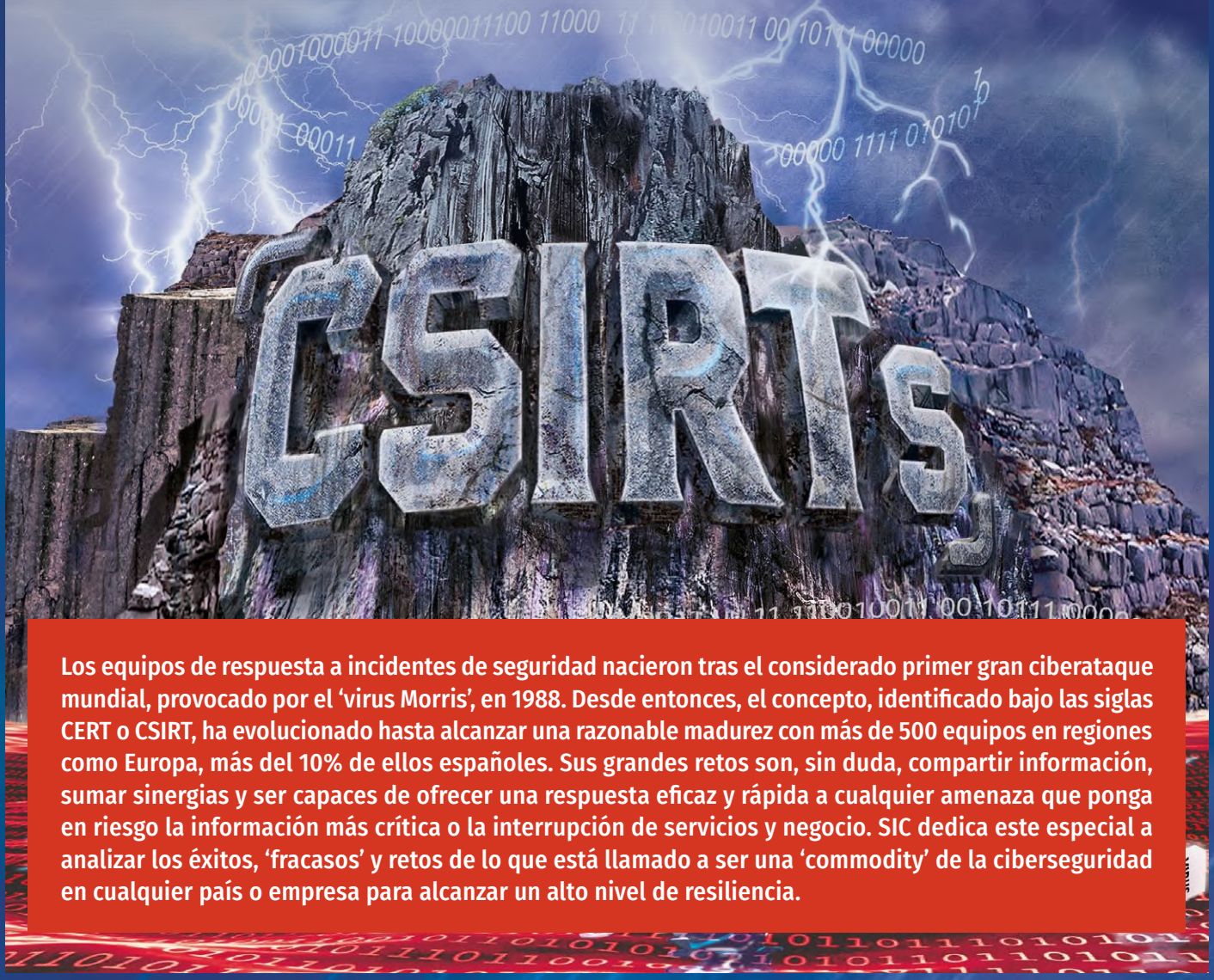
ágoraSIC Centro de Conocimiento en Ciberseguridad

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

* Es posible obtener una versión en pdf de este especial rellenando el formulario disponible en www.revistasic.com

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 **Harward, 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 Trusted 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 arquitectura 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 especialización está llegando a este concepto para dar respuesta a amenazas cada vez más complejas y recurrentes.

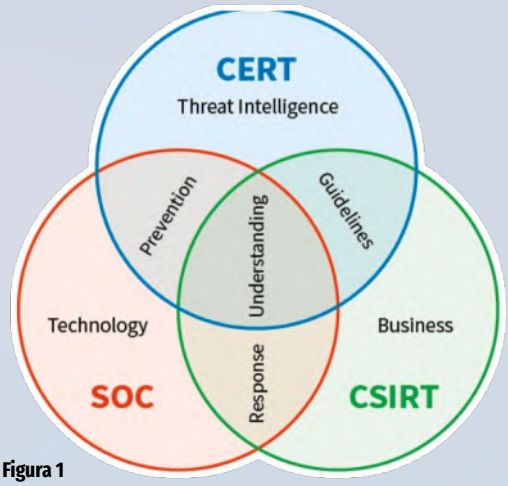


Figura 1

Fuente: Exabeam

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.

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.

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

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 cibercrisis 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

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
• Alertas y advertencias • Tratamiento de incidentes • Análisis de incidentes • Respuesta a incidentes *in situ* • 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	• 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	• 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 CISRT 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 **Exabeam** (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.

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 adecuadamente 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

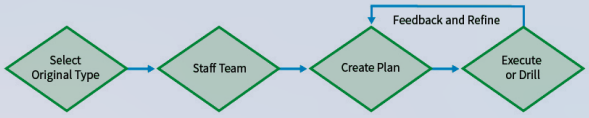
Sin duda, los salarios del personal que compone un CERT/CSIRT depende de muchos factores y es muy difícil de establecer una clasificación específica.

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

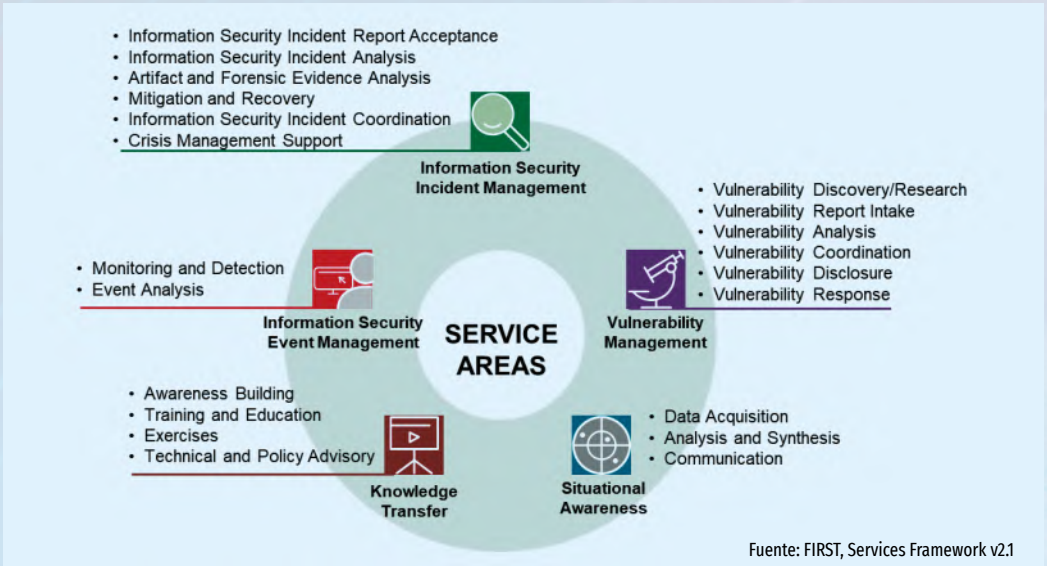
Qué estándares internacionales se deberían adoptar para el trabajo diario de los CERTs/CSIRTs

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 vulnerabilidades 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 basado 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

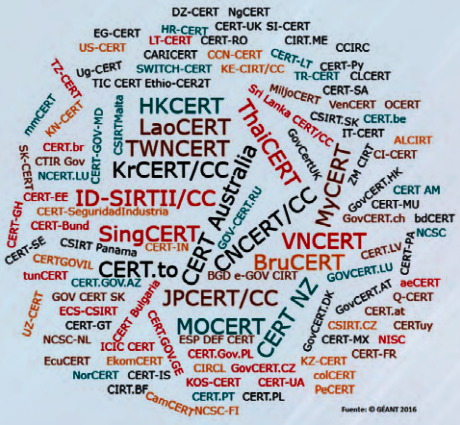
Certificados CSIRT

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.



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 sujeto 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

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 primera categoría es necesario cumplimentar 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 vengan 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

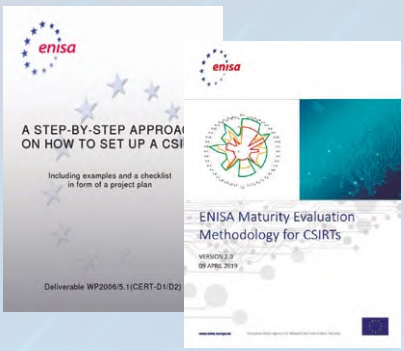
Agencias como ENISA proponen una metodología precisa para medir sus capacidades

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 método 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 empresas, 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 Cibernéti-**

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, **Evangelos 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 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 internacional 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 (Consorcio 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 CiberSOC 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'Escuadra
- 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 ESPAÑOLES 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 (Consorcio de Servicios Universitarios de Cataluña)		CSUC-CSIRT (Consorcio de Servicios Universitarios de Cataluña) www.trusted-introducer.org/directory/teams/ica-sys-cibersoc.html		CSUC-CSIRT (Consorcio 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	ENTELGY-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
			TBSSecurity-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.

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 empresas. 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 desarrollados 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".

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?

