

CSIRTs: Al pie del cañón



Los equipos de respuesta a incidentes de seguridad nacieron tras el considerado primer gran ciberataque mundial, provocado por el 'virus Morris', en 1988. Desde entonces, el concepto, identificado bajo las siglas CERT o CSIRT, ha evolucionado hasta alcanzar una razonable madurez con más de 500 equipos en regiones como Europa, más del 10% de ellos españoles. Sus grandes retos son, sin duda, compartir información, sumar sinergias y ser capaces de ofrecer una respuesta eficaz y rápida a cualquier amenaza que ponga en riesgo la información más crítica o la interrupción de servicios y negocio. SIC dedica este especial a analizar los éxitos, 'fracasos' y retos de lo que está llamado a ser una 'commodity' de la ciberseguridad en cualquier país o empresa para alcanzar un alto nivel de resiliencia.

SUMARIO

- Los equipos de respuesta a incidentes cobran protagonismo como 'última bala' para anticiparse a todo tipo de ciberataques y garantizar la resiliencia.
- De la Edad de Piedra a la Moderna: cómo han cambiado los CERTs / CSIRTs y por qué.
- Qué perfiles profesionales se piden.
- Cómo crear un CSIRT paso a paso.
- Canción triste de Hill Street... ¡Tengan cuidado ahí fuera!, por ALBERTO PARTIDA.
- El futuro de los CERTs / CSIRTs pasa por reglas que generen más confianza y mayores capacidades.
- Equipos de respuesta a incidentes españoles y su situación en foros nacional e internacionales.
- Así piensan: Organismos Internacionales, CERTs de referencia y CSIRTs españoles.



Los equipos de respuesta a incidentes cobran protagonismo como 'última bala' para anticiparse a todo tipo de ciberataques y garantizar la resiliencia

Para garantizar la seguridad del espacio aéreo, el Ejército del Aire tiene en marcha, 365 días al año y 24 horas al día, el denominado protocolo 'Alerta Scramble'. Gracias a él, en menos de 15 minutos despegar para interceptar en vuelo a cualquier avión no identificado. Una operación que, en España y coordinada con la OTAN, se pone en marcha desde el bunker del Centro de Operaciones Aéreas Combinadas (CAOC), en Torrejón de Ardoz (Madrid). En cierto modo su trabajo se parece mucho al que tienen los equipos de respuesta a incidentes cibernéticos, los denominados CERTs / CSIRTs, que permiten hacer frente a cualquier ataque y estar preparados para repeler el siguiente gracias a sus 'lecciones aprendidas'. España es el país de la Unión Europea con más equipos registrados en Enisa y el tercero del mundo en el foro FIRST.

| ANA ADEVA y JOSÉ MANUEL VERA (Equipo SIC) |

El 2 de noviembre de 1988, a las ocho y media de la mañana, un recién diplomado de **Harvard, Robert Tappan Morris**, de 23 años, sentado al frente de su ordenador en el **Instituto de Tecnología de Massachusetts (MIT)**, liberó en Internet el código del llamado 'gusano Morris' sin ser consciente de hasta qué punto estaba haciendo historia.

En sólo 24 horas, su software malicioso se 'reprodujo' infectando 6.000 de los 60.000 sistemas informáticos conectados entre universidades en EE.UU. y, de hecho, se calcula que afectó hasta al 10% de los sistemas conectados del momento. Viendo el daño causado, de forma anónima publicó unas instrucciones para eliminarlo y prevenir de su infección, pero ya era tarde para evitar uno de los mayores caos informáticos de la historia. Curiosamente, sólo tenía la intención de demostrar que la seguridad de la Red era extremadamente débil. Tras su 'ataque' comenzaron a llegar al mercado los primeros antivirus y, también, surgió uno de los conceptos que más de 30 años después continúa evolucionando hacia su madurez: el de los 'Equipos de Respuesta ante Emergencias Informáticas' (CERT) también denominados como 'Equipos de Respuesta a Incidentes de Seguridad Informática' (CSIRT). Y es que, una de las grandes lecciones aprendidas en aquel suceso resultaba evidente; a saber: sin la comunicación y coordinación de organismos y empresas,



un ataque global de este tipo era imposible de parar. Algo que volvió a ser patente, en 1989, con el gusano WANK, de origen *hacktivista* y, ya en nuestros días, con incidentes como WannaCry o NotPetya, en 2017.



Barbara Fraser y Ed DeHart, parte del CERT CC de SEI a principios de la década de 1990.

Para evitar futuras situaciones de este tipo, la **Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA)**, precursora de Internet, financió un programa de la **Universidad Carnegie Mellon (CMU)** para poner en marcha en su **Instituto de Ingeniería de Software (SEI)** el primer **Centro de Coordinación del Equipo de Respuesta a Emergencias Informáticas (CERT/CC)**, que hoy continúa siendo una de las referencias mundiales junto al **US CERT**, dependiente de la **Agencia de Seguridad Ciberseguridad e Infraestructura (CISA)**, que

también colaboran con el **ICS-CERT**, centrado en sistemas de control industrial de infraestructuras críticas. Su objetivo era y es gestionar las emergencias de ciberseguridad y contar con capacidades de respuesta ante ellas, coordinando el esfuerzo de empresas y organismos.

Así, entre sus principales labores está, tras detectarse un incidente, su control y minimización de daños, preservación de las evidencias e investigación de lo que ha ocurrido y, por supuesto, coordinar la respuesta para una rápida recuperación.

Son sólo dos de los más de 700 equipos que hay en el mundo, públicos y privados, que también buscan anticiparse a posibles incidentes compartiendo vulnerabilidades o indicadores de compromiso (IoC) con otros CERTs / CSIRTs integrados en foros y redes organizadas en Europa, Asia, América...



¿Es lo mismo un SOC que un CERT y un CSIRT?

Desde que comenzara el CERT-CC, hace casi 32 años, los equipos de respuesta han sido denominados de diferentes formas, aunque cada uno tenga matices que le haga diferente, ya que cada equipo tiene unas capacidades, objetivos y metodologías concretas –técnicas, forenses, legales, de comunicación, etc.–, según la organización y sus necesidades.

Así, mientras que CERT es una marca registrada por la universidad estadounidense **Carnegie Mellon (CMU)**, en 1997, por la que hay que pagar tras demostrar que se cumplen unos requisitos, CSIRT es un concepto más amplio que cualquiera puede usar.

Por establecer una definición formal, dicha universidad, en un documento de 2007, explicaba que “un equipo de respuesta a incidentes de seguridad informática (CSIRT) es una entidad organizativa concreta (es decir, uno o más miembros del personal) a la que se le asigna la responsabilidad de coordinar y respaldar la respuesta a un evento o incidente de seguridad informática”, frente a lo que considera un CERT que denomina como un “... socio con el gobierno, la industria, las fuerzas del orden y el mundo académico para mejorar la seguridad y la resistencia de los sistemas y redes informáticos...”, recordando que un CERT estudia “...problemas que tienen implicaciones de ciberseguridad generalizadas y desarrollan métodos y herramientas avanzados”. Así, la universidad considera que mientras un CERT recopila y difunde información de seguridad, generalmente para el beneficio de un país o industria, un CSIRT responde a los incidentes en nombre de un país u organización. En paralelo, un Centro de Operaciones de Ciberseguridad (SOC) permite a un país u organización monitorizar y defender su red, servidores, aplicaciones y dispositivos.

Lo cierto es que, a pesar de los esfuerzos de la CMU por diferenciar CERT de CSIRT a día de hoy, ambos conceptos se usan indistintamente para identificar a este tipo de equipos, siendo el más empleado en Europa el de CSIRT aunque especialistas como **Tim Matthews**, CMO de **Exabeam**, consideran que sí hay diferencias importantes en su conceptualización (ver **Figura 1**).

Eso sí, a pesar de que CSIRT no es una marca comercial, para ser aceptado como tal lo habitual es formar parte de uno de los foros que busca impulsar este tipo de capacidades: **FIRST**, el más conocido a nivel mundial, y, en Europa, el ‘**TF-CSIRT Trus-**

ted Introducer’ o figurar en el catálogo de la **Agencia de Ciberseguridad Europea (Enisa)** como tal, entre otros.

Llega la especialización

Lo cierto es que cada vez más países, organismos y empresas apuestan por contar con esta clase de equipos por su capacidad para ofrecer ciberresiliencia, uno de los conceptos más impulsados por las estrategias nacionales de ciberseguridad, también la española, como parte integrada y activa de la arquitect-

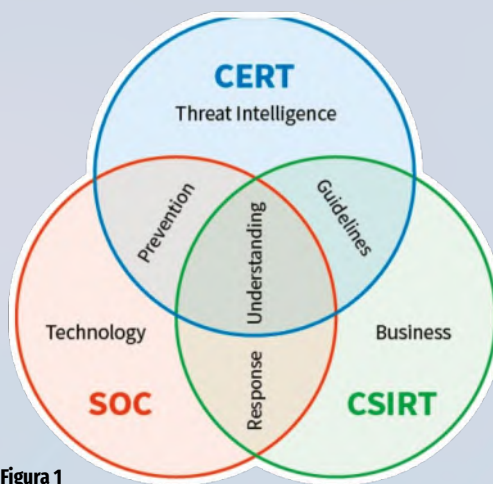


Figura 1

pecialización está llegando a este concepto para dar respuesta a amenazas cada vez más complejas y recurrentes.

Por eso, cada vez hay más países que disponen, dentro de su ‘ciberestructura’, de un CSIRT nacional como punto de referencia para participar en respuestas a incidentes internacionales y como contacto para compartir información. De hecho, los CSIRTS cada vez son más citados por entidades como las **Naciones Unidas (ONU)** o la **Organización de los Estados Americanos (OEA)** como una buena evidencia de madurez en ciberseguridad. También ven en ellos un instrumento óptimo para hacer del ciberespacio un lugar más seguro. La razón es que, mientras muchos países mantienen tensas relaciones en lo político, gracias a la creación de foros de CSIRTS la información más crítica, de vulnerabilidades y amenazas, sí se comparte para reducir su impacto. Un buen ejemplo es el foro **APCERT**, del que forman parte 13 países de Asia, entre ellos Japón, Corea y China.

