vigor el Reglamento Europeo 611/2013[9], de la Comisión, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE. El reglamento se aplica a los proveedores de servicios de comunicaciones electrónicas disponibles para el público y, en ciertos casos, a abonados y particulares afectados, y en España lo ha incorporado la reforma de la Ley General de Telecomunicaciones (LGT), en vigor desde el 11 de mayo. En el caso español, la competencia para recibir estas comunicaciones por parte de los proveedores de servicios corresponde a la Agencia Española de Protección de Datos.

La AEPD puso en marcha un sistema para que los proveedores de servicios de comunicaciones electrónicas notifiquen las eventuales quiebras de seguridad que se hayan producido en sus sistemas y que puedan afectar a los datos personales que tratan. El procedimiento está disponible a través del apartado «Notificación preceptiva de quiebras de seguridad» de la Sede Electrónica de la Agencia.

[8] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

[9] Reglamento (UE) n.º 611/2013 de la Comisión de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, sobre la privacidad y las comunicaciones electrónicas.

No se han incluido en este capítulo otras obligaciones derivadas de reglamentos sectoriales que exigen la notificación o compartición de información relacionada con brechas de ciberseguridad.

Además del sector público en España con INCIBE, CCN, Ministerio de Defensa o CNPIC, entre otros, hay empresas privadas que publican constantemente informes y datos sobre ciber amenazas, ejemplos como 11PATHS (Telefónica) o BLUELIV. Cabe destacar también la labor de organismos como CCI, ISMS FORUM o SIC, que fomentan el intercambio de información, generación de reportes así como foros para la compartición de conocimiento. En líneas generales se ha producido un avance muy significativo en los últimos años en materia de compartición de información y conocimiento.

Áreas para una cooperación efectiva en el intercambio de amenazas

Compartir información sobre amenazas de seguridad supone un gran beneficio siempre que recoja contenido de valor y se difunda de forma estructurada. Respecto al contenido, la información útil debe incluir avisos de seguridad sobre vulnerabilidades, informes y estudios sobre protocolos, sistemas y prácticas de seguridad, pero, sobre todo, información preventiva y reactiva para enfrentar ciberamenazas e incidentes de seguridad.

Figura 4.4. Áreas de intercambio de información (fuente CERT/CSIRTSI).

A continuación se describe la información que, potencialmente, se va a compartir de forma colaborativa entre distintos *CERT* públicos o privados y con sus comunidades:

Avisos de seguridad

Los *CERT*/CSIRT aglutinan un volumen muy alto de información relacionada con eventos de seguridad asociados a la actividad que desarrolla y que

puede complementar en colaboración con otros actores públicos o privados relacionados con la ciberseguridad. Estos eventos, tratados y procesados de forma adecuada pueden dar lugar a la identificación de incidentes de forma proactiva que luego son comunicados dentro y fuera de la comunidad (*constituency*) de actuación del *CERT* para provocar una acción de mitigación.

De forma adicional las vulnerabilidades, puntos débiles de seguridad en productos o servicios, son identificadas y reportadas por los propios fabricantes o por investigadores para que puedan corregirse con los correspondientes parches de seguridad. Los *CERT* evalúan y valoran la información recibida sobre estas vulnerabilidades y emiten avisos que contienen la descripción, la criticidad, los sistemas afectados y las posibles soluciones destinadas a mitigar o minimizar el problema durante el periodo en el que el fabricante elabora el parche.

Informes

Uno de los elementos que utilizan los *CERT* para fomentar la cultura de la seguridad y la generación de conocimiento especializado en la materia es la creación de guías y estudios sobre temas relacionados con la ciberseguridad. Estas guías y estudios tienen como finalidad aportar tanto valor práctico como teórico para fomentar y mejorar la seguridad digital en todos los ámbitos de la sociedad y para los administradores de sistemas y técnicos en ciberseguridad. En su elaboración, los *CERT* se basan en su experiencia práctica en la neutralización de una determinada amenaza, en la gestión de un determinado tipo de incidente, en su conocimiento en relación a cómo configurar una determinada tecnología con el objetivo de minimizar la probabilidad de que se pueda ver afectada por un ciberataque...

Figura 4.5. Publicaciones del CERT/CSIRTSI (fuente CERT/CSIRTSI).

Estudios y herramientas

Los *CERT* ponen a disposición de su comunidad herramientas de ciberseguridad enfocadas a la prevención, detección y respuesta a incidentes de ciberseguridad que, en muchos casos, han sido desarrolladas por el propio *CERT* en

base a la necesidad de responder a una amenaza concreta, posiblemente de alto impacto, para la que el mercado de productos de ciberseguridad no tiene respuesta en ese momento concreto. En otras ocasiones, estas herramientas facilitadas por el *CERT* tienen como objetivo mejorar el nivel de concienciación respectos a los riesgos generales o asociadas a una tecnología específica.

Figura 4.6. Estudios y herramientas de «Protege tu Empresa» (fuente INCIBE).

Indicar que también se difunden guías y manuales con instrucciones técnicas para la configuración segura de servidores, sistemas y aplicativos[10].

Incidentes y ciberamenazas

Una de las tareas más importantes de los *CERT* es proporcionar información sobre nuevas ciberamenazas de forma que la información proporcionada sea relevante y tenga validez y permita que su comunidad u otros *CERT*/CSIRT puedan protegerse de forma adecuada, facilitando el aprendizaje y la mejora efectiva de los niveles de seguridad.