CENTRO CRIPTOLÓGICO NACIONAL–CCN
Carlos Abad
Jefe de Área de Sistemas de Alerta y Respuesta a Incidentes
CCN CERT

❶ "Se están adaptando adecuadamente, están cambiado su rol a un estadio menos operacional y más estratégico, se están convirtiendo en referentes para los Centros de Operaciones de Ciberseguridad en aras de manejar la ciberamenaza, aportando procedimientos, soluciones y conocimiento no solo en la gestión de incidentes sino también en velar por la coordinación e intercambio dentro de la comunidad propia de cada uno de ellos.

No obstante, no está resuelta la coordinación entre SOCs y CERTs por lo que se tiene un claro peligro de descoordinación donde se penalice el intercambio y la respuesta no sea global desde una visión de conjunto. Por ello es necesario que las relaciones de coordinación estén claras desde el principio".

❷ "Si los SOCs son la vigilancia y la respuesta, los CERTs / CSIRTs son el *expertise*, el conocimiento y la guía, el faro que enseña el camino a seguir. El principal reto es disponer de una plataforma común que sirva de punto de encuentro para toda la comunidad, estamos acostumbrados a tener soluciones y a integrarlas ahora toca ponerlas a disposición de la comunidad a través de una única plataforma consensuada por todos los actores implicados. El reto aquí es conseguir una gestión de la ciberseguridad única y eficiente, además de trasversal a todos los ecosistemas con independencia del origen público (con todas sus variantes de AGE, CCAA y EELL) o privado".

❸ "Haciéndolo todo fácil, sencillo y simple... automatizando procesos... en definitiva contando con una Plataforma Común. Y esto acompañado, por supuesto, de una mayor implicación a la hora de compartir de todas las partes, no solo de los CERTs de referencia o de los más veteranos.

Por desgracia, principalmente en el sector privado, existen muchas reticencias a compartir información técnica de los ciberataques, lo que penaliza la respuesta que se pueda dar a nivel nacional a algunas amenazas. Evidentemente la necesidad de notificación expresada en el RDL 12/2018 se ha quedado un poco corta".

INSTITUTO NACIONAL DE CIBERSEGURIDAD–INCIBE

Marcos Gómez Hidalgo
Subdirector Servicios INCIBE CERT

❶ "Sí, razonablemente sí. Los servicios han evolucionado creciendo en capacidades en todo lo que requieren ahora sus públicos objetivos: más detección temprana, más notificaciones hacia posibles víctimas y afectados de incidentes, mayores capacidades para gestionar y dar soporte a más incidentes y a su sofisticación, mejores herramientas, etc. Además, la industria también se ha ido pertrechando con nuevas capacidades de inteligencia, vigilancia digital, etc., que están acompañando muy bien a los CERTs. En INCIBE llevamos innovando en estos campos desde la creación de nuestro CERT en 2007".

❷ "Asentar bien todas estas capacidades, y aumentar aquellas que van dirigidas a la prevención y detección temprana, para evitar y mitigar el impacto negativo de los incidentes en los afectados y en general en la confianza digital. Es un reto global pues con la madurez de más equipos de respuesta a incidentes se conseguirá una mayor ciberresiliencia. En INCIBE es un reto que renovamos todos los años con mucha ilusión".

❸ "Los CERTs y CSIRTs vienen colaborando e intercambiando información, desde hace mucho tiempo. Para eso están las redes de confianza de FIRST, Trusted Introducer y la CSIRT Network de la NIS Directive. La Ley 12/2018 establece un nivel de cooperación técnico entre los diferentes CERTs de referencia y las distintas autoridades competentes. Además, han aparecido, en los últimos años, herramientas muy eficaces de intercambio de dicha información técnica como MISP, que en el caso de INCIBE se llama Ícaro. Es fundamental contar con elementos técnicos, pero también con la voluntad de compartir".

MANDO CONJUNTO DEL CIBERESPACIO–MCCE

Emilio Rico Ruiz
Teniente Coronel Analista en la Fuerza de Operaciones

❶ "Los CERTs / CSIRTs están potenciando sus capacidades para predecir, detectar, prevenir y responder, y el resultado es que cada día están mejor preparados para contrarrestar los problemas de seguridad y para ofrecer una respuesta y una resolución rápida de los incidentes. Además, las organizaciones nacionales e internacionales (CSIRT.es, FIRST, Terena...) están contribuyendo de manera muy positiva al desarrollo y divulgación de buenas prácticas y creando una comunidad de CERTs / CSIRTs cada vez más activa y más comprometida".

❷ "Las amenazas y los actores que hay detrás de ellas, siguen evolucionando constantemente. El reto consiste en no perder el paso y evolucionar a ese mismo ritmo. Y dado que cada vez es más creciente el volumen y la complejidad de las alertas, las organizaciones van a tener que cambiar algunos enfoques de seguridad, dando un impulso decidido a la detección proactiva de estas amenazas, incorporando técnicas y personal experto en *Threat Hunting* y evolucionando hacia sistemas automatizados de alerta-respuesta".

❸ "El modelo de intercambio y la compartición de información entre CERTs / CSIRTs se basa en tres aspectos: unos procedimientos comunes, unas herramientas interoperables y una confianza mutua entre las organizaciones. Se ha avanzado mucho en todas ellas. Disponemos de taxonomías, usamos muchas veces las mismas herramientas, nuestros métodos son similares y se comparte valiosa información acerca de los incidentes que sufrimos. También hemos avanzado mucho en la confianza mutua, pero es aquí donde todavía se necesita seguir sumando esfuerzos para hacer más eficiente la respuesta a los incidentes. La amenaza más grande a un intercambio efectivo de la información es que acabemos 'comercializando' el ciberespacio, es decir, hay que evitar que una posible ventaja comercial competitiva derive en un freno a la comunicación y a la compartición".

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?

ACKCENT

Andreu Mont

Chief Services Officer

❶ "La celeridad con la que evolucionan las amenazas y el aumento de la complejidad de los incidentes constituye un reto importante para los CERTs. Un aspecto clave a nivel organizativo lo constituye la rapidez en la respuesta a incidentes. Aunque en los últimos años ha habido una evolución, todavía hay recorrido hacia estructuras más ágiles y flexibles".

❷ "Los retos a los que se enfrentan los CERTs son, a grandes rasgos, los mismos a los que se enfrentan la mayoría de las organizaciones. Por un lado, la celeridad del cambio a todos los niveles: tecnologías, amenazas, complejidad...; por otro lado, el de la gestión de la entropía en entornos de alta incertidumbre, especialmente de los mercados y de la sociedad en general (sobre todo en momentos como los que estamos viviendo)".

❸ "Tradicionalmente, éste ha sido y continúa siendo uno de los puntos clave de los CERTs / CSIRTs. En un entorno en el que la mayoría de las amenazas provienen de la red, los CERTs deberían organizarse mejor en red, y diseñar y ejecutar estrategias conjuntas en esa dirección".

AIUKEN CYBERSECURITY

Juan Miguel Velasco

Fundador y CEO

❶ "La evolución de los Centros de Emergencia y Respuesta Temprana está más orientada hacia la difusión de información y de políticas de seguridad y de prevención que a la verdadera compartición de datos para prevenir emergencias y sería mucho más práctico que todos empezáramos a mentalizarnos de que los buenos debemos colaborar tanto como los malos, porque si no, no conseguiremos avanzar en la defensa de las administraciones de los clientes y las personas".

❷ "La asignatura pendiente de los CERTs sigue siendo el poder generar la detección temprana de amenazas y la compartición de información con otros centros, así como la generación de IoCs de forma rápida e inmediata y a poder ser preventiva. Creemos que con la evolución de las amenazas inmediatas que ya estamos sufriendo en este año, el próximo será todavía peor y una mayor colaboración, velocidad, agilidad, y precisión serán necesarias para todos los CERTs".

❸ "Deberíamos implementar mecanismos de anonimización para evitar comprometer las fuentes de conocimiento de las amenazas y, a la vez, ser conscientes de que la colaboración entre los centros de alerta temprana es el único camino para poder combatir eficientemente las amenazas y las mutaciones del *malware* que se nos avecinan".

AUREN

Josep Salvador Cuñat

Socio de Consultoría en el Área de Seguridad de la Información

❶ "En general se ha notado una mayor madurez en cuanto a servicios y disponibilidad de actores durante estos últimos años frente a los pocos CSIRTs iniciales, solo disponibles para grandes compañías. No obstante, es importante que el usuario final distinga entre un CSIRT y un SOC, siendo el primero un equipo de respuesta enfocado plenamente a la seguridad de la información y el segundo un concepto más amplio. Además, CERT es una marca registrada por Carnegie Mellon, si bien es usado como sinónimo de CSIRT".

❷ "Por un lado, los canales para interactuar con el receptor final del servicio, que deben ir más allá de un mero boletín o soporte por correo electrónico, así como que los CSIRTs externos puedan de verdad dar respuesta a la organización cliente ante un ciberincidente, lo cual requiere también cierta capacitación o enlace con la organización receptora del servicio para un resultado realmente eficaz".

❸ "Debe fomentarse sin duda la estandarización del formato de la información y fijarse un canal común para la iniciativa pública y privada, evitar los recelos entre estos sectores y colaborar activamente en la detección de nuevos vectores de ataque".

EVERIS

Miguel Ángel Thomas

Socio Responsable del Área de Ciberseguridad

❶ "El incremento en las amenazas y los ataques dirigidos a organizaciones, combinado con una mayor exposición de los usuarios y activos han potenciado la evolución y crecimiento de los equipos CSIRT hacia una respuesta rápida cada vez más coordinada, si bien es necesaria más concienciación referente a las ciberamenazas emergentes en sectores tradicionales y en los nuevos sectores expuestos (ej. IoT)".

❷ "El cambio producido por la situación actual presenta un nuevo paradigma de ciberseguridad, donde los usuarios han pasado de un modelo centralizado en oficinas a un modelo distribuido, haciendo uso continuo de redes no 'securizadas' y dificultando las tareas de prevención, monitorización y respuesta, requiriendo la exposición a Internet de servicios anteriormente solo internos de las organizaciones. La adaptación de forma segura a este nuevo modelo será uno de los principales retos del nuevo año".