De esta forma, lo que en sus comienzos fue una comunidad pequeña, ha ido creciendo hasta llegar a superar los 700 equipos CERTs / CSIRTS repartidos por todo el mundo, un número que continúa creciendo en los cinco continentes para hacer frente a ataques como el que sufrió en 2015 el **Bundestag** alemán, que se apresuró a repeler el peor ciberataque de su historia y a cuyos presuntos responsables sancionó la UE este octubre. Estos equipos también han dado pie a una extensa red de organizaciones nacionales o regionales dentro de foros institucionales organizados más formalmente, como el español **CSIRT.es**. Por eso, muchos profesionales de CSIRTS enfatizan la importancia de la confianza como condición previa para una cooperación con éxito, que a su vez determina una respuesta eficaz a los incidentes.

Qué está pasando en Europa

En el Viejo Continente, los primeros CERTs/CSIRTS surgieron a principios de la década de los 90 dentro de las redes nacionales de investigación y educación (NREN), sentando las bases de los que son actualmente, impulsados por Enisa. Este trabajo fue apoyado de forma especial por la actual Directiva Europea de Seguridad en Redes (NIS), que dedica, entre otros, su Artículo 12 a la necesidad de establecer una red europea de CSIRTS “para contribuir a desarrollar la confianza entre los estados miembros y promover una cooperación operativa, rápida y eficaz”, añadiendo en su punto 2, que “la red de CSIRTS estará

tura cibernética y el plan de ciberprotección de cualquier organización. Incluso, apostando por su especialización, como han hecho multinacionales como **Cisco**, que cuenta con dos entidades separadas: una para ataques exclusivamente cibernéticos (CSIRT) y otra para incidentes en productos (PSIRT). La es-

Diferentes nombres un concepto similar...

No todos son exactamente iguales, pero sí representan el mismo enfoque. Dado que la marca ‘CERT’ estaba registrada por la Universidad Carnegie Mellon, organismos y empresas han usado más de una decena de denominaciones para identificar a estos equipos:

- CSIRT.** Equipo de respuesta a incidentes de seguridad informática.
- CIRC.** Capacidad de Respuesta a Incidentes Informáticos.
- CSIRC.** Centro o capacidad de respuesta a incidentes de seguridad informática.
- CIRT.** Equipo de respuesta a incidentes informáticos.
- IRC.** Centro de respuesta a incidentes o capacidad de respuesta a incidentes.
- IHT.** Equipo de manejo de incidentes.
- IRT.** Equipo de Respuesta a Incidentes.
- SERT.** Equipo de Respuesta a Emergencias de Seguridad.
- SIRT.** Equipo de respuesta a incidentes de seguridad.



compuesta por representantes de los CSIRTs de los Estados miembros y del CERT-EU". Además, "la Comisión participará en la red de CSIRTs como observadora y Enisa se encargará de la secretaría y de apoyar activamente la cooperación entre estos equipos de respuesta a incidentes".

Prueba de su continua evolución, a principios de octubre, precisamente Enisa presentó la **Cyber Crisis Liaison Organisation Network (CyCLONE)**, destinada a facilitar la cooperación en caso de ciberincidentes disruptivos. "Las ciber crisis no tienen fronteras. La Agencia de la UE para la Ciberseguridad se compromete a apoyar a la Unión en su respuesta a los ciberincidentes. Es importante que las agencias nacionales de ciberseguridad se unan para coordinar la toma de decisiones a todos los niveles", destacó al respecto el Director Ejecutivo de ENISA, **Juhan Lepassaar**.

¿Y en España?

A pesar de que este tipo de equipos siempre han sido muy activos, tanto por parte de organismos públicos como de empresas, en 2018, "la necesidad de ofrecer una respuesta coordinada y efectiva ante ataques globales como el WannaCry" impulsó a las principales entidades expertas en ciberseguridad en España a relanzar el grupo **CSIRT.es**, el foro en torno al que están muchos de los CERTs/CISRTs de referencia y que, hasta este momento, cuenta con 45 integrantes.

Además, este concepto también cobró una especial relevancia en el **Real Decreto-Ley 12/2018** con el que España transpuso la NIS. De hecho, en él se delimita el ámbito funcional de actuación de los CSIRTs de referencia previstos en ella, ya que considera que "son la puerta de entrada de las notificaciones de incidentes, lo que permitirá organizar rápidamente la respuesta a ellos...".

Esto no ha hecho más que empezar

De cualquier forma, con la popularización del IoT, la interconectividad que ofrecerá 5G, los edificios y ciudades inteligentes, los automóviles conectados y todo tipo de dispositivos intercomunicándose en todo tipo de sectores, los incidentes en el mundo digital, esta década, tendrán un efecto mucho mayor en el mundo físico, ya que ahora existen riesgos, amenazas y vulnerabilidades en un espectro ciberfísico bidireccional. De hecho, la firma analista **Gartner** predice que el 75% de los directores ejecutivos serán responsables de incidentes ciberfísicos (CPS), por lo que su apuesta por contar con un CSIRT es estratégica por su capacidad para 'apagar el fuego' lo antes posible y evitar cualquier repercusión de cumplimiento y/o económica. ■

FOROS INTERNACIONALES DE CERT/CSIRT

– Forum of Incident Response and Security Teams (FIRST)



Es la principal asociación mundial de CSIRTs. Fundado en 1990, su objetivo es promover la cooperación y coordinación en la prevención de incidentes, así como compartir información entre sus miembros y la Comunidad en su conjunto. Actualmente, cuenta con más de 540 equipos de 98 países, 36 de ellos en España.

www.first.org

– La División CERT



Fue la referencia hace 30 años. Integrada en el Instituto de Ingeniería del Software de la Universidad Carnegie Mellon se define como "un grupo diverso de investigadores, ingenieros de software, analistas de seguridad y especialistas en inteligencia digital que trabajan juntos para investigar las vulnerabilidades de seguridad en productos de software, contribuir a cambios a largo plazo en los sistemas en red y desarrollar información y capacitación de vanguardia para mejorar la práctica de la ciberseguridad". De él forman parte todas las entidades, públicas y privadas, que han solicitado esta denominación y pagado por ello, sumando en la actualidad más de 340 equipos.

www.CERT.org

– European Government CERT (EGC Group)



Se trata del 'Grupo informal de Equipos de Respuesta Gubernamentales' europeos, que busca desarrollar una "cooperación eficaz en materia de respuesta a incidentes entre sus miembros". Creado en 2001, entre sus miembros están 12 CERTs nacionales (el de Austria, Bélgica, Dinamarca, Finlandia, Francia, Alemania, Holanda, Reino Unido), también el de España, el CCN CERT.

www.egc-group.org

– Trusted Introducer



TF-CSIRT
Trusted Introducer

Es el grupo de trabajo creado por la Asociación Transeuropea de Investigación y Educación de Redes (TERENA), que impulsa la colaboración entre los CSIRTs europeos ofreciendo un punto de encuentro para "intercambiar experiencias y conocimientos en un entorno de confianza". Cuenta con más de 400 equipos (entre certificados, acreditados, listados y candidatos) que participan en él, 30 de ellos españoles. Eso sí, **Enisa** cuenta con un registro de CSIRTs y en él se superan los 520 equipos, aunque no todos están certificados por una organización oficial como tal.

www.trusted-introducer.org

– NATO Computer Incident Response Capability (NCIRC)



Se trata del CSIRT de referencia de los países que son miembros de la OTAN, por lo que comparten información con él y la analizan acorde a los objetivos de la Alianza.

www.nato.int

– AP-CERT



Es el principal foro de CSIRTs de Asia-Pacífico, creado para mantener una "red de contactos de confianza de expertos en seguridad informática en aras de mejorar la conciencia y la competencia de la región en relación con los incidentes de seguridad informática". Cuenta con más de 40 miembros, incluidos Japón, Singapur, Australia, China, India, etc.

www.apcert.org



Con los años se han incrementado sus capacidades contando, incluso, análisis forense, y especializándose por sectores para ganar en eficiencia

De la Edad de Piedra a la Moderna: cómo han cambiado los CERTs / CSIRTs y por qué

“Por definición, un CSIRT debe realizar, como mínimo, actividades de manejo de incidentes”, destacaba la experta de la CISA estadounidense, **Georgia Killcrece**, resaltando que ello supone analizar y resolver los eventos e incidentes que reportan los usuarios finales o que se observan a través de la monitorización proactiva de la red y el sistema. Y dado que los CSIRTs “se pueden crear para países o economías, gobiernos, organizaciones comerciales, instituciones educativas e, incluso, entidades sin ánimo de lucro, el objetivo de un CSIRT es minimizar y controlar el daño resultante de los incidentes, proporcionar una guía eficaz para las actividades de respuesta y recuperación, y trabajar para evitar que ocurran incidentes futuros”, resaltaba **Robin Ruefle**, de la División CERT de la CMU, en 2007.

Y es que los servicios que prestan este tipo de equipos se pueden dividir en tres áreas: por un lado, los preventivos, por ejemplo, buscando vulnerabilidades, concienciando a los empleados, notificando a la alta dirección de nuevos ciberriesgos, compartiendo amenazas o posibles incidentes con los empleados; y, por otro, los reactivos, que suponen la gestión de un incidente, incluyendo desde su

análisis, hasta las acciones de respuesta, soporte y coordinación. Algunos especialistas también consideran, un tercer ámbito: que parte del trabajo de los CSIRTs es ayudar a gestionar la seguridad de la organización realizando evaluaciones de riesgo, participando en los planes de continuidad de negocio, de recuperación ante desastres, así como participando en los

programas de concienciación.