Figura 4.7. Qué podemos compartir (fuente: plataforma ICARO-INCIBE).

[10] Pueden consultarse en https://www.incibe.es/protege-tu-empresa/guias

Uno de los principales problemas para facilitar toda esta información, de forma que pueda ser procesada por el receptor e integrada en su arquitectura de ciberseguridad, es el formato adoptado. A continuación se analizará esta problemática.

Los problemas de la normalización: iniciativas privadas vs *estándares* de facto

La siguiente dificultad a superar para el intercambio de información es establecer un formato común y reconocido entre los beneficiarios de la información. En este sentido, el uso de estándares posibilitará un uso y una distribución eficiente y rápida de la información.

Con este objetivo, la IETF da los primeros pasos hacia la estandarización en 2007 publicando el RFC 5070 que define *IODEF*, acrónimo para *Incident Object Description Exchange Format*. Esta especificación recoge una serie de pautas dirigidas a los *CISRT* (*Computer Security Incident Response Team*) que son deseables a la hora de documentar los indicadores significativos en incidentes de seguridad. Se basa en esquemas XML para la gestión de los datos y será un punto de referencia para posteriores adaptaciones.

El camino hacia la adopción de un estándar no siempre es único y rápido, y tras la especificación IODEF surgen múltiples aproximaciones que pugnan por convertirse en el estándar *de facto*. Entre los estándares que han cobrado mayor protagonismo y aceptación podemos destacar por un lado OpenIOC (de la compañía FireEye) y las propuestas más colaborativas CybOX, STIX y TAXII (iniciativa del Gobierno estadounidense a través de MITRE, DHS y US-*CERT*).

Datos a intercambiar

Existen múltiples datos a intercambiar, que van desde simples HASH de ficheros maliciosos, IP registradas, dominios y elementos de red, hasta las

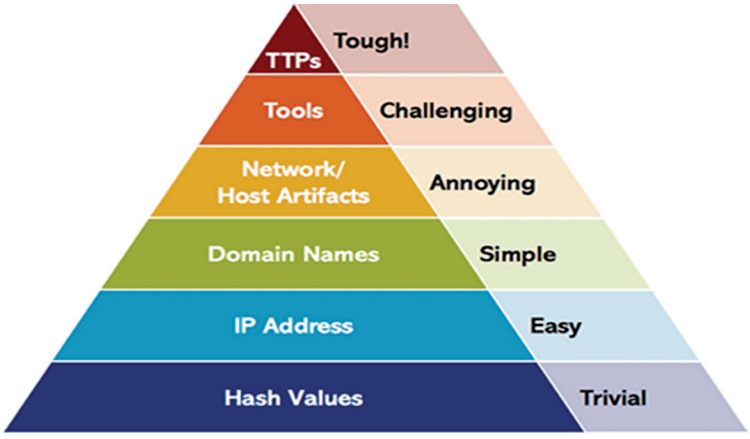

Figura 4.8. «Pirámide del dolor» de David J. Bianco.

herramientas, tácticas y procedimientos de los atacantes. Existen múltiples referencias a los beneficios de la compartición de información para los actores, siendo una de las más conocidas la llamada «Pirámide del dolor» de David J. Bianco (dolor provocado a los atacantes como consecuencia de la acción de compartir).

Métodos de intercambio

Existen tradicionalmente tres métodos de conexión con el objetivo de intercambiar información, además del evidente intercambio uno a uno:

- HUB (Un ente centraliza la información de los productores y la transmite a los consumidores N:1-1:M).
- SOURCE (una repositorio central al que los usuarios se suscriben 1:M).
- P2P (Relaciones que tienen toda la casuística posible 1:1 ,1:M, N:1 o N:M).

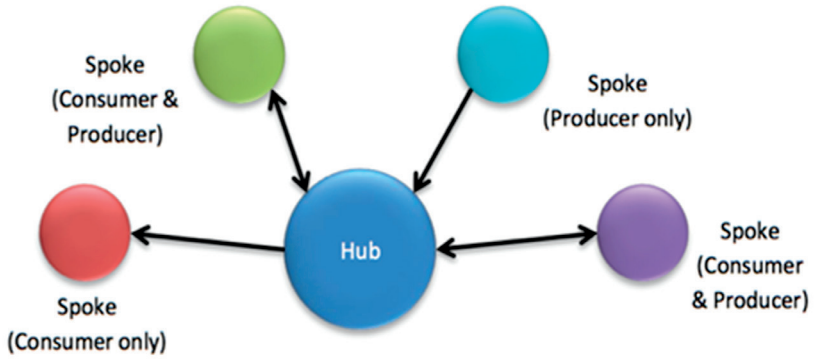

Figura 4.9. HUB.

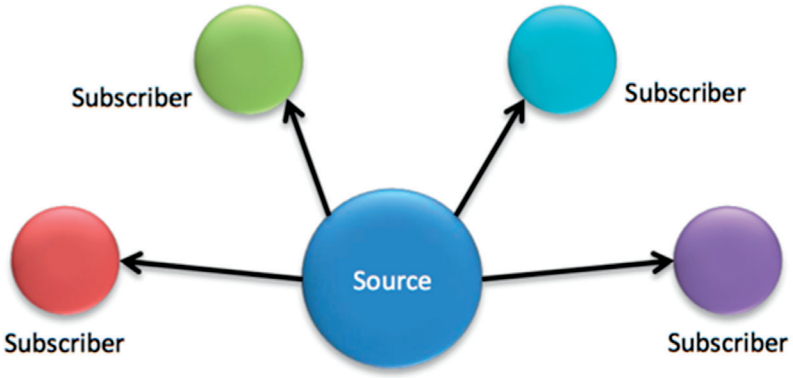

Figura 4.10. SOURCE.