❸ "Estableciendo canales de confianza personales entre los equipos de respuesta de las organizaciones, que garanticen el uso adecuado y la confidencialidad de la información sensible intercambiada es un punto fundamental para motivar a las organizaciones a realizar estos intercambios de forma oportuna y efectiva, con el objetivo único de prevenir y contrarrestar las nuevas amenazas que afectan a todas las organizaciones.

En la actualidad, se está desplegando la Estrategia de Ciberseguridad Nacional; dentro de ésta aparece la figura del Foro Nacional de Ciberseguridad que para 2021 deberá tomar mucho peso. Sería interesante ver cómo integrar la figura de los CSIRTs".

BANCO SANTANDER

Thomas William Harvey

Global Head of Respond

❶ "Sí. La creciente frecuencia y magnitud de los ciberataques de los últimos años, y el enfoque de estar preparados, han llevado a un mayor protagonismo de la ciberseguridad en las estrategias corporativas. Existe una mayor inversión en tecnología y personal especializado para combatir el cibercrimen y prevenir su impacto reputacional, económico y operativo. La contratación y el desarrollo de perfiles especializados, la realización de ciberejercicios y las mejoras en automatización y colaboración son claves para preparar a las organizaciones para afrontar las amenazas más críticas".

❷ "Los grupos criminales son cada vez más sofisticados y el número de ciberataques está creciendo en todos los sectores, acarreando un aumento de presión regulatoria. A este reto se suman la falta de perfiles especializados del sector y las nuevas dinámicas de trabajo remoto y el entorno económico adverso post Covid-19. En 2021 tendremos que aumentar las capacidades de detección de nuevas técnicas y actores con especial dedicación e ingenuidad. Eso sí, como profesionales de la ciberseguridad tenemos una ventaja: estamos acostumbrados a trabajar bajo presión, con lo cual no dudo que lograremos sacar lo mejor de la situación".

❸ "En Santander creemos firmemente que el intercambio de inteligencia sobre ciberamenazas es clave en la lucha contra el cibercrimen. Participamos e impulsamos varios grupos de confianza a nivel sectorial e internacional, destacando nuestra estrecha colaboración con autoridades españolas, Europol, y el impulso de grupos de confianza a nivel europeo. En nuestra experiencia, la compartición franca, ágil y transparente aporta claros beneficios para todos los involucrados, ya sea en la respuesta a amenazas comunes como a incidentes de la cadena de suministro. Aún hay espacio para mejorar en algunos ámbitos, como la colaboración pública-privada, pero se están haciendo grandes avances".

BBVA

Alberto Rey García

Director Ejecutivo de Operaciones Globales de Ciberseguridad

❶ "La tendencia a implantar modelos de servicios gestionados que sustituyan a las tradicionales estructuras de subcontratación es ya imparable, porque soluciona muchos de los retos históricos del mercado de ciberseguridad y, singularmente, los del difícil acceso al talento y la falta de escalabilidad de los equipos dedicados a un solo cliente. La mayoría de las compañías apuestan por ese modelo y esa es, en mi opinión, la dirección adecuada, porque ayuda a contener costes sin comprometer calidad y mejorando el acceso a información de inteligencia. Dado este contexto, esperamos que en los próximos años/meses continúe desarrollándose una evolución positiva del papel de los proveedores de servicios gestionados, que permita alcanzar el grado de madurez óptimo como para adaptar sus ofertas a las necesidades particulares de sus clientes actuales y potenciales de una forma ágil y flexible".

❷ "El reto principal es claramente limitar el impacto de los incidentes más prevalentes en los últimos meses: los ataques basados en *ransomware*. Lamentablemente, esto no es alcanzable únicamente por la acción de los CERTs, sino que implica la revisión de las líneas de integración entre áreas tradicionalmente complementarias, como son las de infraestructura y la gestión de equipos de trabajo individual. Sólo alineando totalmente sus procesos de soporte conseguiremos una atenuación de este impacto a medio y largo plazo".

❸ "La compartición de información de inteligencia con las autoridades y entre empresas es un factor clave para combatir el cibercrimen de forma eficaz y eficiente. Así como los mecanismos de publicación de información de inteligencia desde organismos públicos a los privados están claros, quizá falten instrumentos verdaderamente útiles para que las entidades privadas den el paso de compartir de manera más decidida entre ellas. El intercambio de información de inteligencia únicamente será efectivo si se puede transmitir información de calidad de forma segura entre fuentes confiables y se garantiza que no existen obstáculos legales que impidan dicho intercambio. Sin embargo, las plataformas de intercambio de información existentes se basan en círculos exclusivos de confianza, algu-

nas de ellas impulsadas a nivel nacional, específicas del sector y, en ocasiones, con demasiada información, difícil de procesar y de obtener un beneficio real de la misma.
Existen tres variables que, en mi opinión, pueden influir en la capacidad de estos foros para convertirse en verdaderas comunidades abiertas y transversales: 1) *Confianza*. Cuanta mayor confianza exista entre las entidades, CERTS y demás, más fácil será que compartan información respecto a sus incidentes y mayor valor tendrán estos intercambios. 2) *Flexibilidad regulatoria*. El marco regulatorio debería incluir elementos de incentivo para la compartición de información, sobre todo en el contexto de incidentes e independientemente del impacto de los mismos. 3) *Tecnología*. Hasta hace poco no existían plataformas en las que compartir información sobre incidentes –ya fueran de pago u *open source*– que permitieran a una multiplicidad de entidades acceder a esta información, y aún hoy no existe un consenso sobre el estándar tecnológico a utilizar".

CAPGEMINI

Andrés de Benito
Head of Cybersecurity

❶ "Es una pregunta difícil de responder, ya que, por mucho que uno crea que se está haciendo bien, es el mercado el que dicta el veredicto final. De manera personal, sí creo que la fuerte especialización de los últimos años ha permitido tener equipos cada vez más ágiles y preparados, siendo fundamental seguir insistiendo en el conocimiento específico, no solo de los sistemas protegidos, sino también de los procesos de negocio que dichos sistemas soportan, aportando de esta manera un valor diferencial en la respuesta".
❷ "Aunque pueda parecer fuera de contexto, por ser algo exógeno a la ciberseguridad, afrontar las dificultades impuestas por el Covid y, en particular, el teletrabajo. Es cuestión de tiempo que empiecen a proliferar ataques aprovechando una mala implementación y control de las capacidades de trabajo remoto en las organizaciones que no han sabido o no han podido poner en marcha las medidas adecuadas a tiempo y que, ante la falsa sensación de seguridad por la relativa calma de que todo funciona, se llevarán alguna sorpresa tarde o temprano".
❸ "Es complicado convencer a las organizaciones de los beneficios de compartir cierta información. Tener acceso a información común es clave para la lucha contra los ciberdelincuentes y puede ser la diferencia entre una respuesta efectiva y precisa, y un desastre. Pero también es cierto que la información proporciona poder, y nadie quiere compartir según qué datos con empresas de la competencia. En este caso, es fundamental ser capaces de explicar los beneficios y que juntos se es más fuerte para derrotar a un enemigo que, al fin y al cabo, es común a todos. Las administraciones a nivel global pueden y deben hacer mucho en este aspecto, tanto por el poder que tienen, como para servir de ejemplo a las empresas, aunque ciertamente, si bien ya existen iniciativas, es un objetivo difícil de alcanzar".

CATALONIA–CERT

Xavier Panadero Lleonart
Director SOC/CERT
AGENCIA CATALANA DE CIBERSEGURIDAD

❶ "En líneas generales, podríamos afirmar que evolucionan al ritmo que sus necesidades particulares les plantean. En CATALONIA-CERT tenemos, desde ya hace tiempo, un equipo dedicado exclusivamente a medir el nivel de madurez de nuestras actividades para poder definir y priorizar la evolución necesaria que nos permita hacer frente a las nuevas amenazas a las que nos enfrentamos diariamente. Aun así, en muchas ocasiones no conseguimos evolucionar al ritmo que necesitamos (por condicionantes presupuestarios, procesos de contratación, problemáticas durante la implantación, resistencia al cambio, etc.) y, es por ello que, en este último año hemos apostado por la innovación para acelerar nuestra estrategia evolutiva. A modo de ejemplo cabe señalar el actual contexto generado por la pandemia que, en un abrir y cerrar de ojos, ha dibujado por completo un nuevo escenario de trabajo (teletrabajo, uso de equipos personales, exposición de sistemas internos, adopción de herramientas de colaboración, etc.), dejando obsoletos procesos y tecnología en materia de respuesta a incidentes y, en consecuencia, obligándonos a innovar para encontrar nuevas aproximaciones que se adecuaran a dicha situación (adquisición remota, automatización, gestión de crisis, contención en la nube, etc.)".
❷ "En 2021, tenemos como compromiso la construcción del servicio público de ciberseguridad donde, entre otros, la respuesta a incidentes jugará un papel determinante. Este servicio nos supondrá un reto ya que será necesario entender cómo aproximar la respuesta de incidentes a los diferentes destinatarios. Es evidente que esto tampoco podremos hacerlo con los procesos y herramientas existentes, por lo que será también parte del reto construir un modelo que permita satisfacer las necesidades de cada destinatario y, posteriormente, adoptar soluciones emergentes (asistentes virtuales, *chatbots*, etc.) para dar respuesta a nuestro ámbito de actuación".
❸ "Inicialmente cambiando la aproximación que actualmente existe de 'recibir a cambio de nada' y adoptar la de 'dar a cambio de nada'. Compartir información es clave para hacer frente a las amenazas globales, por lo que primero uno tiene que preguntarse qué información puede ofrecer para que los destinatarios de la misma puedan aprovecharla y estar así más preparados. Es necesario no tener recelos de que compartir información por algún motivo ira en su detrimento y adoptar medidas para que dicha compartición sea efectiva a la par que cumpla la normativa vigente.
En CATALONIA-CERT, adoptamos esta aproximación ya hace unos años y empezamos nuestra andadura compartiendo con nuestros homónimos la amenazas e incidentes críticos que gestionamos solo con el objetivo de que pudieran estar preparados. En este último año, hemos ampliado nuestro alcance, incluyendo a profesionales del sector y generando un ecosistema que potencie la confianza y la compartición. Durante 2020 hemos seguido trabajando en homogeneizar nuestra compartición mediante un programa específico (Threat Intel Program), que permita no solo compartir información sino conocimiento y tecnología".