La razón para este trabajo multidisciplinar es que, con el paso de los años, las organizaciones han ganado en complejidad y el área de trabajo de los CSIRTs también ha crecido como forma de mejorar la resiliencia operacional de cualquier entidad contando con un plan que garantice, incluso en las crisis más graves, que los

QUÉ SERVICIOS BÁSICOS OFRECEN LOS CERTs / CSIRTs

Servicios Reactivos	Servicios Proactivos	Servicios de Gestión de la Calidad de la Seguridad
<ul style="list-style-type: none"> Alertas y advertencias Tratamiento de incidentes Análisis de incidentes Respuesta a incidentes <i>in situ</i> Apoyo a la respuesta a incidentes Coordinación de la respuesta a incidentes Tratamiento de vulnerabilidades Análisis de vulnerabilidades Respuesta a vulnerabilidades Coordinación de la respuesta a la vulnerabilidad Asistencia remota a vulnerabilidades e incidentes 	<ul style="list-style-type: none"> Comunicados y anuncios Observatorio de tecnología Evaluaciones o auditorías de la seguridad Configuración y mantenimiento de la seguridad Desarrollo de herramientas de seguridad Servicios de detección de intrusos Difusión de información relacionada con la seguridad Programas de gestión de listas de configuración segura de sistemas TIC Monitorización de redes 	<ul style="list-style-type: none"> Análisis de riesgos Continuidad del negocio y recuperación ante desastres Consultoría de seguridad Sensibilización Educación / Formación Evaluación o Certificación de productos

Figura 1

CCN-STIC-810

PROS Y CONTRAS DE EXTERNALIZAR LAS FUNCIONES DE UN CSIRT

FUNCIONES DE CSIRT QUE DEBEN TENERSE EN CUENTA	A FAVOR	EN CONTRA
Creación de plan de respuesta a incidentes	Contarás con consultores expertos en la creación de IRP.	Un plan creado por un tercero puede no estar hecho a medida ni contar con supervisión interna
Monitorización	Un proveedor de servicios de seguridad administrada (MSSP) o de detección y respuesta administradas (MDR) son útiles si se carece de personal especializado.	Puede haber un lapso de tiempo entre la detección de eventos y el comienzo de la investigación. Además, la subcontratación no eximirá a su organización de la responsabilidad legal.
Investigación	Hay empresas de informática forense expertas en lidiar con investigaciones	Puede llevar tiempo incorporar un experto forense externo y, por lo general, son costosos
Remediación	Puede encontrar más experiencia en seguridad en un tercero	Es posible que los equipos externos no tengan los derechos de acceso y el contexto para abordar adecuadamente el problema
Comunicación interna	Realmente no hay ninguna ventaja positiva en el uso de un tercero	Esta función crítica no debe ser manejada por un tercero
Relaciones públicas	Es posible que su empresa de Comunicación pueda actuar rápido y cuente con personas expertas en crisis.	Es posible que su empresa de Comunicación no esté tan familiarizada con el negocio y el riesgo en su mercado y trate información confidencial.
Legal	Su abogado externo puede haber manejado un incidente similar para otro cliente.	Por lo general, los abogados externos pueden reaccionar más lentamente que los internos.

Figura 2

Fuente: Exabeam



servicios de “misión crítica” continúen y estén protegidos los activos y datos más estratégicos y confidenciales.

Por ejemplo, el US CERT, de EE.UU., uno de los pioneros, cambió su nomenclatura inicial del CERT, sustituyendo el significado de la letra “R”, pasando del tradicional *Response* (Respuesta) a *Readiness* (Preparación). O el análisis forense, que ha sido uno de los servicios de estos equipos que aconseja tener Enisa, además de contar con especialistas y medios en la gestión de las vulnerabilidades.



Diseño a medida

Así pues, no hay un único diseño como tal para un CSIRT sino que se considera que su estructura debe estar adaptada a las necesidades de cada organización.

De esta forma, puede haber CSIRTS integrados en estructuras como los Centros de Operaciones de Ciberseguridad (SOC) o como equipo aparte. Incluso, se puede contemplar este tipo de equipos exclusivamente para hacer frente a crisis concretas con profesionales de diversos departamentos que no trabajan como tal en su día a día. También, por supuesto, se puede contar con estos equipos subcontratados como servicios con entidades que los ofrezcan: es cuestión de analizar sus pros y contras, como recomienda **Exa-beam** (ver **Figura 2**).

De cualquier forma, la clave para que trabaje con éxito es que impulse la coordinación tanto dentro de la empresa con el departamento de TI y la alta dirección como con otros equipos de CSIRTS compartiendo información que pueda ayudar a evitar incidentes o, en el peor de los casos, recuperarse rápido de uno. Y, por supuesto, poniendo en marcha mejoras que permitan no volver a sufrirlos. ■

Qué tipos de CSIRTS existen...

Aunque, según su presupuesto, medios y objetivos, las funciones y responsabilidades de los CSIRTS varían notablemente, agrupándose en diferentes tipos, según los servicios que ofrecen o los sectores en los que trabajan.

Hay varias clasificaciones. Y de entre ellas se destaca la realizada por ENISA en 2013, en la que se recogen los tipos:

- CERTs/CSIRTS Nacionales/Gubernamentales
- CERTs/CSIRTS Gubernamentales
- CERTs/CSIRTS Nacionales
- CERTs/CSIRTS Nacionales de facto
- CERTs/CSIRTS Académicos
- CERTs/CSIRTS Militares
- CERTs/CSIRTS de MSSPs
- CERTs/CSIRTS de Organizaciones no Comerciales
- CERTs/CSIRTS de empresas TIC
- CERTs/CSIRTS de Organizaciones Comerciales
- CERTs/CSIRTS del sector Financiero
- CERTs/CSIRTS del sector de la Energía
- CERTs/CSIRTS del sector Industrial

En España, a efectos oficiales y a grandes rasgos, existe hoy las siguientes entidades: el CCN-CERT (sector público en general y sistemas que manejan información clasificada); el INCIBE-CERT (ciudadanía y sector privado, instituciones afiliadas a RedIRIS, en coordinación con el CCN-CERT cuando se refiera a organismos públicos); y el ESP-DEF-CERT del Mando Conjunto del Ciberespacio del Ministerio de Defensa.

Estas entidades se constituyen como CSIRTS de referencia en el Real Decreto-ley de transposición de la directiva NIS. El Centro Nacional de Protección de Infraestructuras Críticas, CNPIC, a través de la Oficina de Coordinación en Ciberseguridad, OCC, materializa su capacidad de respuesta mediante estos CSIRTS.

(Para ampliar información se recomienda la lectura del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información). Existen también centros autonómicos, como por ejemplo Andalucía CERT, Catalonia CERT (Cataluña) o el BSCS CERT (País Vasco).

Y, por supuesto, CERTs/CSIRTS empresariales, como el Telefónica Global CSIRT, o el Santander Global CERT, entre otros.

ÁMBITOS DE ACTUACIÓN DE LOS CERT / CSIRT



Fuente: CCN



Por su especialización cada vez son más demandados y mejor pagados

Qué perfiles profesionales se piden

Los equipos que forman cada CERT/CSIRT son únicos, en el sentido de que cada uno establece la proporcionalidad de sus recursos tanto humanos como tecnológicos y operacionales, según una serie de aspectos como el tamaño de la Comunidad a la que da servicio, los niveles de dichos servicios (por ejemplo, si serán sobre un modelo 24x7), así como su nivel de madurez y planes estratégicos, entre otros factores.

Con todo, hay una serie de perfiles con los que, aunque su número y organización evolucionen con el tiempo, es necesario contar. Una de las clasificaciones más representativas es la que ofrece **Exabeam** en su 'Guía completa para la organización de un CSIRT: cómo construir un equipo de respuesta a incidentes', de 2018, y la que establece el **CCN** en su 'Guía de creación de un CERT/CSIRT'. Estos documentos destacan que todo CERT/CSIRT debe contar con un responsable de equipo, que para el CCN debe actuar como "punto de contacto con la Comunidad a la que se da servicio y el resto de CERTs con los que se vaya a colaborar". Y para Exabeam debe garantizar, además, que se reciba la atención y el presupuesto adecuados.

Los CERTs/CSIRTs también deberían de tener un gestor o equipos de gestión de incidentes e investigadores que lleven a cabo las indagaciones y análisis necesarios de un incidente de seguridad.

Dentro de los equipos más técnicos, desde el CCN se apuntan dos categorías: de primer nivel, que "necesitan un grado de conocimiento técnico básico especializado en tecnologías TIC suficiente para entender la situación notificada"; y de segundo nivel, que "son los especialistas que realmente tienen el conocimiento técnico y las habilidades de intercomunicación con otros CERTs o miembros de la comunidad".

En este sentido, cabe recordar que el marco NICE, creado por el **NIST** en su esfuerzo por establecer una taxonomía y léxico comunes de los trabajos y trabajadores del sector de la ciberseguridad, ofrece una lista con los conocimientos, tareas y capacidades de los especialistas en respuesta a incidentes.

Es posible acceder a dicha lista buscando 'Cyber Defense Incident Responder' en el apartado 'Work Roles'. Sin duda, un recurso muy útil para comprender los antecedentes, el conocimiento, las obligaciones y los requisitos laborales que piden las organizaciones de dichos perfiles.

Junto a ellos, se recomienda disponer de un experto legal, otro en comunicación y relaciones públicas y un equipo de atención al cliente. Así, Exabeam incluye, incluso, un jefe o equipo de recursos humanos en tanto que el CCN añade un equipo de formación, para que el personal del CERT/CSIRT esté adecuada-

mente instruido y actualizado sobre nuevas tecnologías, amenazas y técnicas de ataque.