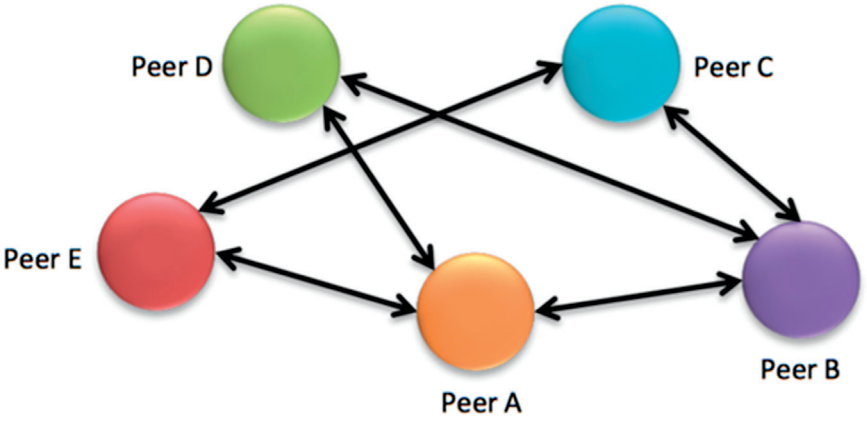

Figura 4.11. PEER to PEER.

Formatos de intercambio de datos de amenazas

Existen múltiples formatos que estandarizan los mecanismos de intercambio de información: STIX, CIF, OPENIOC, CybOX, VERIS, IODEF, TAXII o TLP.

Standard/Framework	2015	2016
Open Threat Exchange (OTX)	50.8%	40.0%
Structured Threat Information Expression (STIX)	45.9%	29.2%
Collective Intelligence Framework (CIF)	39.3%	26.2%
Open Indicators of Compromise (OpenIOC) Framework	32.8%	16.9%
Other	6.6%	13.8%
Cyber Observable eXpression (CybOX)	26.2%	11.5%
Vocabulary for Event Recording and Incident Sharing (VERIS)	19.7%	9.2%
Incident Object Description and Exchange Format (IODEF)	23.0%	8.5%
Trusted Automated eXchange of Indicator Information (TAXII)	32.8%	N/A
Traffic Light Protocol (TLP)	27.9%	N/A

Figura 4.12. Formatos de intercambio de datos de amenazas.

Se distinguen dentro de los estándares varios tipos: los distintos lenguajes formales para la descripción de los indicadores de compromiso (OpenIOC, IODEF o STIX), las definiciones para el intercambio de información (TAXII o RID), las plataformas de gestión de la misma (CDXI, MISP o CIF) y los mecanismos de manejo de incidentes (RT o RTIR).

OpenIOC

Es una iniciativa liderada por la compañía MANDIANT perteneciente a la multinacional FireEye que ha estado presente de manera pionera en la definición y establecimiento del concepto *IoC* (*Indicator of Compromise*)[11] en la gestión de incidentes. Un *IoC* es un ente que describe una evidencia forense para identificar una intrusión en un sistema o red.

OpenIOC se distribuye abiertamente bajo licencia Apache2 [12]y se basa en un esquema XML para definir *IoC* y permite la extensión con información propia. Cuenta con un alto grado de madurez, simplicidad y reconocimiento, si bien en la parte crítica se trata de una implementación libre apoyada principalmente por una empresa y se le acusa de falta de flexibilidad, dado que en gran medida sigue directrices de un único fabricante orientando su uso hacia productos propios. Esta desventaja, asimismo, tiene su parte positiva, pues hay más de quinientas descripciones de entornos completos desarrollados por MANDIANT, lo cual genera una base de datos de adversarios muy completa.

CybOX, STIX, TAXII

Por otro lado, la organización norteamericana MITRE, organización sin ánimo de lucro y mucho más orientada hacia desarrollos colaborativos en múltiples disciplinas tecnológicas que incluye la ciberseguridad, ha puesto grandes esfuerzos en la estandarización de esquemas de *Information Sharing*. MITRE, en conjunción con el Department of Homeland Security, el National Cyber Security Communications, Integration Center y el US-*CERT* de Estados Unidos ha dirigido el desarrollo de los estándares: STIX, TAXII y CybOX. Este desarrollo ha transicionado hacia el consorcio de estándares OASIS. Los esfuerzos de estandarización de MITRE están siendo ampliamente respaldados por la industria y AAPP, por lo que múltiples herramientas lo soportan como estándar *de facto*.

Cyber Observable eXpression (CybOX)

El primer borrador de este estándar es de 2010 e incorpora formatos JSON para la caracterización de información sobre *malware*, detección de intrusiones, respuesta y gestión de incidentes y forense digital. En su estructura se definen más de setenta objetos (ficheros, sesión HTTP, conexión de red, etcétera) caracterizados por tipos base de datos, propiedades y relaciones, utilizando un vocabulario predefinido.

[11] Back to Basics Series: OPENIOC BY Will Gibb.

[12] www.openioc.org, licencia de contenidos abiertos que fomenta la compartición de la información.

***Structured Threath Expression* (*STIX*)**

Este estándar es relativamente reciente y presenta un lenguaje estructurado para describir las ciberamenazas en un formato que puede ser compartido, almacenado y analizado de forma consistente. Aparece para aportar una organización de la información de manera altamente estructurada e interrelacionada para lograr una alta legibilidad y fácil comprensión.