CENTRO VASCO DE CIBERSEGURIDAD BCSC

Asier Martínez Retenaga
Responsable del CERT

❶ "Considero que aún queda un largo camino por recorrer. Existen modelos de madurez como SIM3, los cuales, permiten rápidamente autoevaluarse y mejorar las capacidades, pero que todavía no están ampliamente implantados. Así mismo, considero que el rol de los CSIRTs / CERTs no está lo suficientemente valorado, hecho que dificulta su evolución, y que se debería apostar más por dotarles de los recursos necesarios para prevenir y responder a los incidentes de ciberseguridad, algo que desafortunadamente no sucede en la mayoría de los casos".

❷ "Ante esta situación derivada de la pandemia, los CSIRTs / CERTs probablemente adquieran un mayor protagonismo, ya que para poder adaptarse las organizaciones han tenido que aplicar grandes cambios en poco tiempo y en muchos casos sin tener presente la ciberseguridad, por lo que previsiblemente se incrementará significativamente el número de incidentes. Por lo tanto, entiendo que el principal reto será hacer frente a un mayor volumen de incidentes con recursos limitados, es decir, se va a tener que hacer más con lo mismo o menos".

❸ "Independientemente de la gran cantidad y heterogeneidad de plataformas de ciberinteligencia o de compartición de amenazas, habría que fomentar una cultura de transparencia y compartición, junto con la utilización de estándares como STIX y TAXII. Así mismo, convendría invertir en la automatización de las tareas para ser más eficientes y poder compartir la información más rápido y mejor, y hacer así un frente común contra las ciberamenazas".

CIPHER

Jorge Hurtado
Vicepresidente EMEA

❶ "Creo que empieza a haber una saturación de este tipo de centros, y que muchas veces no responden al propósito original del término (Gestionar y Responder a Incidentes de Seguridad). La multiplicación de centros no ha venido acompañada de una mayor exigencia en las capacidades que deben tener, ni en la estandarización de procesos y terminología que cada uno de ellos utiliza. En general observamos CERTs con capacidades avanzadas, incluyendo estar a la vanguardia de la innovación en términos de respuesta, mientras que otros disponen de unas capacidades claramente insuficientes para ser considerados como tales".

❷ "En 2021 todavía persistirán las dificultades de la actual pandemia, y la necesidad de adaptar los actuales procesos a un modelo híbrido en el que se consolide el modelo de CSIRT distribuido que hemos vivido durante estos meses. El reto será cómo habilitar un modelo de CSIRT en el que la ubicación de las personas no implique menores medidas de seguridad y ciberseguridad, y que fomente un ambiente que consiga las mismas cuotas de colaboración y trabajo en equipo que un entorno 100% presencial".

❸ "Queriendo compartir, que desafortunadamente es una premisa de partida que no se da en la mayoría de los casos, ya que, en la actualidad, la mayoría de las informaciones que fluyen lo hacen de una manera informal y no reglada. Una vez exista esa voluntad, creo que es importante alinear y estandarizar la información mediante una taxonomía común, establecer mecanismos de 'anonimización' y establecer un foro de intercambio en el que poder hacerlo utilizando las tecnologías y protocolos que ya existen desde hace años".

COMUNIDAD DE MADRID
Consejería de Sanidad

Ángel Luis Sánchez García
Jefe de Servicio de Seguridad de Sistemas de Información (CISO)

❶ "En nuestro caso, al ser una AAPP, contamos con la inestimable colaboración del CCN-CERT, que evoluciona favorablemente según le permiten sus recursos. Con respecto a los CSIRTs, el SERMAS pertenece a CSIRT.es, donde se produce una necesaria colaboración público-privada entre los distintos CSIRTs españoles".

❷ "Es necesario contar con Centros de Análisis e Intercambio de Información Sectoriales, en nuestro caso especializado en el Sector Sanitario".

❸ "Contando también con esos Centros Sectoriales por los que ha apostado Europa y que llama ISAC (Information Sharing and Analysis Centers). En este sentido, conviene indicar que el SERMAS ya participa con Enisa en el proyecto de creación del European Health ISAC".

COMUNIDAD DE MADRID
Madrid Digital

Esther Muñoz Fuentes
Directora de Ciberseguridad, Protección de datos y Privacidad de Madrid Digital

❶ "Los equipos de respuesta a incidentes de seguridad CERTs/CSIRTs están evolucionando hacia una respuesta más eficiente y rápida ante el escenario de amenazas crecientes e incidentes de seguridad cada vez más graves y de mayor impacto. Esta es la evolución adecuada, y para que sea exitosa es clave el intercambio ágil de información sobre el ciclo completo del incidente, desde su detección hasta su erradicación, lo que permite también actuar en prevención".

❷ "La extensión del teletrabajo y la aceleración de los procesos de transformación digital de todas las administraciones públicas y empresas privadas durante este año, en respuesta a la situación de pandemia nacional, ha tenido como efecto negativo un incremento exponencial de ataques dirigidos a explotar debilidades y vulnerabilidades de seguridad, materializados en el aumento de

incidentes de seguridad en todas las organizaciones. Ante esta situación, la colaboración en la vigilancia continua de nuevas amenazas de seguridad, el intercambio ágil de información de incidentes entre organización y la respuesta coordinada pasan a ser el reto fundamental para el próximo año".

❸ "Uno de los obstáculos que frenan la compartición efectiva de información entre equipos de respuesta a incidentes, especialmente entre el sector público y el privado, es el recelo por el posible daño al sector o a la marca que puede derivarse si se intercambia información de un incidente de seguridad, olvidando una frase célebre de Robert Mueller "Solo hay dos tipos de empresas: las que han sido pirateadas y las que serán". Es primordial impulsar foros como CSIRT.es, creado para promover esta cooperación entre equipos en la respuesta a incidentes, donde se pueden intercambiar experiencias entre todos los sectores productivos nacionales".

CSIRT–CV (GENERALITAT VALENCIANA)

Lourdes Herrero

Directora

❶ "En líneas generales sí, aunque hay dos aspectos claramente mejorables. El impacto que ha producido la pandemia del Covid-19 en las estructuras de servicio de estos Centros, era algo difícil de prever y de dimensionar. En este sentido, aunque la cualificación técnica de los equipos que los componen sea alta y acorde con los desafíos técnicos a los que tenemos que hacer frente, es claramente insuficiente en número. La escasez de técnicos altamente cualificados que veníamos sufriendo en años anteriores no ha hecho más que agravarse y el desequilibrio entre la oferta y la demanda es cada vez mayor. El otro aspecto a mejorar sería la falta de autoridad dentro de nuestros respectivos ámbitos que, de haber sido mayor, algunos de los incidentes graves que han ocurrido este año se hubieran podido evitar".

❷ "La sofisticación cada vez mayor de los ataques, las amenazas derivadas del aumento de la superficie de exposición que nos trae la generalización del teletrabajo, la adaptación de la vigilancia a las nuevas soluciones *on-cloud* con nuevas fuentes a monitorizar, junto con la mencionada escasez de personal en los CERTs, conforman un panorama complejo para los equipos de respuesta ante incidentes.

Si a ello unimos el hecho de que la ciberseguridad aún se considere un mero ornamento y no una parte esencial de las estrategias corporativas en algunas organizaciones, y que todavía no se tengan en consideración suficiente las directrices de ciberseguridad emanadas desde sus CERTs correspondientes, podremos entender fácilmente que el principal reto para 2021 sea conseguir el "full authority" en nuestros respectivos ámbitos. ¡Hazte oír! debería ser el reto para 2021".

❸ "Los esfuerzos de algunos de los CSIRTs más veteranos en el pasado para mejorar la compartición de información entre nosotros no han sido en vano y se han materializado en que dispongamos desde hace una década del Foro Nacional CSIRT.es, cuya forma y estructura, –aunque mejorables–, facilitan tal propósito. Iniciativas de compartición e intercambio de información como la que se ha puesto en marcha desde el Foro Nacional de Ciberseguridad –del que CSIRT.es ya forma parte–, pueden contribuir también a ello, así como el ofrecimiento por parte del CCN-CERT de asumir su secretaría permanente y la renovación del comité de dirección de CSIRT.es, que se han visto ambas retrasadas por la pandemia".

DELOITTE

César Martín Lara

Socio Risk Advisory Cyber

❶ "En España tenemos una red de CSIRTs / CERTs de primer nivel que evoluciona adecuadamente adaptándose diariamente a las nuevas amenazas".

❷ "El principal reto de un CSIRT / CERT es el de ser capaz de aportar a un cliente respuesta rápida en detección de amenazas y contención de incidentes. Las amenazas evolucionan constantemente pero el reto permanece".

❸ "Ya existen plataformas y mecanismos potentes de compartición de información entre CSIRTs / CERTs. La mejora de la información compartida no reside en el mecanismo sino en la calidad de la información que se comparte, y es por esa vía por donde se debe trabajar en mejorar la información que se comparte".

ENTELGY INNOTEC SECURITY

Myriam Sánchez

CERT-CSIRT | Responsable de Cyber Threats

❶ "Depende de la organización. En el caso de la nuestra hemos ido mejorando las capacidades de las soluciones clásicas, al tiempo que se ha apostado por ofrecer nuevos servicios para mejorar la Seguridad. No obstante, en otros muchos casos se ha evolucionado; pero no al ritmo que exige este sector. Las limitaciones presupuestarias y de recursos dificultan la ejecución de un plan realista de evolución adaptado a los riesgos a los que nos enfrentamos todos los días".

❷ "En general, el principal reto al que se enfrentan los equipos CSIRT / CERT de las organizaciones es adecuarse continuamente a la rápida evolución de las amenazas. Además, en el contexto de esta pandemia, con la implantación del teletrabajo de manera generalizada y la digitalización de los servicios cotidianos, el reto es aún mayor. Todo ello, unido a la necesidad de controlar las graves amenazas que están golpeando a muchas organizaciones, como el *ransomware* o el ciberespionaje".