Certificaciones

Las habilidades y la experiencia requeridas por un CERT/CSIRT varían según la naturaleza de su negocio y la capacidad de respuesta a incidentes que decida desarrollar internamente. No obstante, junto con la educación básica y universitaria y la experiencia, las certificaciones pueden ser de gran ayuda a la hora de acceder a un puesto de trabajo en esta área.

De acuerdo con una información publicada por el medio especializado **TechTarget**, entre ellas, están las certificaciones de seguridad general como CISSP, CISM o Security +; una certificación perteneciente a un área profesional relacionada, como Auditor de sistemas de información certificado o Hacker ético certificado; o incluso certificaciones específicas de la tecnología o del proveedor, como Cisco Certified Network Associate o Cisco Certified Internetwork Expert. Eso sí, puntualiza que, de los programas de



certificación dirigidos a la respuesta de incidentes, los dos más conocidos son, probablemente, el GCIH (**SANS Institute** Certified Incident Handler) y el ECIH (**EC-Council** Certified Incident Handler).

Buen sueldo

Sin duda, los salarios del personal que compone un CERT/CSIRT depende de muchos factores y es muy difícil de establecer una clasificación específica.

Existen algunos datos genéricos que pueden servir de guía, en su mayoría extraídos del análisis de webs de oferta y demanda de empleo. Por ejemplo, una de las más conocidas a nivel internacional como es **Indeed.com** indica que, de la búsqueda de las palabras clave 'analista de respuesta a incidentes', el promedio de los salarios se situaba en los 97.000 euros anuales, en 2019, según publicó **CyberDegrees.org**, una cifra que dista un poco de los 72.000 euros que atribuye a dichos profesionales la plataforma **CyberSeek**, apoyada por el NICE del NIST.



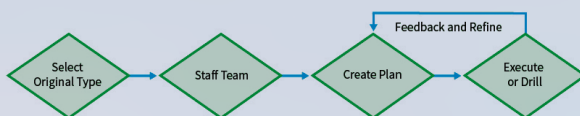
Ser reconocido como tal en foros internacionales y contar con capacidades en todo tipo de ámbitos son dos elementos imprescindibles

Cómo crear un CSIRT paso a paso

Desde 2004, la **Agencia de Ciberseguridad de la UE (Enisa)** ha generado decenas de informes con todo tipo de recomendaciones, buenas prácticas y la experiencia de especialistas en equipos de respuesta para que tanto empresas como organismos públicos pongan en marcha CSIRTs.

Entre sus puntos de partida, la Agencia recomienda comenzar por establecer unos objetivos y en función de ellos “determinar quién estará en el equipo, sus roles y responsabilidades, qué funciones

subcontratar y dónde se ubicarán los miembros de su equipo”. Además, empresas como **Exabeam** recomiendan que el equipo actúe en concordancia con un plan de respuesta a incidentes (RI) que sea fácil de asimilar y usar para evitar que “durante el pánico de una posible crisis” sea fácil de llevar a cabo por todo el personal, también el ajeno al CSIRT. Además, aconseja participar en simulacros al menos dos veces al año para conocer, de forma realista, la preparación del equipo.



PASO 1

Los principales foros, los CERTs gubernamentales y los organismos de ciberseguridad ofrecen amplia información para lograrlos

Qué estándares internacionales se deberían adoptar para el trabajo diario de los CERTs/CSIRTs

Foros como el **FIRST**, trabajan en estándares y normas para mejorar la interoperabilidad de los CSIRTs, como el marco abierto **Common Vulnerability Scoring System (CVSS)**, para comunicar las características y la gravedad de las vulnerabilidades del software; sobre el **protocolo TLP**, un estándar destinado a facilitar un mayor intercambio de información confidencial; así como en **marcos de servicios** que pueden proporcionar los CSIRTs y los PSIRTs, como el ‘*Computer Security Incident Response Team Services Framework v2.1*’, de noviembre de 2019 y el ‘*PSIRT Services Framework*’ de principios de 2020; y un **marco de Políticas de Intercambio de Información (IEP)**, destinado a automatizar el intercambio de información de seguridad y amenazas, entre otros.

Además, este grupo ha actualizado sus **‘Directrices para la coordinación y divulgación de vulnerabilidades entre múltiples partes’**, publicada en mayo, en aras de mejorar la comunicación y colaboración de vulnerabilida-

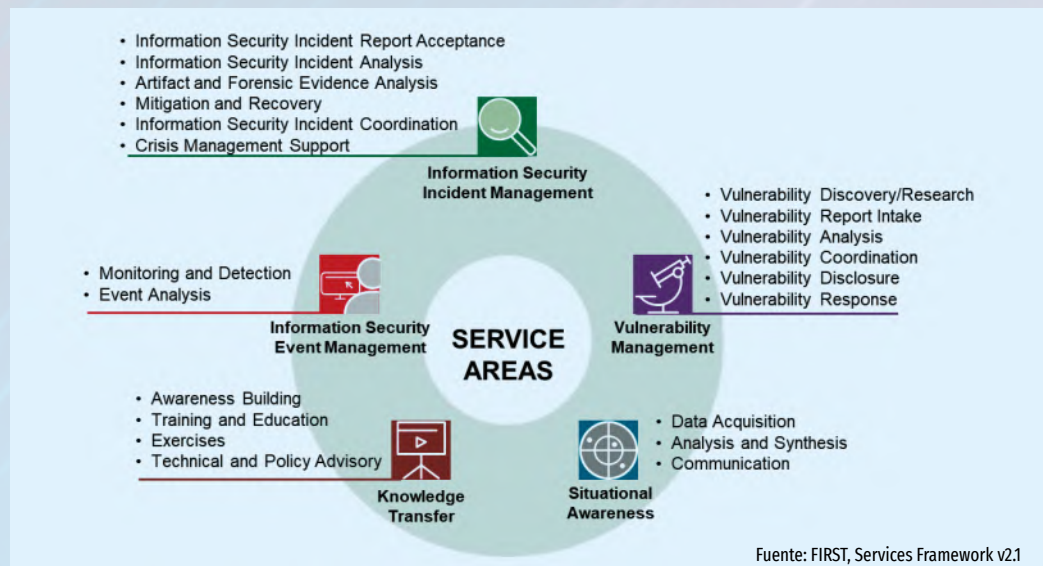
des que pueden afectar a varios proveedores y tecnologías al mismo tiempo. El pasado octubre también hizo público un nuevo código ético, denominado ‘**ethicsFIRST Framework**’, que cuenta con una página web dedicada: ethicsfirst.org. El objetivo es cubrir una serie de principios de responsabilidad de los profesionales de ciberseguridad durante

un incidente en cuanto a sus deberes de confianza, información, divulgación coordinada de vulnerabilidades, de reconocimiento de límites jurisdiccionales, etc.

Gestión y difusión de alertas y vulnerabilidades

Otros organismos internacionales disponen también de

documentación de interés para los equipos de respuesta a incidentes. Por ejemplo, el **Instituto Nacional de Estándares y Tecnología (NIST)** de EE.UU.; aunque no cuenta con ninguna publicación específica sobre CERTs/CSIRTs, dispone de una serie de documentos de buenas prácticas y procedimientos centrados en la gestión de incidentes, como



Fuente: FIRST, Services Framework v2.1



su 'SP 800-61 Computer Security Incident Handling Guide', de 2012, y la 'SP 800-83 Guide to Malware Incident Prevention and Handling', de 2013, como las más recientes y entre otros que, como es bien sabido, abarcan el vasto campo de la ciberseguridad en todas sus áreas.

Asimismo, la **Organización Internacional para la Estandarización (ISO)** y la **Comisión Electrotécnica Internacional (IEC)** cuentan con la **ISO 27035**, un estándar que consta de dos partes abordando, por un lado, los principios básicos de la gestión de incidentes y, por otro, las pautas para planificar y prepararse para la respuesta a incidentes.

También cuenta, entre otros muchos, con la **ISO/IEC 29147** sobre Divulgación de Vulnerabilidades y, dentro de la reconocida norma **ISO 27001**, su Anexo A, que es un documento normativo, atiende en su sección A.16 a la 'Gestión de incidentes de seguridad de la información'.

Cabe recordar, además, la existencia desde hace años de otras fuentes de información, como la **Common Vulnerabilities and Exposures (CVE)**, una gran base de datos de vulnerabilidades y exposiciones de ciberseguridad conocidas públicamente. Éstas, representadas mediante 'identificadores comunes', permiten el intercambio de datos entre

soluciones de seguridad, proporcionando una base para evaluar la cobertura de herramientas y servicios, además de habilitar el intercambio automatizado de información.

A ello, se le unen desde hace años otros estándares como el **Lenguaje de descripción de vulnerabilidades de aplicaciones (AVDL)** de **OASIS**, uno de los organismos de normalización sin ánimo de lucro más respetados del mundo. AVDL es un estándar XML que permite la comunicación de información sobre vulnerabilidades en las aplicaciones web de forma estándar. También, cuenta con el **Protocolo de Alerta Común (CAP)**, un estándar, también basa-

do en XML, que permite el intercambio de información de alertas y avisos públicos sobre todo tipo de redes y sistemas de alerta. Por ejemplo, permite que una alerta se difunda de manera constante y simultánea a través de varios sistemas a un gran número de aplicaciones, como Google Public Alerts.

En este sentido, resulta interesante echar un vistazo a la publicación de Enisa 'Estándares y herramientas para el intercambio y procesamiento de información procesable', el cual, aunque es de 2014, recoge un total de 53 estándares de intercambio de información diferentes para CERTs/CSIRTS.