Figura 4.13.

STIX serializa los datos en formato JSON y adopta un formato basado en grafos para ofrecer una representación muy intuitiva de los objetos y relaciones entre los mismos. Los objetos se agrupan en nueve dominios clave: observables, indicadores, incidentes, procedimientos, objetivos de explotación, acciones de respuesta, campañas, actores y reportes.

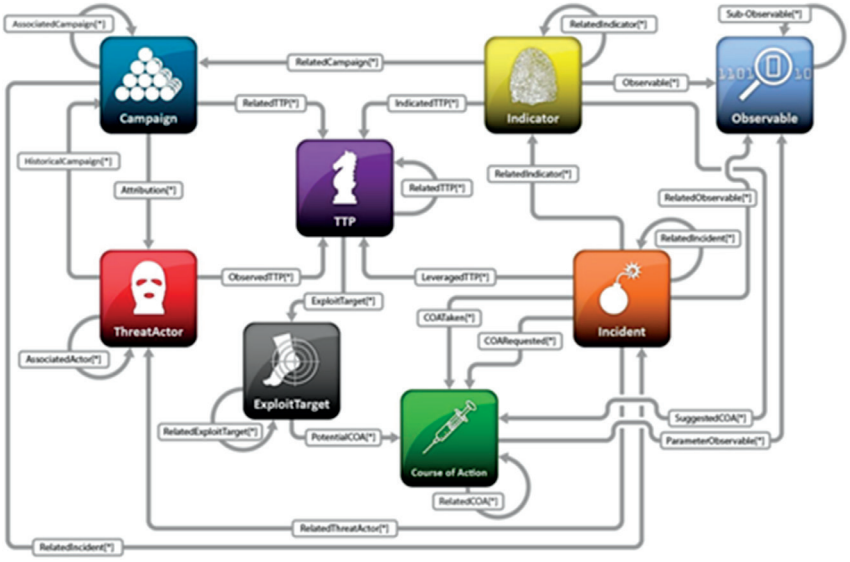

Figura 4.14. Detalle de elementos en STIX. «Detect, SHARE, Protect Solutions for Improving Threat Data Exchange among CERT». ENISA. Octubre de 2013.

Los objetos STIX son indicadores que se encuadran en los referidos dominios y comparten una serie de propiedades para presentar los datos existiendo además objetos de relación que sirven para establecer enlaces entre los dominios (nodos). Es un modelo que está ganando fuerza por su consistencia y usabilidad. Aunque principalmente integra el esquema CybOX, tiene extensiones para incluir otros estándares e indicadores como TLP, OpenIOC, reglas de Snort y YARA.

TAXII, cuya especificación inicial viene de 2012 y fue consolidada en 2014, proporciona unas especificaciones orientadas a conformar un mecanismo flexible de transporte de información de ciberamenazas. TAXII se centra en los mecanismos de distribución de información y adopta otros estándares para el formato de la misma. Así, a través de los servicios definidos por TAXII, las organizaciones pueden intercambiar información de forma segura y automatizada con soporte para múltiples formatos de representación de información de ciberamenazas, especialmente STIX y CybOx. Soporta diversas arquitecturas de comunicación (Hub and Spoke, Peer to Peer y cliente/servidor).

Versión STIX	Información
1.2	Publicada por DHS/MITRE. Esquemas XML.
1.2.1	Publicada por OASIS. Esquemas UML y XML.
2.0	Publicada por OASIS. Basada en JSON y esquema UML.

Tabla 4.1. Estándares de arquitecturas de comunicación.

Estos tres estándares, con el respaldo del consorcio de estándares OASIS, empiezan a consolidarse como opción preferida por múltiples fabricantes para dar formato a la información en sus productos de inteligencia. Entre ellos están importantes multinacionales como IBM (IBM QRadar), Splunk (Splice), Intel Security (McAfee Advanced Threat Defense),VeriSign(iDefense), etcétera.

Múltiples estándares para intercambio de información, un mismo objetivo

ESTÁNDAR	VENTAJAS	DESVENTAJAS
IODEF	Estándar IETF definido por *CERT*/CSIRTS- Independiente de fabricantes- Formato flexible XML-	Adopción limitada- Orientada a incidentes, puede contener información sensible difícil de compartir. Alta granularidad que dificulta implementaciones.
OpenIOC	Licencia libre (Apache 2). Esquema XML. Herramientas libres de gestión: IOC Editor, IOC finder.	Adopción limitada. Menor flexibilidad de integración. No soporta descripción de tácticas, técnicas y/o procedimientos de intrusión.

ESTÁNDAR	VENTAJAS	DESVENTAJAS
CybOx	Proporciona amplia lista de objetos detallados. Integración con STIX. Independiente de fabricante.	Alta granularidad que dificulta implementaciones.
STIX	Legibilidad. Representación global de objetos con grafos, incluyendo relaciones. Integración de esquema CybOx. Flexibilidad para integrar otros esquemas.	Adopción relativamente reciente.

Tabla 4.2. Múltiples estándares para intercambio de información.

Aunque no se pueda decir que exista un único procedimiento universalmente aceptado en *Information Sharing*, sí podemos concluir que los métodos descritos en este artículo se perfilan como los más utilizados. Estos estándares cuentan cada uno con sus pros y sus contras, siendo en última instancia una decisión del emisor de la información escoger entre uno u otro.