❸ "En los últimos años ha habido una importante evolución en las plataformas de compartición de información y los esquemas comunes que permiten que esta pueda realizarse de manera ágil y eficiente. Sin embargo, en muchas ocasiones, el verdadero hándicap radica en la calidad de la información que se comparte. Para poder hacerlo es necesario dedicar recursos (personales, técnicos, tiempo...) que, desgraciadamente, son muy escasos en las organizaciones. Hay que tener en cuenta que compartir información de calidad representa un gran esfuerzo de diferentes

equipos que doten de contexto a dicha información para que pueda ser útil. Esta situación dificulta en gran medida la compartición desinteresada de los indicadores, excepto en entornos más acotados. Al final debemos conseguir un "quid pro quo" en el que todas las partes salgan beneficiadas de dicho intercambio. Iniciativas como el grupo CSIRT.es, a nivel nacional, o el FIRST, a nivel internacional, y en los que estamos integrados desde sus orígenes, son muy importantes y favorecen la compartición de la información".

GMV

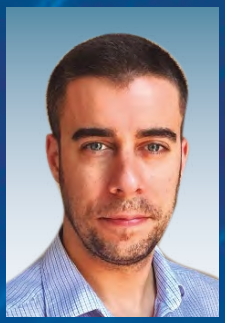
Óscar Riaño

Responsable de GMV-CERT

❶ "Las capacidades estándares se encuentran razonablemente cubiertas y evolucionan adecuadamente, si bien dada la situación actual, la evolución diferencial se centra en la incorporación de capacidades de investigación del contexto tales como NSM y EDR, que permiten la realización de dictámenes ágiles ante una situación de alerta".

❷ "La situación actual nos ha abocado al teletrabajo y a la 'remotización' de servicios. Uno de los retos para el 2021 es la extensión de dichas capacidades de investigación hacia entornos híbridos, así como avanzar en la consolidación de una base de conocimiento esencial para sacar el máximo provecho a los servicios gestionados".

❸ "Es fundamental asegurar la confiabilidad de las partes implicadas en los distintos foros en donde se gestione/comparta la información con la finalidad de garantizar un uso adecuado de la misma. Habría que establecer mecanismos de compartición/restricción acorde al grado de cooperación de las organizaciones/países en los procesos de investigación de incidentes de seguridad".



GRUPO BANCO SABADELL

Oriol Navarro

Global Incident Response Manager

❶ "La complejidad actual de las amenazas, así como el número de incidentes con impactos graves en organizaciones relevantes, hace necesaria la constante evolución y capacitación de los CERTs / CSIRTs. Las organizaciones están realizando un esfuerzo en esta dirección, y se observa una madurez mayor tanto en el mercado de soluciones tecnológicas como de profesionales cualificados. Aun así, esta apuesta debe ser constante e incremental para estar preparados frente a la evolución de los ataques actuales".

❷ "Mencionaría dos retos principales. Por un lado tenemos la necesidad de seguir adaptando las capacidades de respuesta a los nuevos entornos (nubes híbridas, entornos de trabajo remoto, etc.) que rompen con el paradigma tradicional de la delimitación de la información contenida en sistemas en los propios centros de datos de la organización. Por otro, la integración de tecnologías que nos ayuden a mejorar la detección de incidentes entre el 'ruido' de datos actual, y que nos ayuden en la automatización de las capacidades de respuesta.

❸ Actualmente existen numerosos foros de compartición de información: sectoriales, privados, públicos, etc. En esta profesión existe una cultura de la compartición de información y compañerismo que facilita nuestras labores. El reto es conseguir hacer operativos estos foros con los diferentes niveles de detalle que las organizaciones están dispuestas a permitir divulgar. El riesgo reputacional es un factor a tener en cuenta en estos casos".

GRUPO ICA

Alberto Cañadas Álvarez

Gerente de Preventa y Desarrollo de Negocio de Ciberseguridad

❶ "La tendencia que vemos es la proliferación de CERTs / CSIRTs en estos últimos dos años. Sin embargo, la especialización de los servicios y la búsqueda continua de plataformas innovadoras y sofisticadas que se integren en los procesos de ciberseguridad, es el camino a seguir: personas y plataformas para prestar un servicio de excelencia a todas las empresas, desde el Corporate a la PYME".

❷ "El principal reto para 2021 es la automatización y orquestación de los servicios prestados y la integración de todos ellos con la inteligencia de amenazas interna y externa de ciberseguridad, así como la compartición de información de calidad y en tiempo real entre las entidades privadas y públicas".

❸ "La confianza entre los CSIRTs / CERTs privados y los públicos debe ser máxima, con un único objetivo: la seguridad nacional. Para ello, hay que organizar y fomentar dicha compartición de inteligencia de amenazas, teniendo en cuenta las diferentes motivaciones público-privadas".

GRUPO OESIA

Omar Orta

Director de Transformación Digital

❶ "Los equipos de respuesta a incidentes de seguridad, a nivel general, han evolucionado los últimos años de manera importante, en parte, gracias a la organización de los Foros de CERT / CSIRT a nivel mundial que sirven de espacio para que estos profesionales puedan colaborar y compartir información. Y, por otro, de las inversiones que realizan las organizaciones y gobiernos para garantizar que se disponga de la tecnología, personal y procesos necesarios para garantizar la seguridad del ciberespacio".

❷ "Por un lado, tenemos el reto de preparar nuevos profesionales de ciberseguridad que sean capaces de dar respuesta a los nuevos, diversos y cambiantes tipos de ciberataques que suceden continuamente, por otro, el reto será hacer seguro

el 'nuevo perímetro', es decir, el usuario, todos los que estamos en el mundo de ciberseguridad tenemos la responsabilidad y el deber de concienciar a los ciudadanos para generar un entorno de resiliencia en materia de ciberseguridad y construir un ciberespacio seguro para todos".

❸ "Creo que deben potenciarse y crearse nuevos espacios público-privados, principalmente, para generar *know how* que dé respuesta a las amenazas de ciberseguridad que se generan a diario en el ciberespacio, tanto a nivel local (entendiéndose por países) y globales".

GUARDIA CIVIL

Col. Juan Salom Clotet

Jefe de la Unidad de Coordinación de Ciberseguridad

❶ "La Guardia Civil no cuenta con un CSIRT propiamente dicho. No obstante, sí que es cierto que varias de nuestras Unidades, por la propia idiosincrasia de su trabajo, realizan funciones que bien podrían identificarse como propias de un CSIRT, principalmente en el ámbito de la concienciación de nuestros "clientes" –en este caso de la ciudadanía–, pero también algunas otras de carácter más técnico, y que desarrollamos en el marco de nuestras investigaciones".

❷ "El contacto y el intercambio de información con los CSIRTs resulta sin duda fundamental para el desempeño de nuestra misión. El creciente impacto económico del cibercrimen, la cada vez mayor dificultad técnica que entraña su investigación y eventos como el de *Wannacry* y *NotPetya* que vivimos hace unos tres años, son algunos de los factores que aconsejaron un acercamiento y un estrechamiento de las relaciones entre las capacidades de respuesta técnica y las Fuerzas y Cuerpos de Seguridad que, a nivel nacional, en el caso de Guardia Civil se materializó a través del Foro CSIRT.es.

El Foro CSIRT.es, del que Guardia Civil forma parte, está compuesto por los principales equipos de respuesta a incidentes españoles. Pertenecer a este foro nos permite una interlocución directa y fluida con todos los miembros de esta comunidad tan importante para nosotros y con la que, a pesar de tener diferentes objetivos, compartimos roles complementarios y la obligación de colaborar. Por nuestra parte ofrecemos a los miembros de la comunidad CSIRT un punto de contacto permanente al que acudir en busca de asesoramiento en aspectos relacionados con las investigaciones de ciberdelitos".

❸ "Los retos a los que nos enfrentamos están siempre relacionados con la mejora de los procesos de comunicación e intercambio de información. La forma de enfrentar estos retos tampoco es novedosa, y suele pasar por evitar la duplicación de esfuerzos, aumentar la rapidez de los intercambios, generar confianza entre las distintas partes, simplificar y estandarizar procesos, realizar actividades de manera conjunta, utilizar un lenguaje común, promover una cultura de intercambio de información, etc. Sin duda todos estos ámbitos son susceptibles de ser mejorados de manera continua y en esa línea seguirá trabajando la Guardia Civil en el futuro".

INGENIA

Carlos Cortés Danta

Gerente de Negocio – Ciberseguridad y Servicios Gestionados

❶ "El creciente número de amenazas y las necesidades cada vez más exigentes en materia de ciberseguridad están propiciando una clara evolución del papel que desempeñan los CERTs / CSIRTs, en mi opinión, dando pasos en la dirección adecuada, aunque la velocidad de adaptación siempre podría ser mayor. Han ido ampliando el catálogo de servicios prestados para potenciar el desarrollo de actividades más relacionadas con la defensa y protección proactivas, asumiendo que deben cubrir también mecanismos de ciberinteligencia, alerta temprana, detección, acciones de formación y concienciación, además de las capacidades originales relacionadas principalmente con la respuesta a incidentes".

❷ "La hiperconectividad, el 5G, una mayor complejidad y heterogeneidad de la tecnología, la aceleración de la transformación digital y la adopción masiva de la nube, así como el fomento del teletrabajo, suponen desafíos actuales que se mantendrán en 2021 y que obligarán a los CERTs / CSIRTs a potenciar el desarrollo de capacidades para prevenir y anticiparse a un incidente. Esto incluye el análisis de grandes cantidades de información sobre amenazas para extraer tendencias y para modelar patrones de ataque que ayuden a conseguir un mayor conocimiento del entorno cambiante al que nos enfrentamos y que nos permitan desarrollar estrategias de respuesta adecuadas".