PASO 2

Asociaciones como FIRST, TF-CSIRT o CSIRT.es validan, por sus competencias y referencias, quienes deben ser considerados como tal

Integrarse en los foros que 'deciden' quién es o no un CERT / CSIRT

Certificados CSIRT

Existe una amplia variedad de siglas para equipos de respuesta a incidentes, aunque los términos 'CERT' y 'CSIRT' son, sin duda, los más escuchados, junto al de 'SOC', incluso aunque este último tiene un ámbito de seguridad y ciberseguridad más amplio. Lo cierto es que, a menudo, los dos primeros se usan como sinónimos. Sin embargo, aunque muchas compañías usan 'CERT' de forma genérica, cabe recordar que es una marca registrada por la **Carnegie Mellon University (CMU)** desde 1997. Así pues, las organizaciones que quieran tener dicha consideración pueden solicitarlo a la Universidad, que prohíbe identificarse como tal si no se han superado sus trámites (y pagado por ello). Así, en su página web, la CMU tiene un apartado especial dedicado a los CSIRTS que deseen solicitar la autorización para usar la marca 'CERT'.

Para ello, deben seguir un proceso que, *grosso modo*, consiste en completar un formulario de calificación, que el personal de CERT revisará. Éste acudirá también al sitio web del CSIRT para

asegurarse de que cumple con las Directrices para el uso del término 'CERT'. Posteriormente, se establece contacto con el personal del CSIRT sobre cualquier cambio que deba realizarse y, posteriormente, se procederá a la firma del acuerdo.

Caso distinto es la consideración CSIRT, ya que no existe un reconocimiento oficial, y cualquiera puede autodenominarse como tal, amparándose en lo que supone este acrónimo. Sin embargo, su éxito depende en gran medida de "la confianza y reconocimiento que logre en su comunidad", como bien apunta el CCN en su Guía de Creación de un CERT/CSIRT. Esto requiere, entre otras cosas, la participación en eventos y formar parte de asociaciones o foros, tanto a nivel nacional como internacional, donde se promueva la colaboración entre CSIRTS y se intercambien experiencias y conocimientos en un entorno de confianza. Para afiliarse a ellos, normalmente, es necesario reunir una serie de requisitos (certificaciones, membresía, aceptación

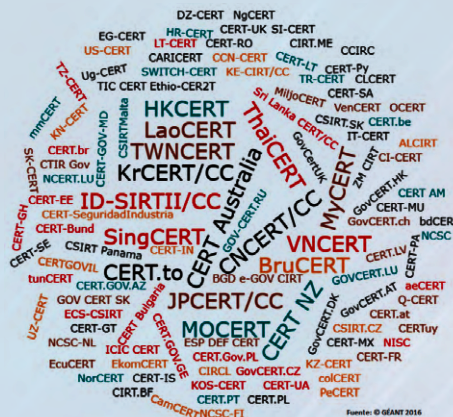
por dos o más miembros, etc.).

Por ejemplo, para convertirse en miembro de uno de los foros más importantes a nivel mundial, como es **FIRST**, los CSIRTS deben pasar por un procedimiento de validación de la comunidad.

jeto a una visita al centro donde se aloja el equipo de respuesta a incidentes". Aunque, en su reunión de abril de 2020, la Junta de FIRST decidió "suspender esta visita física hasta nuevo aviso", dada la situación generada por la pandemia de la Covid-19. Para ambos niveles, los solicitantes deben de cubrir ciertos criterios establecidos en dos formularios para cada uno de ellos, a los que se tiene acceso previo registro en la página web, sobre la información del CSIRT, sus miembros, servicios, políticas de clasificación y manejo de la información, etc.

La solicitud de membresía, que comienza con una petición formal a la Secretaría de FIRST, cubre un período de seis meses para su confirmación. Una vez que la Junta la apruebe, los solicitantes deben pagar una cuota anual de alrededor de 1.700 euros para los miembros de pleno derecho y de 210 euros para los 'enlaces'.

Un participante que presente la solicitud de FIRST debe pagar una tarifa de solicitud inicial única



Como en otros foros, existen varios niveles de membresía. En FIRST están los Miembros de Pleno de Derecho y los llamados *Liaisons* (enlaces). En el caso de los primeros requiere que un CSIRT sea "nominado por dos miembros de pleno derecho de FIRST y, luego, sea aprobado por dos tercios de los votos de su Comité Directivo, así como estar su-



de 800 dólares (cerca de 700 euros) antes de que se considere confirmada su membresía. Esta tarifa solo se aplica a las membresías completas, no a las de 'enlace'.

Por su parte, el **Trusted Introducer** (TI), uno de los principales foros europeos de CSIRTs, diferencia tres categorías: 'listado', que proporciona información básica sobre el equipo en sí y muestra el respaldo del equipo por parte de la comunidad de TI; 'acreditado', que asegura un nivel definido de mejores prácticas y la aceptación de las políticas de TI establecidas para dichos equipos; y 'certificados', para aquellos que han sido acreditados anteriormente y demuestran un nivel de madurez según lo definido por el marco SIM3 (que se explica en este mismo especial). Además, da la oportunidad a los profesionales expertos en seguridad de participar como 'Asociados de TI'.

Para registrarse en la prime-

ra categoría es necesario cumplir un formulario con información básica del Equipo y contar con al menos dos miembros acreditados o certificados como 'patrocinadores'. Para ello, no se cobra ninguna tarifa.

Solo los equipos ya 'listados' pueden acreditarse. La acreditación la realiza el Trusted Introducer siguiendo un proceso estandarizado que toma entre uno y cuatro meses, dependiendo del estado actual y la preparación, así como de la retroalimentación recibida durante este proceso. Existe una tarifa de acreditación única de 800 euros y una tarifa anual de 1.200 euros.

En el siguiente escalón estaría los certificados, destinados a los equipos acreditados que tienen razones internas y/o externas para medir su nivel de madurez de manera independiente. Ésta se mide a través del marco SIM3 y, en este caso, la primera tarifa

de certificación es de 1.800 euros, mientras que la anual es de 800.

Y quién reconoce a los CSIRT en España...

En nuestro país, uno de los foros más importantes es CSIRT.es, que se define como "una plataforma independiente de confianza y sin ánimo de lucro compuesta por aquellos equipos de respuesta a incidentes de seguridad informáticos cuyo ámbito de actuación o comunidad de usuarios en la que opera, se encuentra dentro del territorio español".

Se indica que para ser miembro candidato hay que "cumplir con la definición genérica ofrecida por la Enisa, FIRST o Trusted Introducer para este tipo de equipos". De hecho, uno de los requisitos para ser admitido en el grupo es ser miembro del FIRST o estar acreditados en el Trusted Introducer. Solo "se podrán hacer

excepciones a esta norma en el caso de Centros de ámbito público, para los que se podría proponer su entrada si disponen de al menos dos miembros que avalen su entrada al Foro, o en el caso de Fuerzas y Cuerpos de Seguridad del Estado (FFCCS), en el que tienen entrada directa", puntualiza.

Además, considera "requisito indispensable el prestar servicio a una comunidad de usuarios del territorio español, tener capacidad de reacción ante incidentes de seguridad y cuyas misiones y objetivos vengán sobrevenidos por mandato legislativo u organizativo para mejorar la seguridad de las tecnologías y comunicaciones de la Comunidad a la que presta servicio". Y, para asegurar la cooperación y confianza entre los miembros del Foro, "la admisión de nuevos miembros será sometida a votación por unanimidad por parte de los miembros de pleno derecho del foro".

PASO 3

Agencias como ENISA proponen una metodología precisa para medir sus capacidades

Cómo evaluar el nivel de madurez de un CSIRT...

Cada vez más organizaciones, como FIRST y TF-CSIRT, así como los países con redes nacionales de CSIRTs establecidas ofrecen, para ayudar a empresas y administraciones públicas en su trabajo con este concepto, documentos para incrementar la capacitación de personal, mejorar sus prácticas y su orientación.

Uno de los principales indicadores para conocer el nivel de madurez de un equipo de respuesta a incidentes es el modelo de madurez de Gestión de Incidentes de Seguridad (más conocido como Modelo SIM3), un esfuerzo impulsado por distintas comunidades para medir cómo un equipo gobierna, documenta, realiza y evalúa sus funciones.

La comunidad del **Task Force on Computer Security Incident Response Teams (TF-CSIRT)**, fue la primera en utilizar SIM3 como requisito, en 2009, para la certificación (opcional) de sus miembros. **Enisa** lo usa como base de su mé-

todo de evaluación para los CSIRT nacionales de la UE, teniendo muy en cuenta, además, los requisitos de la Directiva NIS. Asimismo, siguiendo este método, fue adoptada en 2018 por la Red de CSIRT de la UE. Además, SIM3 es la base



del Marco de Madurez Global para CSIRTs del **Global Forum on Cyber Expertise (GFCE)** e, incluso, es utilizado por la **Nippon CSIRT Association (NCA)**, que cuenta con más de 300 miembros en Japón. En la actualidad, está siendo considerado para su adopción por otras

organizaciones internacionales de CSIRTs.

Respecto a sus desarrollos más recientes, se espera la publicación de una próxima versión, SIM3 v2, este año. Además, cabe destacar, que es la **Open CSIRT Foundation** la principal organización de gestión de este modelo. De hecho, Enisa destaca que, durante todo el proceso de evaluación de la madurez de un equipo de respuesta a incidentes, "se recomienda mantenerse en estrecho contacto" con esta Fundación.

El método de Enisa CSIRT

El modelo de evaluación de Enisa se describe en el documento 'Modelo de evaluación de la madurez de ENISA CSIRT', cuya última versión fue publicada en abril de 2019. El proceso consta

de dos partes principales. Por un lado, una encuesta de autoevaluación, que se puede realizar en línea, sobre 44 parámetros del modelo SIM3 divididos en cuatro categorías: organización, procesos, herramientas y recursos humanos de un equipo de respuesta a incidentes. Estos determinarán un nivel de madurez básico, intermedio o avanzado. En este sentido, Enisa recuerda que su modelo requiere un nivel de evaluación más alto que el requerido por el Esquema de Certificación de TI, ya que también tiene en cuenta los requisitos de la Directiva NIS. Por otro lado, dicha evaluación se complementa con una revisión por parte de 'pares', es decir, de otros equipos dentro de la red de CSIRTs, como una forma de apoyo intracomunitario a fin de mejorar aún más la madurez de todos los equipos.