Respecto a los repositorios para la compartición, cabe destacar *CIF* y MISP. Mediante *CIF* (*Collective Intelligence Framework*) se detalla el marco para el almacenamiento de la inteligencia en un repositorio central, donde la información es guardada según IODEF.

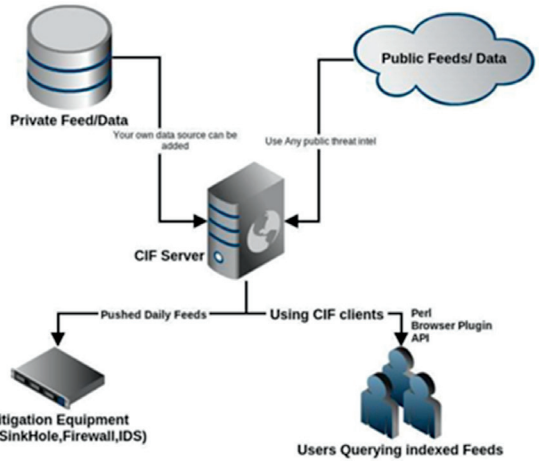

Figura 4.15. «Detect, SHARE, Protect Solutions for Improving Threat Data Exchange among CERTs». ENISA. Octubre de 2013.

OTX

Open Threat Exchange es la apuesta lanzada por ALIEN VAULT; fabricante conocido por sus sistemas USM (Gestión Unificada de la Seguridad) y desarrolladores originales del proyecto OpenSource OSSIM. OTX es una plataforma para el intercambio en la nube, que funciona con su propio formato + OpenIOC + STIX, que facilita la compartición de amenazas. La plataforma describe tanto el intercambio de información, el metalenguaje y el API para su conexión. La principal ventaja es la posibilidad de suscripción a los distintos *PULSES* (IOC de una fuente/s) así como la creación de nuevos, asi como una lista de IP con su reputación. Gracias a toda la información almacenada, no solo se define el intercambio sino que la existencia de un repositorio alimentado en tiempo real por ALIENVAULT y diversos aliados (empresas y particulares) otorga un valor diferencial a este sistema.

El repositorio soporta incluir información en formato OPEN IOC o ficheros STIX, por lo que representa en la actualidad una fuente de indicadores de compromiso ampliamente utilizada.

MISP

MISP es una plataforma de intercambio de amenazas basado en un *software* libre de código abierto y orientado a facilitar la compartición de información de indicadores de compromiso (IOC) y de amenazas cibernéticas. MISP puede almacenar IOC de una manera estructurada, simplificando el proceso

Figura 4.16. Formas de utilización de MISP.

de correlación, las exportaciones hacia sondas de detección de intrusiones (IDS) o sistemas de correlación de eventos de seguridad (SIEM), ya sea en formatos STIX o en OpenIOC.

Inicialmente fue construido para ser utilizado en el ámbito del NATO Computer Incident Response Capability (*NIRC*), MISP permite compartir características técnicas de las amenazas dentro de una comunidad de confianza, sin tener que incluir información sobre el contexto del incidente. Esto facilita la preservación de la confidencialidad de información sensible relacionada con un incidente de ciberseguridad, como el activo afectado y el grado de impacto o de afectación.

MISP combina un repositorio de búsqueda de información multidireccional con mecanismos para su distribución dentro de la comunidad. También proporciona automatización para la importación y exportación de datos de forma automática y una interfaz para conectar con otros entornos y sistemas.

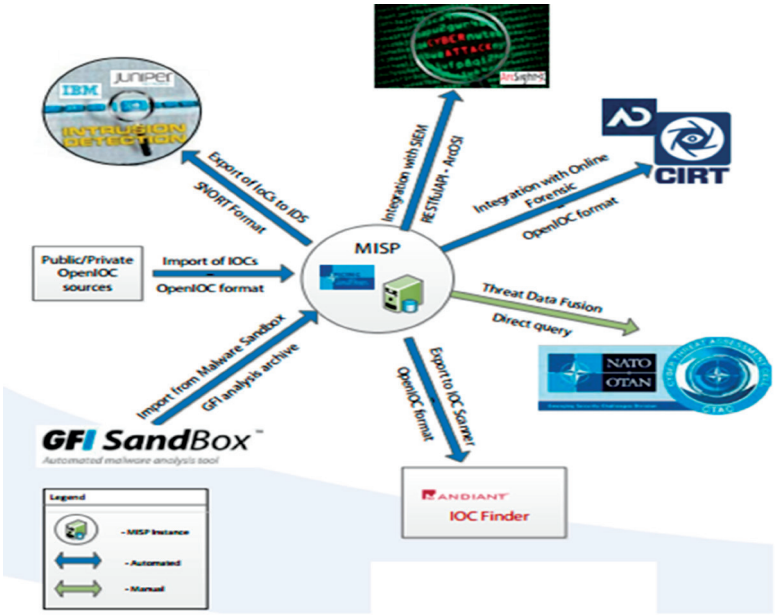

Figura 4.17. Uso de MISP en NCIRC.

Otra ventaja de la plataforma es la posibilidad de establecer una arquitectura federada entre comunidades. Esto permite que el intercambio de información entre comunidades que representan, por ejemplo, países, se haga de forma segura y controlada en base a los criterios que se hayan establecido dentro de esa comunidad, y facilita la configuración de plataformas «de segundo nivel» que representan necesidades específicas de los distintos ámbitos en los que se pueda estructurar esa comunidad, por ejemplo, los distintos sectores productivos: energía, transporte, finanzas, etcétera. De esta

manera, la información es relevante en cada nivel y no se comparte fuera de ese colectivo de confianza de forma no controlada.