❸ "Me gustaría resaltar dos puntos de mejora principales. Por una parte, seguir promoviendo y favoreciendo plataformas para la asociación de los distintos Centros, como CSIRT.es a nivel nacional o FIRST a nivel global y, por otra, continuar con la estandarización de los mecanismos para compartir la información normalizada, de forma que sea consumible por toda la comunidad y grupos de interés, potenciando así su análisis automático para poder actuar de forma colaborativa, eficaz y coordinada".

INETUM

Simón Cordero

IRT Manager

❶ "En España hemos presenciado un avance significativo en el número y en la evolución de estas entidades, tanto en el ámbito público como en el privado. Sin embargo, dependiendo del ámbito, y desde mi punto de vista, considero que aún es necesario seguir avanzando hacia niveles de mayor madurez. Estos avances pasan por mejorar la compartición de la información (pero la información necesaria, no la 'infoxicación' que podría tener lugar si se comparte todo) para tener una gestión eficiente en la respuesta a los incidentes".

❷ "Terminar de asentar las bases que, debido a la pandemia que estamos sufriendo, se han establecido a la hora de realizar trabajos de respuesta a incidentes desde los diferentes CERTs. Además, tendremos que adaptarnos a que la protección no sólo pasa por el entorno empresarial, sino también por aumentar la concienciación de los usuarios sobre los aspectos de ciberseguridad. En esto, los CERTs / CSIRTs podemos colaborar con nuestras compañías, ya que somos sus equipos de respuesta y nos estamos enfrentando a estas situaciones".

❸ "Creo que debemos avanzar hacia una mayor compartición de información sobre ciberataques, especialmente, incidiendo en la necesidad de derribar la barrera de la 'vergüenza' que supone para las empresas verse afectadas por este tipo de incidentes. Para ello, la labor clave a desempeñar entre organizaciones y los CERTs / CSIRTs gira en torno a la puesta en marcha de buenas prácticas compartidas y lecciones aprendidas, pero no solo con la propia compañía, sino con el resto de CERTs. En esa labor, nos pueden ayudar, y nos ayudan, los CERTs públicos de referencia que hay en España".

INTEC

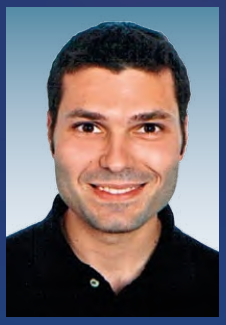
Juan José Fuster

CEO

❶ "Sí, se está evolucionando adecuadamente. Hay que tener en cuenta que siempre vamos detrás de los delincuentes, lo que nos ha obligado a ser más proactivos y creativos para poder predecir cómo serán los próximos ataques, los cuales, cada día son más sofisticados técnicamente. Ello implica una inversión muy fuerte en I+D y en la atracción de talento en la materia para poder diseñar sistemas más proactivos para evitar incidentes y mejorar toda la parte reactiva a fin de poder detener lo antes posible los ataques que sucedan. A nuestro parecer está fuertemente condicionado a que operamos desde nuestro propio SOC, que está continuamente mejorando para poder estar al día en las últimas TTPs".

❷ "No hay un reto concreto para el año 2021, es el mismo de siempre: poder disponer de sistemas que permitan anticiparse a los incidentes y detener los que ocurran a la mayor brevedad posible, lo cual abarca distintas áreas de trabajo dentro de un CSIRT: mejorar el modelado de amenazas, mejorar la inteligencia de los sistemas para identificar etapas de la *killchain* de un ataque, contar con una coordinación interna más eficiente en la respuesta a incidentes…"

❸ "En la actualidad, existen organismos como el FIRST o el TF-Introducer, a nivel internacional, o el CSIRT.es a nivel nacional, para que los CSIRTs compartan información. Una mejora sería facilitar la entrada en estos organismos a otros CSIRTs reduciendo la burocracia que implica el darse de alta, además de permitir que otros actores/*stakeholders* del sector pudiesen formar parte".



ITS BY IBERMÁTICA

Miguel Tubía

Responsable de Operaciones Ciberseguridad-CERT

❶ "En los últimos años hemos sido testigos de una gran proliferación de CERTs / CSIRTs, tanto públicos como privados. Esto ha ayudado a consolidar un ecosistema de ciberseguridad en el panorama nacional y a establecer una comunidad cada vez mayor y más conectada, de la que nuestro CERT (ITS CERT/SOC) es miembro activo. Como consecuencia directa, las empresas tienen más conocimiento de ciberseguridad, aumentan las capacidades competitivas de estos centros y la compartición de información y herramientas en la comunidad".

❷ "Distinguimos dos grandes retos en ciberseguridad para el 2021: las llamadas Amenazas Avanzadas Persistentes (APT por sus siglas en inglés), y la concienciación de usuarios finales. Las APT cada vez son más sofisticadas, y, al tratarse de ataques dirigidos, complicados de detectar. En este punto, no cabe duda de que la concienciación de usuarios resulta imprescindible debido a que la mayor parte de los incidentes se han realizado por descuidos humanos o malas prácticas".

❸ "Existen ya iniciativas en grupos nacionales que persiguen una mayor calidad en la información compartida. Por otro lado, ya se está trabajando en un estándar para arquitecturas de sistemas de compartición de información. La estandarización y normalización de esta práctica y la implicación y colaboración altruista de los diferentes CERTs / CSIRTs, deben ser los motores que permitan mejorar el flujo de información entre los centros".

JUNTA DE ANDALUCÍA

Eloy Rafael Sanz Tapia

Gabinete de Seguridad y Calidad

Unidad de Seguridad TIC

❶ "Por desgracia, la rapidez con la que evolucionan las técnicas usadas por los cibercriminales y su sofisticación hacen que el mundo del cibercrimen y el fraude *online* avancen más rápido de lo que evolucionan los recursos dedicados a luchar contra ellos. El incremento de madurez en los procesos de gestión de incidentes, la adopción de nuevas tecnologías para la detección y la respuesta y la colaboración eficiente son claves para seguir la carrera".

❷ "Sin lugar a dudas el nuevo entorno de teletrabajo masivo derivado de la pandemia. Debe abordarse el correcto bastionado y monitorización de las conexiones VPN, el control de acceso a sistemas corporativos desde equipos domésticos y la concienciación de los usuarios y su promoción a 'última red de defensa'. Esto último con especial interés, ya que los cibercriminales están aprovechando esta situación en la que estamos inmersos para lanzar campañas maliciosas contra usuarios finales".

❸ "Potenciando la actividad de ciertos foros nacionales e internacionales, como CSIRT.es, FIRST o TF-CSIRT, promoviendo reuniones periódicas de sus miembros, patrocinando la organización de congresos de seguridad y creando grupos de trabajo para avanzar en ciertos aspectos concretos de la seguridad".

LIGHT EYES

Joel Araujo
CTO

❶ "Los equipos de respuesta a incidentes han ido creciendo en número y se han adaptado a las nuevas amenazas que han ido surgiendo y surgirán. A nivel internacional, los CSIRTs están evolucionando adecuadamente, pero aún hay mucho trabajo por delante. Sobre todo, dentro de este contexto de inestabilidad que dificulta el orden y la metodología".

❷ "El principal reto para 2021 seguirá viniendo de una falta de adaptación de las empresas e instituciones. Muchas entidades no están preparadas contra los ataques dañinos de las organizaciones criminales del ciberespacio. Será todo un reto tanto para los equipos de respuesta a incidentes como para los departamentos técnicos, concienciar y aplicar las correspondientes medidas de seguridad en un tiempo menor de lo esperado".

❸ "La compartición de información sigue o ha de seguir los estándares según la sensibilidad de los datos. La clave sigue estando en la seguridad que nos proporciona el cifrado, la rapidez en la que los CSIRTs se comunican y la correcta clasificación de esa información. La mejora de la compartición de cada vez más información deberá venir acompañada de tecnologías de Big Data, así como del procesamiento de los datos con IA y otras tecnologías que mejorarán la seguridad y la autenticidad de esa información. El reto de estas mejoras será el consenso de equipos que provienen de diferentes regiones y pensamientos distintos".

MNEMO

Fernando García Vicent
Director Operaciones

❶ "En Mnemo pensamos que los pasos que se están dando globalmente son correctos. Existe una concienciación global por parte de los CSIRTs / CERTs para evolucionar haciendo frente a las nuevas amenazas de atacantes cada vez más organizados y fuertes. Es necesario crecer en la especialización, utilización eficiente de las tecnologías disponibles y mejora en los procesos de anticipación a los ataques".

❷ "Para nosotros los retos principales son una mejor preparación para el conocimiento y anticipación a los ataques por todo tipo de *malware* –en especial *ransomware*–, una mejor capacidad organizativa y de reacción ante los incidentes de seguridad de muy alta complejidad, y una profundización muy importante en procesos de inteligencia para mejorar los sistemas de prevención, detección y alerta".

❸ "Cualquier mejora en la compartición de información y aumento de la colaboración entre los CSIRTs / CERTs es importante. Yo destacaría la relevancia de la colaboración entre proveedores y organismos públicos cuando se está en medio de un proceso de respuesta a un incidente grave en una organización en la que pueden estar involucrados varios actores con distintas responsabilidades y servicios".

POLICÍA NACIONAL

José Antonio Fernández Molina
Jefe del Servicio de Seguridad TIC. SOC

❶ "Atendiendo a los últimos incidentes de seguridad recogidos en prensa, la sensación es que no vamos suficientemente rápidos. Pero si miramos dos años atrás y comparamos los recursos actuales con los que contábamos, el salto es abismal".

❷ "Disminuir la superficie de exposición a las amenazas y aumentar la madurez en los procedimientos para afrontar la recuperación de los sistemas en el menor tiempo posible".

❸ "La solución Reyes del CCN-CERT, basada en la tecnología MISP, vertebra nuestra forma de compartir información de ciberamenazas. La implantación de esta tecnología en el mayor número de actores sería una mejora que revertiría en la ciberseguridad de todos".