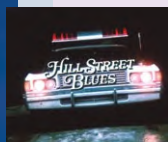




Canción triste de Hill Street... ¡Tengan cuidado ahí fuera!

Aquellos lectores nacidos en las penúltimas décadas del siglo pasado aún recordarán la serie policíaca “Canción triste de Hill Street”, con el “capitán Furillo” al mando, cuya trama giraba en torno a posibles diferencias entre lo correcto y lo que funciona.

Justo un año después de esa serie, en 1988, la universidad Carnegie Mellon en Pennsylvania, Estados Unidos, acuñó, y patentó, el término “Computer Emergency Security Team” (CERT). Este primer CERT fue la respuesta a la aparición la noche del 2 al 3 de noviembre de 1988 del pionero de los software maliciosos y auto-replicantes: el gusano de Morris. Desde entonces, la necesidad de disponer de un equipo profesional de intervención rápida frente a emergencias digitales sólo ha crecido y crecido.



Un detalle controvertido pero crucial es conocer al equipo que protegerá tu información: su experiencia, su formación, su motivación y sus condiciones laborales y nivel de rotación.

Por cierto, como el nombre de CERT está patentado, se recomienda utilizar el término genérico “Computer Security Incident Response Team” (CSIRT) para cualquier otro equipo de emergencias digitales que exista. Los CSIRTs iniciales han evolucionado hasta los centros de operaciones de seguridad (SOCs) actuales, cuya misión es la monitorización en tiempo real de los eventos de seguridad de una organización y la respuesta frente a posibles incidentes de seguridad.

Hoy en día hay cientos de CSIRTs por todo el mundo, de origen privado y público, sectoriales, nacionales, multinacionales, etc. La organización que agrupa a más CSIRTs es FIRST (el “Forum of Incident Response and Security Teams”), creado en Carolina del Norte en 1990 como organización sin ánimo de lucro.

El servicio de respuestas a incidentes es esencial para cualquier empresa conectada a Internet, independientemente de su tamaño. Eurostat publicó en 2017 que el 66% de la población activa en la Unión Europea, unos 94 millones de personas, trabajan en pequeñas y medianas empresas (pymes). Un ataque certero a cualquiera de estas em-

presas, por ejemplo un “phishing a medida” o un “ransomware” bien inyectado, puede suponer un daño de reputación irreparable o, incluso, sencillamente su desaparición. Los recursos disponibles de estas pequeñas empresas no permiten la creación de su propio CSIRT. Desde esta columna sólo puedo recomendar a empresarios y autónomos que contraten un servicio profesional de respuesta a incidentes digitales. ¿Cómo elegir el adecuado? Aquí van algunas pistas para seleccionar el SOC adecuado:

- Averigua el tamaño medio de sus clientes, no te interesa ser el cliente “más diminuto de su cartera”.
 - Confirma cómo recogen inteligencia operativa de ataques reales en tu sector y cómo interactúan con CSIRTs públicos autonómicos, nacionales y europeos.
 - Es importante que reciban y compartan información operativa con otros SOCs.
 - Solicita información sobre su grado de automatización de respuestas frente a incidentes: en ocasiones aún estamos anclados en la imagen de un analista junior pegado a una pantalla de monitorización sin pestañear, confiando en que sepa reaccionar frente a todas las alertas que el SIEM (“Security Incident and Event Monitoring”) de turno le muestre.
 - Un detalle controvertido pero crucial es conocer al equipo que protegerá tu información: su experiencia, su formación, su motivación y, relacionado con este punto, sus condiciones laborales y nivel de rotación.
 - Adicionalmente, infórmate sobre cómo pueden ayudarte en tus procesos de comunicación con clientes, fuerzas del orden, proveedores y empleados, tras sufrir un ataque digital.
 - Finalmente, recomiendo que denuncies todo ataque exitoso. Tus atacantes son delincuentes digitales.
- Como bien decía el “capitán Furillo”, tengan cuidado ahí fuera... y busquen un SOC que les funcione.

Alberto Partida
Analista en Ciberseguridad
itsecuriteer@gmail.com
@itsecuriteer en twitter



<https://linkedin.com/in/albertopartida>

Organizaciones y foros del sector ofrecen más de un centenar de documentos y guías para impulsar los CERTs/CSIRTs

Existen un gran abanico de documentos e informaciones sobre buenas prácticas, instrucciones, guías y recomendaciones para que los responsables de los equipos de CERTs y/o CSIRTs dispongan de la suficiente información y de marcos de referencia probados para desempeñar con criterio su función. Curiosamente, el mercado aún no está tan maduro como para generar informes de análisis del negocio que generan los CERT/CSIRTs, ya sea como clientes de la industria de ciberseguridad o prestando servicio. Algunos como Exabeam, que

estudia de forma anual el estado de los SOC, contemplan los CSIRT como una de las principales capacidades de estos.



De cualquier forma, la información para poner en marcha un CERT/CSIRT es abundante. En España, uno

de los documentos más importantes es, sin duda, la ‘Guía de Creación de un CERT/CSIRT’, del Centro Criptológico Nacional (CCN), perteneciente a la serie CCN-STIC-800, que fue creada específicamente para cumplir con lo establecido en el Esquema Nacional de Seguridad (ENS).

La guía, aunque fue publicada en septiembre de 2011, sigue siendo un documento de referencia, que ofrece una visión global de todas las implicaciones, no sólo tecnológicas, que conlleva la puesta en marcha de estos equipos, tanto en su diseño como en el desarrollo y

funcionamiento especialmente entre las administraciones públicas; pero, también, para los de ámbito privado.

En ella, se desarrolla la estrategia general, las experiencias y ámbitos de actuación de los CERTs/CSIRTs a nivel nacional, la normativa, buenas prácticas y legislación aplicable, así como la formación e información necesaria y las herramientas que pueden ser usadas.

Igual de importante en este ámbito es la más reciente versión de la ‘Guía Nacional de Notificación y Gestión de Incidentes Cibernéticos’



A pesar de sus más de 30 años, los equipos aún deben evolucionar mucho

El futuro de los CERTs/CSIRTs pasa por reglas que generen más confianza y mayores capacidades

Todos aquellos que trabajan en la respuesta a incidentes y los esfuerzos de intercambio de información saben que queda mucho por hacer. Si bien hay un gran trabajo en progreso en esta área de seguridad de la información, uno de los documentos más amplios e interesantes en cuanto a la evolución y actuales tendencias que rodean a los CSIRTs y las capacidades de respuesta a incidentes (IR) lo ha publicado **Enisa**, siendo éste uno de los pocos dedicados a analizar la evolución y tendencias titulado 'Estudio sobre el panorama de los CSIRTs e IRs en Europa 2025'.

Para realizarlo, dichas tendencias y hallazgos se identificaron mediante el mapeo de CSIRTs nuevos y menos visibles creados recientemente y mediante la investigación de políticas europeas y su impacto fuera de Europa. Así, se identificaron 81 nuevos CSIRTs y se analizó un *corpus* de 36 documentos de política, legislación y estrategias relacionadas con el desarrollo de capacidades de respuesta a incidentes.

Entre sus conclusiones destaca que uno de los principales retos que marcarán la evolución de los CSIRTs y los IRs, especialmente dentro de Europa, es el creciente número de los sectoriales y la evolución de un modelo vertical como complemento al modelo horizontal y centralizado. De hecho, esta es una de las principales prioridades de la actualización de la Directiva NIS, en cuya revisión se ha detectado que el grado de madurez de las capacidades nacionales de respuesta a incidentes varía de un

estado a otro, por lo que el papel y el alcance de acción de los CSIRTs también pueden variar de un país a otro, existiendo un riesgo de fragmentación en términos de capacidades. De hecho, en un reciente encuentro organizado por Kaspersky, el Jefe de la Unidad de Infraestructura y Servicios de Seguridad de Enisa, **Evan-gelos Ouzounis**, comentó que, en el caso de



los CSIRTs "es necesario seguir desarrollando medidas de acción en caso de grandes crisis, aumentando la colaboración y la cooperación con el sector privado especialmente, para compartir información de forma regular". Añadió, además, que se está trabajando para armonizar las capacidades de ciberseguridad de los estados miembro y reducir lo máximo posible la fragmentación existente.

Evolución natural

El documento de Enisa destaca también, cómo los CSIRT y los equipos de respuesta a incidentes (IR) están cambiando rápidamente

te por naturaleza, subrayando el desarrollo de este tipo de capacidades en las fuerzas armadas. Y es que éstas "están inmersas en un proceso de digitalización similar a la observada en el mundo civil ya que, cada vez más, hacen uso de herramientas tecnológicas similares y, por lo tanto, se enfrentan prácticamente a los mismos problemas de seguridad". Asimismo, el documento destaca que, en algunos estados miembros de la UE, el Centro Nacional de Seguridad Cibernética ha absorbido los CSIRTs nacionales o gubernamentales, como parte de una evolución natural de los mismos.

IoT, motor de cambios

El sector privado y los fabricantes de dispositivos digitales también están desempeñando un papel cada vez más importante en la respuesta a incidentes. Los fabricantes de dispositivos están desarrollando sus propios CSIRTs, a veces llamados PSIRT (*Product Incident Response Teams*), como IBM, Cisco, Huawei, etc. La idea se originó a partir de que muchos expertos en este campo se dieran cuenta de que los CSIRTs en sí no aunaban completamente las funciones y responsabilidades que debería de tener un PSIRT. Tal es así que, incluso, FIRST publicó a principios de este año un nuevo borrador sobre el marco de trabajo de este tipo de servicios bajo el título '*Product Security Incident Response Team (PSIRT) Services Framework Version 1.1*'. En él, se indica que "en la creación del marco de trabajo sobre los servicios de un CSIRT quedó claro que los PSIRTs brindan servicios y operan, por lo general, en entornos muy diferentes", y establece que "un PSIRT es una entidad dentro de una organización que, en esencia, se centra en la identificación, evaluación y disposición de los riesgos asociados con las vulnerabilidades de seguridad dentro de los productos, incluidas las ofertas, soluciones, componentes y/o servicios que una organización produce o vende". Además, "un PSIRT correctamente implementado no es un grupo que opera de forma independiente, sino que está conectado al desarrollo de los productos de la organización".