Análisis de requisitos de los actores del ecosistema público-privado para el intercambio de amenazas

En la actualidad existen numerosos ecosistemas para el intercambio de información que pueden dividirse en según múltiples atributos:

- Alcance: nacionales, regionales y mundiales.
- Tipología: privados, Administraciones públicas o acceso universal.
- Acceso: gratuitos, membresía o pago.
- Ámbito: B2B (empresas), B2C (particulares), G2G (Estados) o G2C (ciudadanos).
- Sectores: industriales, operadores críticos, banca, universales, etcétera.

Empresas, Administraciones y usuarios/ciudadanos

Una vez vistos los métodos de descripción de las posibles amenazas, es importante reseñar cómo se genera la inteligencia por los diversos actores así como, cómo se produce el consumo de la misma. Normalmente la inteligencia es generada desde:

- Administraciones: locales (ejemplo: CESICAT o GVA *CERT*), nacionales (CCN o INCIBE) o regionales (ENISA, OAS o USCERT)
- De empresas: normalmente con ámbito global (Telefonica, Karspersky, Mandiant-FEYE, ThreatConnect, ThreatStream, Symantec, McAfee o Digital Shadows entre otras).
- Organizaciones: principalmente englobadas en los distintos grupos de FS-ISAC (SOLTRA) o bajo organizaciones sin ánimo de lucro tipo FIRST-TERENA, APWG o ISMS.
- Particulares: con el auge de las tecnologías sociales, cada vez se comparte más información en *blogs*, Twitter o simplemente repositorios creados por personas con el ánimo de compartir información. El rol que normalmente tienen los particulares/ciudadanos en la compartición de información de este tipo, es el de receptores de la inteligencia. Organismos como INCIBE dedican gran parte de sus programas a la concienciación y sensibilización de los ciudadanos en materias de ciberseguridad.

ISAC vs *ISAO*

El ecosistema formado por los centros de análisis y compartición de información (*Intelligence Sharing and Analysis Centers*, *ISAC*) y su unión con los diversos actores forma uno de los mecanismos más ágiles para la distribución

de la información. El Gobierno americano ha fomentado la creación de estos organismos para la compartición de información con especial énfasis en la protección de operadores críticos.

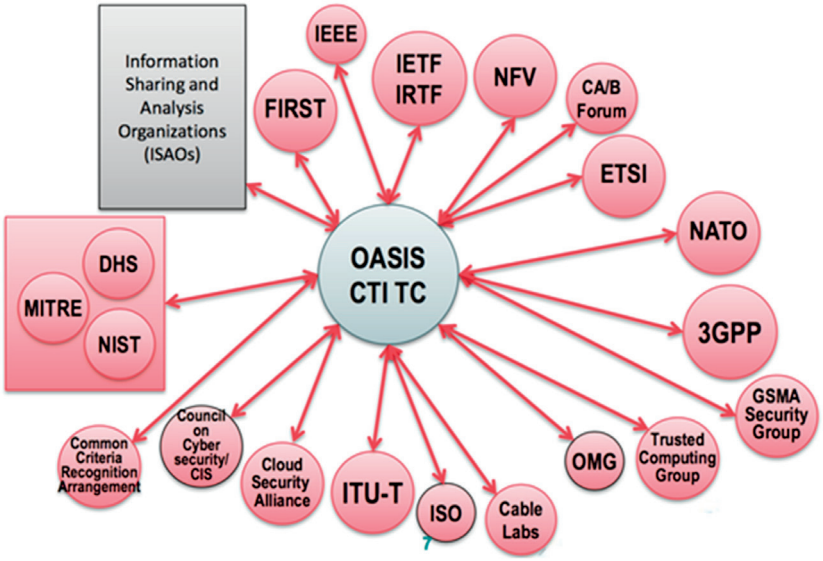

Figura 4.18. Fuente www.oasis-open.org.

En España cabe recalcar que la protección de las infraestructuras críticas está bajo el CNPIC, el cual gestiona alertas y compartición del conocimiento en dicho ámbito.

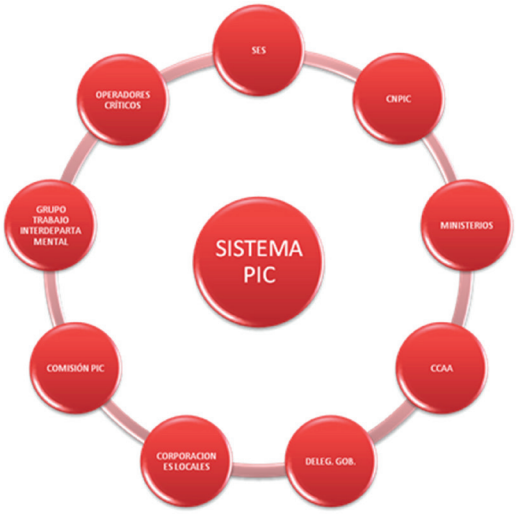

Figura 4.19. Sistema PIC.

Enisa define en Europa los operadores críticos como: energía, agua, alimentación, salud, finanzas, orden publico, transporte, espacio, nuclear-química y tecnología-comunicaciones.