RENFE

José Carlos Sánchez Dolado
Jefe de Ciberseguridad
Dirección de Transformación Digital y Tecnología

❶ "Personalmente creo que los equipos de respuesta a incidentes (CSIRTs) evolucionan en la medida en que se van generando nuevas amenazas; y estas cada vez son más sofisticadas. Todo esto hace que la preparación de los CSIRTs vaya evolucionando y perfeccionando ante las ciberamenazas".

❷ "El impulso de utilización y automatización de herramientas SOAR, al permitir a las organizaciones recopilar un mayor volumen de datos, tanto externos como internos, y poder procesarlos de una manera mucho más rápida y precisa. Todo esto va a permitir a los CSIRTs / CERTs una toma de decisiones mucho más rápida, inteligente y con mayor información".

❸ "Lo ideal e interesante seria la transparencia a la hora de compartir información sobre los ciberincidentes sufridos, y poder dar un apoyo desinteresado entre los distintos miembros de la organización (ejemplo CSIRT.es) a la organización que se vea afectada y solicite ayuda como consecuencia de haber sufrido un ciberincidente muy grave".

S2 GRUPO

José Miguel Rosell

Socio

❶ "Los CERTs, en general, no están evolucionando al ritmo de la ciberdelincuencia, el ciberespionaje o la ciberguerra. Se observa, en muchos casos, una actitud reactiva y muy poco especializada contra las actividades ilícitas que desarrollan los equipos de ciberdelincuentes o los ciberejércitos. Es necesario tomar la delantera mediante la respuesta de centros especializados en ciberseguridad y una decidida apuesta por la innovación y la investigación y desarrollo que les permita, incluso, el desarrollo de herramientas propias y capacidades para estar a la altura de las circunstancias. El problema es que no todo lo que lleva la etiqueta de CERT o CSIRT es realmente un centro especializado de ciberseguridad".

❷ "Crecer en capacidades sin crecer en recursos humanos. Sin duda es necesario que seamos capaces de hacer que nuestros centros de operaciones de ciberseguridad utilicen más y mejor la tecnología y, si puede ser tecnología europea, mucho mejor. Necesitamos independencia tecnológica en Europa que nos permita asegurar nuestra forma de entender la convivencia y los derechos de las personas, y esto no lo vamos a conseguir utilizando de forma masiva servicios o tecnología de terceros países que entienden los derechos fundamentales de forma completamente distinta a la de Europa".

❸ "Desde luego es un tema muy complejo; pero a la vez muy necesario. Es importante que la compartición de información entre centros de operaciones de seguridad se desarrolle en un ambiente de confianza real. Decirlo es una cosa, hacerlo otra completamente distinta. Para mantener ese 'ambiente' necesario de confianza debería evitarse la participación, directa o indirecta, en la gestión de este tipo de actividad, de actores que buscan el beneficio propio, ya que estamos hablando de una actividad de interés público. En mi opinión esta compartición de información debería estar liderada y gestionada por centros públicos neutros de prestigio sin participación privada, pero con colaboración privada. Los ISAC sectoriales liderados o impulsados por entidades públicas podrían ser una solución interesante, aunque el hecho de ser sectoriales les priva de parte de la información. Iniciativas como CSIRT.es, lideradas por organismos públicos, pueden actuar como punto de encuentro y compartición de información de los ISAC".

S21SEC

Ignacio Paracuellos

SOC Manager Spain

❶ "La evolución de los CERTs / CSIRTs podría ser más completa. Sin embargo, existen esfuerzos e iniciativas no públicas en la línea de la mejora y adecuación a la realidad de la respuesta a incidentes. Hay una tendencia fuerte en tres direcciones: 1) Adaptación de los servicios de monitorización y detección al mapa de riesgos específicos de cada empresa y de las condiciones particulares de sus negocios; 2) Integración de inteligencia de amenazas para poder anticipar futuros ataques –conociendo metodologías y técnicas de ataque que utilizan los ciberdelincuentes en la actualidad–; y 3) Mejora de las capacidades y protocolos de respuesta a incidentes para acortar tiempos de respuesta y conseguir minimizar la posibilidad de que el ataque afecte a más sistemas o genere más daños".

❷ "La evolución del teletrabajo, tanto desde el punto de vista de foco de incidentes como desde el punto de vista de integración de los miembros de los equipos CSIRT. El teletrabajo es tanto un nuevo vector de ataque, con usuarios conectados en redes no completamente asegurables desde un punto de vista empresarial, como un reto para la operativa de los CSIRTs, que tienen que gestionar la dispersión geográfica de parte de sus equipos sin afectar a eficiencia y seguridad".

❸ "Más allá de la completa adopción de herramientas de intercambio de información, y la integración de los distintos equipos, es imprescindible la potenciación de equipos de trabajo inter-empresariales donde, en un ámbito de completa confidencialidad, se compartan experiencias e iniciativas que nos hagan a todos más fuertes. Sigue habiendo un conflicto entre la ciberseguridad como un esfuerzo compartido entre estados, instituciones y empresas –tanto usuarios finales como proveedores de ciberseguridad– y la ciberseguridad como área de actividad o negocio que tiene su propia estructura de costes y necesidades para financiarse y seguir operando. Este conflicto lleva a que la compartición de la información sea apoyada por todos a nivel teórico, pero no sea llevada a la práctica completamente. Dado el carácter estratégico de la ciberseguridad para cualquier nación, quizá la solución pasaría por la creación de marcos de colaboración regulados que contemplen la necesidad de financiar la investigación, el desarrollo de capacidades de detección de amenazas y ciberinteligencia y otros aspectos operativos clave para la industria de la ciberseguridad".

SECURE & IT

Francisco Valencia

CEO

❶ "En general, sí. Cada vez existe más oferta y más profesionalizada. La tipificación de incidentes de seguridad y los CERTs gubernamentales en toda Europa están ayudando mucho a este desarrollo. En el lado contrario, creo que también están apareciendo compañías que anuncian este tipo de servicios sin disponer de la capacidad suficiente, generando desconfianza en el sector".

❷ "Principalmente dos: por un lado, la captación y retención de talento especializado que de soporte en los CERTs / CSIRTs y, por otro, la sensibilización en las organizaciones de la idoneidad de contar o implantar un servicio especializado en respuesta a incidentes. Esto obliga a reconocer la probabilidad de incidentes y brechas de seguridad, aspecto que aún cuesta reconocer en las organizaciones".

❸ "Ya existen asociaciones y *hubs* creados para ello, pero una gran medida sería la creación de protocolos y estándares para el intercambio de Indicadores de Compromiso entre los mismos, por ejemplo, mediante sitios centrales donde podamos reportar y consultar estos indicadores".

SIA

Roberto Pérez
Head of Managed Security Services Business

❶ "Claramente, sí; nuestro nivel de madurez está incrementando significativamente, tanto a nivel español, como en particular de SIA, quedando lejos nuestros inicios al comienzo de los años 2000. De acuerdo a los datos publicados por ENISA, España es el primer país de la UE en número de CERTs (54 en España, de un total de 399 equipos en la UE).
Somos un referente en este tipo de equipos. La realidad actual del cibercrimen nos empuja a abordar servicios orientados a maximizar las capacidades de detección y respuesta ante incidentes, con un enfoque 360º, es decir, con un ojo puesto en las amenazas internas y otro en las externas; servicios adaptados a la realidad de cada cliente y en los que, al mismo tiempo, se automatiza y orquesta para conseguir que todas las alertas se traten, y los tiempos de detección, investigación y respuesta sean lo más bajos posible. Y, por supuesto, como no puede ser de otra forma en SIA al formar parte del grupo Indra, la mayor empresa tecnológica de nuestro país, apostamos por CSIRTs tanto en los entornos IT como para la protección de los sistemas industriales (OT)".

❷ "Todos los expertos y analistas coinciden en que el número de incidentes va a seguir creciendo. Es, sin duda, algo que obliga a poner foco en prepararse para los incidentes de seguridad que se puedan sufrir. En este sentido, es fundamental el Plan de Continuidad de Negocio. Es importante que esté definido y probado antes de que se produzca la crisis, incluyendo escenarios para ataques de tipo *ransomware*. E igual de importante es tener definida la estrategia de recuperación, con dos objetivos: evitar que haya improvisación y que los equipos de trabajo se desgasten más de lo imprescindible, y que los tiempos en la recuperación sean los menores posibles. Algunos de los mecanismos más efectivos para prevenir y proteger de este tipo de ataques son los relacionados con la gestión de identidades, accesos y cuentas privilegiadas y 2FA. Toma también especial relevancia la concienciación de usuarios y empleados.
Y por último, deben considerarse la protección del puesto de usuario (virtual y físico), que a raíz de la Covid-19 es el nuevo perímetro, y del *datacenter* (virtual, *cloud* o físico); la protección de los vectores de entrada clásicos, si no lo están ya (*email*, navegación web y conexiones con terceros), con un enfoque de arquitecturas Zero Trust; la prevención de incidentes con actividades que evalúen los vectores físico, lógico y social –*Red Team*–, seguridad en el ciclo de vida del *software*, y la gestión de Controles Técnicos); la detección avanzada de amenazas internas y externas; y finalmente la Respuesta basada en un equipo con experiencia que aborde las crisis con garantías".

❸ "Compartir información no es sencillo porque existen acuerdos de confidencialidad que debemos respetar. Pero una vez que se ha salvado este aspecto, la información se comparte con las personas, organizaciones y foros con los que se tiene confianza y relación. Por tanto, me parece fundamental buscar mecanismos para potenciar estas relaciones. Los foros como FIRST, TF-CSIRT, CSIRT.es, APWG, etc., de los que formamos parte, disponen de medios para compartir información de amenazas que puedan afectar a los socios o a sus clientes".

SOTHIS

Miguel Monedero
Director de Seguridad de la Información
UNE Consultoría y Sistemas de la Información

❶ "Nuestra percepción es que existe una evolución aceptable de los principales CERTs / CSIRTs, que constantemente invierten esfuerzos en ampliar sus capacidades de detección y reacción, incorporando nuevas técnicas como *Threat Hunting* o aplicando la filosofía Zero Trust. Debemos considerar que los cibercriminales invierten enormes recursos en evolucionar las técnicas, tácticas y procedimientos que utilizan para comprometer la información de las organizaciones y actualmente existe una importante brecha entre la inversión que una organización puede asumir para contrarrestar dichas amenazas y la que una organización criminal invierte".