Y, aunque este tipo de capacidades viene siendo ampliamente tratado desde hace un par de años, la tendencia es que "este tipo de oferta se expanda", a medida que la IoT va ganando terreno en muchos de los sectores de la sociedad, según concluye el informe de Enisa. ■

cos', editada con "el objetivo de ofrecer un marco de referencia consensuado por parte de los organismos nacionales competentes en el ámbito de la notificación y gestión de incidentes de ciberseguridad, alineándose con la normativa española, transposiciones europeas, así como documentos emanados de organismos supranacionales que pretenden armonizar la capacidad de respuesta ante incidentes de ciberseguridad".

En el ámbito de la UE, **Enisa** dispone de más de 70 informes para mejorar las funciones de respuesta a incidentes, la preparación del equipo en su conjunto, así como la cooperación

en el intercambio de información. Los más recientes, publicados a principios de este año, se destinan a proporcionar una hoja de ruta para fomentar la cooperación entre los CSIRTs y el poder judicial en la lucha contra el ciberdelito, como el documento titulado '**Una descripción general sobre la mejora de la cooperación técnica entre CSIRTs y LE**'. A él se le unen dos guías de 2019, que describen el modelo y la metodología de madurez de la Agencia para los CSIRTs, así como otros con una proyección más amplia, como el '**Informe del estado de desarrollo de la respuesta a incidentes de los estados miembros de la**

UE', tras la transposición de la Directiva NIS, o su documento '**Comunicaciones seguras entre grupos**', publicado como punto de partida para la mejora de la cooperación operativa, la preparación y el intercambio de información.

También, hay organizaciones internacionales que han generado informes de gran interés, como la Carnegie Mellon, creadora del primer CERT, que dispone, entre otros, de un amplio documento de más de 300 páginas, de 2001; y el **CERT-EU**, que generó un documento a mediados de año para hacer frente a las ciberamenazas más frecuentes durante la pandemia, entre otros.



Hay cerca de 60, tanto de organismos públicos como de empresas privadas

España, uno de los países que más apuestan por los equipos de respuesta cibernética

Con 54 equipos registrados en la Agencia de Ciberseguridad de la UE, España es el país europeo con más equipos de respuesta a incidentes cibernéticos, frente a los 51 de la República Checa, los 47 de Alemania, los 40 de Francia o los 26 del Reino Unido. No es el único foro interna-

cional donde somos referencia cuantitativa, ya que en First, la principal asociación del mundo de CSIRT, somos el tercer país con mayor número de miembros, tras EE.UU. y Japón. Además, desde 2018, impulsado por el CCN, también es muy activo el foro CSIRT.es con más de 40 integrantes.

PRINCIPALES EQUIPOS DE RESPUESTA A INCIDENTES ESPAÑOLES

- ACK CERT
- Aiuken CERT
- Anadat CERT
- Andalucía CERT
- Auren CERT
- Banco Sabadell CERT
- Basque Cybersecurity Centre CERT (BCSC)
- BBVA CERT
- CaixaBank CSIRT
- Catalonia CERT
- CCN-CERT
- Cipher CERT
- CNPIC
- CSA Global CSIRT
- CSIRT CARM (Murcia)
- CSIRT.gal (Galicia)
- CSIRT-CV (Valencia)
- CSUC CSIRT (Consortio de Servicios Universitarios de Cataluña)
- Deloitte Cyber SOC CERT
- DXC Iberia CSIRT
- Entelgy Innotec CSIRT
- ERIS-CERT (Sothis)
- Ertzaintza SCDTI
- esCERT-UPC (Universidad Politécnica de Cataluña)
- ESP DEF CERT (Mando Conjunto de Ciberespacio)
- Eulen-CCSI-CERT
- Everis CERT
- Getronics CERT
- GMV CERT
- Grupo ICA CyberSOC CERT
- Guardia Civil - Ciberinteligencia y Ciberterrorismo
- Guardia Civil - Dpto. de Delitos Telemáticos
- Iberdrola Cyber-Security Incident Response Team
- IECISA CERT (Informática El Corte Inglés)
- INCIBE-CERT
- INDITEX CSIRT
- Ingenia eSOC
- Intec CERT
- ITS CERT
- Light Eyes CERT
- Madrid Digital (CSIRT)
- Mapfre-CCG-CERT
- Minsait CERT
- MNEMO-CERT
- Mossos d'Esquadra
- NestleSOC
- Nunsys-CERT
- Oesía CERT
- OSSI-CERT SERMAS (Serv. Madrileño de Salud)
- Policía Nacional
- Prosegur CERT
- RedIRIS
- Renfe CERT
- Repsol CERT
- S2 Grupo CERT
- S21sec CERT
- Santander Global CERT
- SCC CERT (Centros Informáticos Especializados)
- Secure&IT (S&IT CERT)
- Seidor CERT
- Sergas CERT (Serv. Gallego de Salud)
- SIA-CEC CERT
- Telefónica CSIRT
- UAM CERT (Universidad Autónoma de Madrid)
- UC3M CERT (Universidad Carlos III de Madrid)
- Versia CERT /CSIRT

CERTs / CSIRTs ESPAÑOLES EN LOS PRINCIPALES FOROS NACIONAL E INTERNACIONALES*

ENISA	FIRST	TRUSTED INTRODUCER	CERT (Carnegie Mellon University)	CSIRT.es
ACKCERT	ACKCERT			
			ACK3 CERT	
		ACN_IBE_CSIRT (Accenture. Candidato)		
CERT Aiuken	CERT Aiuken			
			Anadat CERT	
Andalucía CERT		Andalucía CERT		Andalucía CERT
			Auren CERT	
			Grupo Banco Sabadell CERT	
BBVA CERT	BBVA CERT		BBVA CERT	
BCSC	BCSC www.first.org/members/teams/bcsc	BCSC	Basque Cybersecurity Centre CERT	Basque Cybersecurity Centre
• CaixaBank CSIRT • CaixaBank Team CSIRT	CaixaBank Team CSIRT	CaixaBank CSIRT	CaixaBank CERT	CaixaBank CSIRT
				CSIRT CARM (Región de Murcia)
			Cast Info CERT	
• CATALONIAN-CERT • CESICAT-CERT • Catalonia CERT	Catalonia CERT	Catalonia CERT	Information Security Center of Catalonia	CESICAT-CERT



CERTs / CSIRTs ESPAÑÓLES EN LOS PRINCIPALES FOROS NACIONAL E INTERNACIONALES*

ENISA	FIRST	TRUSTED INTRODUCER	CERT (Carnegie Mellon University)	CSIRT.es
CCN-CERT	CCN-CERT	CCN-CERT	Cryptology National Center Computer Emergency Response Team	CCN-CERT
· Cipher CERT · PROSEGUR CERT	Cipher CERT		Prosegur CERT	Prosegur CERT
				CNPIC
CSA-CSIRT	CSA-CSIRT			Global CSIRT (CSA)
· CSIRT-CV · CSIRTCV	CSIRT-CV	CSIRT-CV	Comunidad Valenciana CERT	CSIRT-CV
CSUC-CSIRT (Consortio de Servicios Universitarios de Cataluña)		CSUC-CSIRT (Consortio de Servicios Universitarios de Cataluña) www.trusted-introducer.org/directory/teams/ica-sys-cibersoc.html		CSUC-CSIRT (Consortio de Servicios Universitarios de Cataluña)
Deloitte EDC	Deloitte EDC	Deloitte EDC	Deloitte CyberSOC CERT	Deloitte EDC
DXC Technology Iberia CSIRT	DXC Technology Iberia CSIRT		Security Competence Center CERT (SC2-CERT)	
Entelgy-CSIRT	Entelgy Innotec CSIRT	Entelgy Innotec CERT	ENTEGLY-CSIRT InnoTec System	Entelgy Innotec Security CSIRT
ERIS-CERT	ERIS-CERT	ERIS-CERT	Equipo de Respuesta a Incidentes – Sothis ERIS-CERT	ERIS-CERT
				Ertzaintza SCDTI
ESP DEF CERT	ESP DEF CERT	ESP DEF CERT	CERT Mando Conjunto de Ciberdefensa	ESP DEF CERT
Eulen-CCSI-CERT	Eulen-CCSI-CERT		Eulen Seguridad	Eulen-CCSI-CERT
everis CERT	everis CERT	everis CERT	Everis Aerospace, Defense & Security	everis CERT
CSIRT.gal		CSIRT.gal (Galicia)		CSIRT.gal (Galicia)
			Getronics CERT	
GMV-CERT	GMV-CERT		GMV Computer Incident Response Team	GMV-CERT
				Guardia Civil Ciberinteligencia y Ciberterrorismo
				Guardia Civil Departamento de Delitos Telemáticos
· CiberSOC · ICA SYS CiberSOC · ICA Sistemas y Seguridad CiberSOC	ICA Sistemas y Seguridad CiberSOC	ICA SYS CiberSOC	Grupo ICA CERT	ICA SYS CiberSOC
Iberdrola CSIRT	IBERDROLA CSIRT			Iberdrola Cyber-Security Incident Response Team
INCIBE-CERT	INCIBE-CERT	INCIBE-CERT	National Cybersecurity Institute of Spain (INCIBE)	INCIBE-CERT
		IECISA CSIRT (Candidato)	Informática El Corte Inglés (IECISA CERT)	
eSOC Ingenia	eSOC Ingenia			Ingenia eSOC
			Intec Cert	