Fabricantes y proveedores de servicios de inteligencia

En la actualidad existen cientos de empresas que proveen servicios de inteligencia. Dentro de la cadena de valor existen principalmente cuatro enfoques:

Generadores de información, inteligencia estándar y accionable. Asimismo, se produce desde información básica, pasando por inteligencia de fuentes abiertas OSINT hasta la que requiere de intervención manual HUMINT.

Herramientas para la gestión de la inteligencia y gestión de incidentes: aparecen desde simples plataformas para la gestión de la información hasta mega *suites* que gestionan todo el ciclo de la inteligencia así como su aplicación en la organización y el enriquecimiento constante de la información.

Servicios de acción sobre la inteligencia: normalmente prestados por MSSPs o compañías especialistas en seguridad que, tras la recolección de la inteligencia, son especialistas en aplicarla sobre elementos de red (por ejemplo, para evitar un ataque de denegación de servicio) o sobre un incidente existente (por ejemplo, realizar un análisis forense completo y poder atribuir las causas, origen y atribución completa).

Fabricantes de tecnología: permiten el uso automático o semiautomático de la inteligencia para mejorar la prevención y detección en materia de seguridad.

*Organismos oficiales (*CERT*, CSIRT y agencias públicas)*

La compartición de información en Europa ha evolucionado en los últimos años de manera drástica. En base a los informes de 2013, donde básicamente el email (seguro o estándar) era la principal fuente de intercambio no estructurado, en la actualidad numerosos *CERT*/CSIRT intercambian información mediante STIX/TAXII.

Los datos recolectados provienen de un estudio de ENISA[13] sobre dieciocho *CERT* gubernamentales, cinco universitarios y cuatro de empresas.

En el informe realizado se destacan los puntos que inhiben el intercambio, con su clasificación en: legal, técnica, procedimientos, confianza o interés.

[13] *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches*. ENISA. Diciembre de 2015.

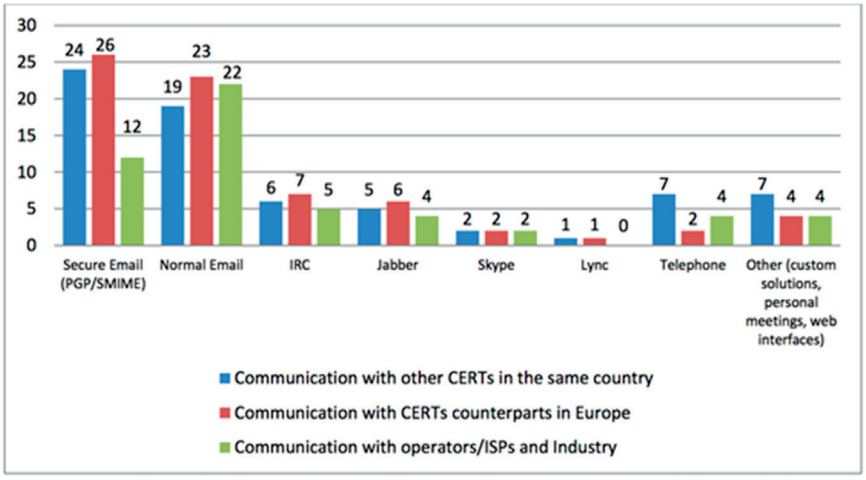

Figura 4.20.

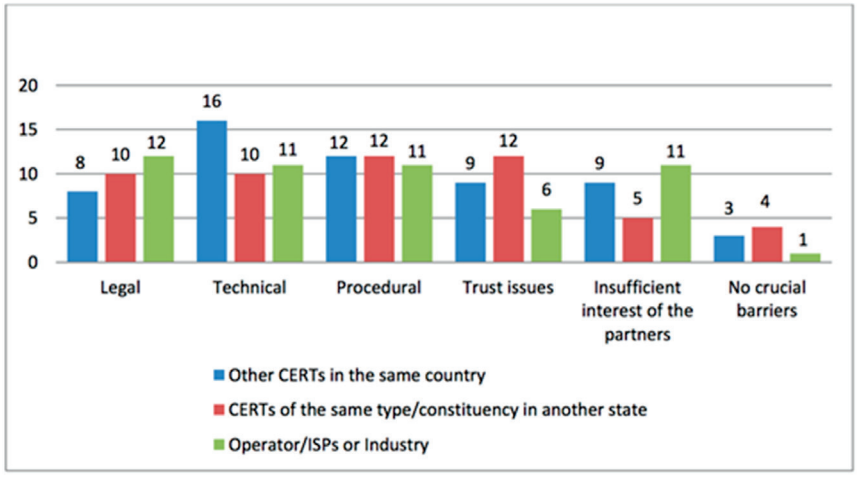

Figura 4.21.

El caso norteamericano: Cyber Threat Intelligence Integration Center (CTIIC)

CTIIC[14] nace en febrero del año 2015 a través de un Memorando Presidencial[15] con el objetivo de proporcionar análisis de inteligencia de todas las fuentes integradas relacionadas con las amenazas informáticas extranjeras e incidentes cibernéticos que afectan a los intereses nacionales, apoyando

[14] www.dni.gov/index.php/about/organization/ctiic-who-we-are

[15] Presidential Memorandum-Establishment of the Cyber Threat Intelligence Integration Center.

a los centros responsables de la seguridad cibernética y de la defensa de la red del Gobierno de Estados Unidos y facilitar y apoyar los esfuerzos para contrarrestar las amenazas cibernéticas.

El *CTIIC* no es un centro operativo y, por tanto, no gestiona incidentes pero apoya a distintos organismos federales con sus funciones operativas, proporcionando a estas entidades, además de a otros departamentos y organismos, la inteligencia necesaria para llevar a cabo sus misiones de seguridad cibernética.