CERTs / CSIRTs ESPAÑOLES EN LOS PRINCIPALES FOROS NACIONAL E INTERNACIONALES*

ENISA	FIRST	TRUSTED INTRODUCER	CERT (Carnegie Mellon University)	CSIRT.es
ITS-CERT	ITS-CERT	ITS-CERT	ITS Industrial Cybersecurity CERT	ITS-CERT
ITXCSIRT		ITXCSIRT (Inditex)		
LE-CERT (Light Eyes CERT)		LE-CERT (Light Eyes CERT)		
MAPFRE-CCG-CERT	MAPFRE-CCG-CERT	MAPFRE-CCG-CERT	CCG de MAPFRE Equipo de Respuesta a incidentes de Seguridad de la Información	Mapfre-CCG-CERT
Minsait CSIRT	Minsait CSIRT	Minsait CSIRT	Minsait CERT	Minsait CSIRT
		Mnemo-CERT		MNEMO-CERT
				UCIBER-Mossos d'Esquadra
				NestleSOC
NS-CERT (Nunsys)		NS-CERT (Nunsys)	Nunsys CERT (NS-CERT)	NUNSYS-CERT
CERT OESÍA	CERT OESÍA		Oesia Networks S.L.	Cert Oesía
				OSSI-CERT SERMAS (Oficina de Seguridad de Sistemas de Información – Servicio Madrileño de Salud)
			P3rseus CERT	
				Policía Nacional
RedIRIS	RedIRIS	RedIRIS		RedIRIS
RENFE	RENFE			RENFE CERT
REPSOL CERT	REPSOL CERT			Repsol CERT
S2 Grupo CERT	S2 Grupo CERT	S2 Grupo CERT	S2 Grupo CERT	S2 Grupo CERT
S21sec CERT	S21sec CERT	S21sec CERT	· S21sec CERT · S21sec Labs	S21sec CERT
Santander Global CERT	Santander Global CERT		Santander Global CERT	
			Specialist Computer Centres SL SCCes-CERT (SCC Spain)	
			Secure and IT Proyectos (S&IT CERT)	
			Seidor CERT Cybersecurity Operations Center	
			Sergas_CERT (Servicio Gallego de Salud)	
SIA-CEC CERT	SIA-CEC CERT		SIA-Cybersecurity Expert Center CERT	SIA-CEC CERT
			TBSecurity-CERT	
· TEFCSIRT · Telefónica-CSIRT	Telefónica-CSIRT	TEFCSIRT		CSIRT Global Telefónica
CERT-UAM		CERT-UAM (Univ. Autónoma de Madrid)		
CERT-UC3M		CERT UC3M (Univ. Carlos III de Madrid)	CERT-UC3M	CertUC3M
esCERT UPC (Univ. Politécnica de Cataluña)	esCERT UPC	esCERT-UPC		esCERT-UPC
Versia-CSIRT	Versia-CSIRT		Versia-CERT	

* Recopilación actualizada a fecha de 30/10/2020

* Las denominaciones recogidas se atienen a lo reflejado en los listados de cada apartado, independientemente de la categorización con la que está registrados. Son meramente informativas.



Así opinan

ORGANIZACIONES INTERNACIONALES DE REFERENCIA

1.

¿Le parece que los CERTs / CSIRTs están evolucionando adecuadamente?

2.

¿Cuál es el principal reto para 2021?

3.

¿Cómo se podría, en concreto, mejorar la compartición de información entre CERTs / CSIRTs?



CARNEGIE MELLON UNIVERSITY-SEI

James Lord

Gerente Técnico de Operaciones de Seguridad en la División CERT

“La respuesta a incidentes está convirtiéndose en un área más, más que un simple enfoque como pasaba en muchas empre-

sas. El Software Engineering Institute (SEI) ahora está comprometido, principalmente, con los centros de operaciones de seguridad y las agencias nacionales de ciberseguridad. En este sentido, la comunidad también ha pasado de funciones proactivas y reactivas a áreas de servicio”.

De cara a 2021, “la importancia de la Infraestructura Crítica (CI) para las naciones continuará creciendo. El SEI participa a nivel mundial con socios y partes interesadas en la identificación de CI y luego en definir capacidades para Identificar, Proteger, Detectar, Responder y Recuperar, principalmente a través de CERTs / CSIRTs del sector”.



TF-CSIRT TRUSTED INTRODUCER

Silvio Oertli

Presidente

“Los diferentes CSIRTs de nuestra comunidad han adoptado muy bien las nuevas circunstancias y las nuevas amenazas. Sin duda, fue un desafío adaptar los procesos y organizar los equipos de acuerdo con la situación. El contacto social entre los CSIRTs individuales es un poco limitado, pero esto no afecta al intercambio de información.

Los ciberataques a las organizaciones son más sofisticados hoy en día que hace 20 años. Debido a que cada organización tiene un mejor conjunto de herramientas técnicas, los ataques utilizan el factor humano para tener éxito, por lo que muchos de ellos comienzan con *phishing* o ingeniería social. Y los atacantes están utilizando circunstancias como la Covid-19 para preparar campañas en su contexto. El gran desafío ahora y en 2021 será controlar el factor humano. Por lo tanto, debemos llamar la atención de la gerencia para capacitar al personal de acuerdo con las amenazas de *phishing*”.



FIRST
Serge Droz
Presidente

“FIRST se complace en ver la mayor atención que los CSIRTs están ganando a nivel mundial. Esto se refleja en el aumento de nuestros integrantes y la profesionalidad de los equipos que solicitan ser miembros.

Empresas y estados se están dando cuenta de la importancia de los CSIRTs para mantener seguros a los usuarios de Internet y, por lo tanto, a Internet. Por eso, los CSIRTs de todo el mundo deben colaborar para garantizar la seguridad de la Red. El clima político actual, así como una política equivocada amenazan esto y hacen que sea menos segura”.



ENISA
Edgars Taurins
Experto de ENISA

“La Agencia de la Unión Europea para la Ciberseguridad (Enisa) ha apoyado a los CSIRTs durante más de 15 años y cooperado con ellos no solo en Europa, sino también en todo el mundo. Actualmente,

tenemos 555 equipos registrados. Los CSIRTs están evolucionando de manera adecuada y rápida y la Agencia los ayuda a ello. De hecho, como uno de los proyectos de este año, estamos analizando las capacidades frente a incidentes de CSIRTs de sectores concretos, como son los de Aviación y Energía. El objetivo de este estudio es analizar sus capacidades específicas, así como los cambios recientes generados en el contexto de la Covid-19 y la próxima revisión de la Directiva NIS. Los resultados del estudio cubrirán el desarrollo de la madurez de la respuesta a incidentes sectoriales, los servicios prestados, así como los desafíos y lagunas identificados. Esperamos tenerlo terminado a final de año.

En 2006, Enisa publicó la Guía de configuración de CSIRT, que describe el proceso de configuración de un CSIRT desde todas las perspectivas relevantes y este año estamos desarrollando directrices, disponibles a finales de año, para ayudar a los equipos en aspectos concretos como el ciclo de mejora y el enfoque basado en resultados, así como actuando como repositorio de información para el trabajo relacionado de Enisa en capacitaciones técnicas en particular”.



OTAN
Emmanuel Bouillon
Jefe de Operaciones de Seguridad Cibernética en el Centro de Ciberseguridad

“En 2016, los Jefes de Estado y de Gobierno aliados reconocieron el ciberespacio como un ámbito de operaciones en el que la OTAN debe defenderse tan eficazmente como lo hace en aire, tierra y mar. Esta decisión activó una gama completa de

actividades de planificación, incluida la Transformación del Comando Aliado, para prepararse para la futura lucha contra las ciberamenazas aprovechando las oportunidades generadas por las nuevas tecnologías. Los expertos de la agencia apoyan a ACT en estos esfuerzos.

El Centro de Seguridad Cibernética de la OTAN juega un papel central en el intercambio de información, que es primordial para Allied CERTs. Somos un centro para defensores cibernéticos técnicos en toda la Alianza. Además, nuestro equipo intercambia información periódicamente con sus pares en el CERT-EU. Es importante destacar que estamos colaborando estrechamente con la industria. Todos reconocemos que aprender unos de otros es la mejor manera de responder a las amenazas similares a las que todos enfrentamos. El Centro de Seguridad Cibernética de la OTAN también participa activamente en el mundo académico.

En definitiva, la OTAN se adapta continuamente a las ciberamenazas emergentes centrándose en el intercambio de información. Cuando trabajamos juntos y aprendemos unos de otros, somos más fuertes”.



APCERT (plataforma de colaboración)
Mohd Shamir Hashim
Vicepresidente Malasia Ciberseguridad

“Mantenerse al día con el avance de la tecnología de Internet es una tarea abrumadora para los CERTs / CSIRTs. Debido al enfoque y énfasis de cada país, las capacidades de los CERTs para mitigar los incidentes de ciberseguridad varían. Algunos, principalmente en los países desarro-

llados y en desarrollo, pueden manejar bien los incidentes, y hay muchos que todavía están luchando por ello. Esa es una de las razones por las que se forman plataformas de colaboración CERTs internacionales, como APCERT, para ayudar a los miembros a desarrollar las capacidades necesarias para manejar las amenazas a la seguridad cibernética. Hoy en día, las redes están interconectadas y la fuerza de dicha red es tan buena como su eslabón más débil.

Por eso, la reacción a las ciberamenazas debe ser rápida. Es vital que los equipos técnicos de los CERTs puedan comunicarse directamente entre sí, porque hablan el mismo idioma. Pasar por las líneas de comunicación internacionales gubernamentales habituales no hará posible una comunicación rápida”.