Estructura organizativa

El *CTIIC* apoya al Consejo Nacional de Seguridad en el cumplimiento de sus responsabilidades de seguridad cibernética y tienen una estrecha colaboración con todos los departamentos y organismos que realizan funciones de seguridad cibernética en el Gobierno.

Figura 4.22. Escudo oficial del CTIIC (Fuente DNI).

Responsabilidades del Centro

Proporciona análisis de todas las fuentes de la inteligencia integrada en relación con amenazas informáticas extranjeras o relacionadas con incidentes cibernéticos que afectan a los intereses nacionales de Estados Unidos.

Apoya al Centro de Integración Nacional de Seguridad Cibernética y Comunicaciones, al Mando Conjunto de Ciberdefensa, a la Fuerza Conjunta de Investigación Cibernética y a otras entidades gubernamentales de Estados Unidos correspondientes a proporcionar acceso a la inteligencia necesaria para llevar a cabo sus respectivas misiones.

Supervisa el desarrollo y aplicación de las capacidades de inteligencia compartida (incluidos los sistemas, programas, políticas y estándares) para mejorar el conocimiento de la situación de la inteligencia relacionada con las

amenazas informáticas extranjera o relacionados con incidentes cibernéticos que afectan a los intereses nacionales.

Se asegura que los indicadores de la actividad maliciosa y los informes de amenazas se puedan distribuir a las agencia de los Estados y a las entidades del sector privado.

Facilita y apoya los esfuerzos para desarrollar e implementar planes para contrarrestar amenazas informáticas contra los intereses nacionales de Estados Unidos.

Conclusiones y Recomendaciones

Como se ha descrito en el capítulo, el proceso de recolección de datos y su conversión en información para poder llegar a generar inteligencia sobre la misma no es un proceso trivial. Asimismo, la capacidad de «accionar» dicha inteligencia es diversa, dependiendo de la calidad de la misma, su naturaleza o capacidad del receptor. Los avances en estandarización en los últimos cinco años han sido espectaculares, por lo que desde OASIS a buen seguro se generara un estándar que será usado ampliamente por la industria *de facto*.

Cabe destacar la necesidad de mejorar los incentivos para la compartición, dado que la complejidad existente en el ecosistema actual (origen de la información, receptores, privacidad, confidencialidad o la propia integridad) genera una complejidad que inhibe la distribución de información por problemas políticos, económicos, socioculturales, técnicos o legales.

Las distintas administraciones locales, nacionales o regionales disponen de equipos para fomentar la creación y distribución de inteligencia en ciberamenazas (ejemplos desde los *CERT* locales de administraciones públicas, *CERT* de Seguridad e Industria, el CCN-*CERT* o el *CERT* de las Fuerzas Armadas (ESPCERTDEF) y organismos europeos como EUROPOL EC3 o ENISA). Asimismo, los distintos Ejércitos cuentan en la mayoría de los países *NATO* con un quinto dominio (CyberSpace) donde se genera información y se coopera para la mitigación de las distintas ciberamenazas existentes. En el caso de España, esas funciones son realizadas por el Mando Conjunto de Ciberdefensa, responsable del planeamiento y la ejecución de las acciones relativas a la ciberdefensa en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa y otras que pudiera tener encomendadas.

Por otro lado en el sector privado se consumen ampliamente las informaciones generadas para operadores críticos así como la inteligencia generada por las múltiples empresas existentes, si bien cada vez es más frecuente el uso de la información desde los líderes del mercado y organizaciones FSISAC.

En materia de capacidades, en la actualidad, tanto Estados Unidos como China e Israel llevan la delantera en los modelos públicos, por todo ello desde

los distintos organismos y empresas europeas englobados bajo ECSO, se ha priorizado la ciberseguridad en el horizonte 2016-2019 con 450 millones de euros en ayudas, lo cual a buen seguro ayudará a la creación de datos de ciberinteligencia de calidad y su compartición óptima.

Bibliografía de consulta

INCIBE (2016). León, julio de 2016. www.incibe.es

Bitácora: https://www.certsi.es/alerta-temprana/bitacora-ciberseguridad/threatexchange

blog de ciberseguridad:

§ https://www.certsi.es/blog/unidos-las-ciberamenazas-information-sharing

Servicio ICARO:

§ https://www.certsi.es/servicios-operadores/icaro

Plataforma MISP.

http://www.misp-project.org/

https://circl.lu/services/misp-malware-information-sharing-platform/

HiTrust. 2016.

Intercambio de información sobre amenazas:

https://blog.hitrustalliance.net/threat-information-sharing-an-increasingly-effective-weapon-for-fighting-ransomware-and-other-cybercrime/

ENISA, European Union Agency for Network and Information Security

(2014) Detect, SHARE, Protect. *Solutions for Improving Threat Data Exchange among*.

(2015) *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches*.

OTAN, Organización del Atlántico Norte.

https://www.ncia.nato.int/Documents/Agency%20publications/Malware%20Information%20Sharing%20Platform%20%28MISP%29.pdf

Libros y todo J: http://dl.acm.org/citation.cfm?id=2994544

The White House (2015). *Fact Sheet Cyber Threat Intelligence Integration Center*.

https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center

Office of the Director of National Intelligence (2015).

https://www.dni.gov/index.php/about/organization/ctiic-who-we-are

https://www.dni.gov/index.php/about/organization/ctiic-what-we-do