❷ "Uno de los principales retos por resolver en 2021 será la capacidad de inversión de las organizaciones, actualmente estamos viviendo una época en la que los recursos de las compañías se verán afectados en gran medida debido a la pandemia mundial que estamos sufriendo; un hecho que sin duda tratan de aprovechar los ciberdelincuentes. Por ello debemos afrontar esta realidad y realizar un esfuerzo pensando en mejorar los sistemas de seguridad y adecuarlos a las nuevas necesidades y riesgos futuros de ciberseguridad. El crecimiento de los ciberataques que venimos observando en los últimos meses muestra una tendencia alcista que, con toda probabilidad, continuará en 2021. Por ello, será vital adecuar, madurar, automatizar y optimizar los procesos de ciberseguridad de las organizaciones; la eficiencia de nuestros procesos será fundamental durante el próximo año".

❸ "Para luchar contra el cibercrimen es de vital importancia la colaboración entre equipos de detección y respuesta a todos los niveles. Por ello, consideramos que fomentar foros de colaboración como CSIRT.es o FIRST permite compartir conocimiento y, por lo tanto, responder eficientemente ante una amenaza de seguridad. Además, inherente a estos foros, es importante la utilización de plataformas de compartición de información de ciberseguridad, donde se comparte tanto información a tiempo real como reglas Yara, indicadores de compromiso (IoC) o muestras de *malware*".

TELEFÓNICA, S.A.

Pedro Hernansáez Liarte
Gerente del CSIRT Global

❶ "Efectivamente, se está reforzando la función de los CSIRTs, tanto en el ámbito privado como en el público, porque la realidad del día a día de los incidentes nos ha forzado a evolucionar y también para dar soporte a las normativas que afectan a la gestión de incidentes de seguridad. Una vez asumido que los incidentes van a ocurrir, cada vez están cobrando más relevancia los CSIRTs para reforzar la detección y respuesta".

❷ "Uno de los principales retos es la automatización, tanto para el enriquecimiento de la información de contexto de las amenazas detectadas como para la respuesta. Por esto durante 2021 se incrementará el uso de plataformas SOAR. Otro reto es la armonización de las normativas de manera que queden más claras las obligaciones regulatorias de los CSIRTs".

❸ "Es necesario dejar atrás los complejos y las reticencias a la hora de compartir información teniendo en cuenta que no es lo mismo compartir información de ciberinteligencia que sobre incidentes que se han sufrido por implicaciones legales que pudiera haber. Iniciativas como la de CSIRT.es, precisamente, tienen como uno de sus puntos destacados el de la compartición de información".

UNIVERSIDAD CARLOS III DE MADRID

Rafael Calzada Pradas

Responsable de Seguridad de la Información

❶ "Los CERTs académicos están evolucionando, pero de forma heterogénea, dependiendo del nivel de madurez de cada una de las instituciones, algunos están mejorando aspectos organizativos y otros los aspectos más operativos. La pandemia nos ha enfocado en los accesos remotos que hasta ese momento eran casi testimoniales, al menos en las universidades públicas presenciales. Nuestros usuarios de VPN habituales se multiplicaron por seis nada más establecerse el confinamiento en marzo y hubo que poner un esfuerzo especial para integrar los equipos de los usuarios o proporcionar soluciones de Virtualización de Escritorio que escalasen al volumen de usuarios y tráfico que estaba siendo demandado".

❷ "Consolidar los procedimientos y controles establecidos para las situaciones de teletrabajo, y siempre mejorar, detectar los ataques antes para aplicar medidas adaptativas que dificulten el éxito de los atacantes, detectar precozmente los posibles compromisos especialmente en sistemas periféricos, que pueden permitir al intruso pivotar a equipos más sensibles y si todo lo anterior falla, reducir los tiempos de recuperación".

❸ "Actualmente, existe comunicación informal a nivel de CERTs especialmente en determinados sectores; por ejemplo: los CERTs académicos contamos con foros de comunicación, reuniones periódicas, donde se exponen los problemas y enfoques que hemos tomado de modo que entre todos mejoramos. Sin embargo, todavía nos queda pendiente la eterna automatización de la comunicación de Indicadores de Compromiso y otra inteligencia de seguridad. Afortunadamente, en España contamos con el CCN-CERT, que apoya iniciativas tanto con herramientas, como con contenido. La mejora vendrá cuando todos los participantes pasemos de ser consumidores de esa inteligencia de seguridad a ser contribuidores/generadores de la misma. Aquí puede haber problemas con los intereses económicos de algunas empresas, pero las instituciones públicas no tenemos excusa".

VERSIA

Andoni Alcalde

Director del CERT/CSIRT

❶ "Aunque la evolución –con CERTs / CSIRTs cada vez más maduros– es adecuada, existe la necesidad de mejorar los servicios proactivos que se ofrecen con la automatización basada en IA y en la orquestación DevSecOps".

❷ "Uno de los grandes retos de 2021, que no sólo amenaza a los CERT/CSIRT, es la falta de talento que pueda satisfacer la demanda actual para cubrir los perfiles necesarios".

❸ "Los CERTs/CSIRTs que formamos parte de foros establecidos como el FIRST, disponemos de canales que promueven y facilitan enormemente la compartición de información de forma eficiente. A pesar de ello, es necesario seguir apostando por establecer vías de cooperación más amplias que retornen en flujos de información más abiertos entre los participantes".

XUNTA DE GALICIA

Gustavo Herva

Jefe del Departamento de Seguridad y Calidad

❶ "Los retos a los que tienen que hacer frente en la actualidad los CERTs / CSIRTs son muchos. El número, variedad y gravedad de las amenazas y el posible impacto de las mismas en las organizaciones no para de crecer, muchas veces más rápido de lo que crecen las capacidades de los CERTs / CSIRTs. Creo que en general la evolución es buena y, aunque es cierto que siempre nos gustaría tener más, en nuestro caso la dotación presupuestaria dedicada a ciberseguridad ha ido creciendo en los últimos años y hemos ido poco a poco reforzando nuestras capacidades. Actualmente tal vez uno de los principales problemas es la escasez de profesionales formados y con experiencia, debido a la enorme demanda que hay, y esto es algo que nos afecta periódicamente cada vez que necesitamos ampliar el equipo humano".

❷ "Nuestra intención es incrementar en 2021 nuestra madurez en la gestión de la ciberseguridad, optimizando nuestros procedimientos y automatizando en lo posible. Además, queremos poner el foco en la colaboración con el resto de agentes del sector, potenciando la actividad del nodo gallego de ciberseguridad CIBER.gal, que tiene el objetivo de ser la estructura de colaboración público-privada en la que participen las entidades y organizaciones relacionadas con la ciberseguridad en el ámbito de la comunidad autónoma de Galicia (administraciones públicas, universidades, centros tecnológicos, empresas, etc.)".

❸ "Pertenecemos desde hace un par de años a CSIRT.es, que puede ser un elemento que sea necesario potenciar para mejorar la compartición de información de forma efectiva en un contexto de colaboración público-privada. En el ámbito público, nuestra referencia es el CCN-CERT, que nos presta siempre su ayuda y con quien seguiremos colaborando para mejorar en lo relativo a compartición de información".

Así opinan

EXPERTOS QUE IMPULSARON E IMPULSAN LOS CSIRTs / CERTs EN ESPAÑA

España ya cuenta con cierta veteranía en el mundo de los equipos de respuestas a incidentes teniendo en cuenta que el primer equipo, el CERT-UPC, fue creado a finales de 1994, en la Universidad Politécnica de Cataluña, por un equipo liderado por el profesor Manel Medina. Un año después, en 1995 se formó el IRIS-CERT, el servicio de seguridad de RedIRIS, en cuyo desarrollo participó de forma activa Francisco Montserrat. También ha sido, entre otros, destacable la labor de Javier Berciano que colaboró decisivamente en el CERT de INTECO (actual-

MANEL MEDINA

Profesor, Director de esCERT-UPC
Másters de Gestión de Ciberseguridad
y de Blockchain de UPC-School

"Cuando empezaron a reportarse incidentes de ciberseguridad en España, tanto Iris-CERT como esCERT-UPC, nos ofrecimos voluntarios para prestar servicios a las Administraciones Públicas y al sector privado, respectivamente, aunque no de una forma rigurosa. Ambos nos dimos de alta en la organización FIRST para poder recibir información confidencial de los procedimientos de respuesta empleados por otros CSIRTs. Lo más complicado fue conseguir financiación y soporte para cumplir los requisitos de FIRST y TF-CSIRT en Europa y me siento especialmente orgulloso de haber podido ayudar a muchos equipos de respuesta a incidentes y de investigación españoles a formar a sus primeros especialistas. Quizá lo más complejo ha sido mantener un crecimiento sostenido. Pero tal vez haya sido mejor así, con varias spin-off'de esCERT-UPC consolidando ese crecimiento.

En cuanto a su evolución, destaca el Profesor que "las tareas de consultoría y auditoría se desviaron hacia 'spin-off' completamente privadas; esCERT se ha especializado en dar soporte a otros CSIRTs y a formar a profesionales del sector y a los ciudadanos en general con campañas de concienciación". De cualquier forma, considera "que sí" se ha cumplido lo esperado, aunque lo que aún queda por hacer es "la colaboración entre CERTs / CSIRTs –ya que resulta todavía incipiente– y el uso de las herramientas de intercambio de información todavía no está generalizado".

JAVIER BERCIANO

Ex responsable de Gestión de Incidentes
en el CERT de INCIBE, único español
en la Junta de FIRST y Principal Incident
Response Engineer en Citrix

"Los comienzos fueron apasionantes porque se estaba empezando a desarrollar algo prácticamente desconocido en nuestro país, con muchos retos, algunas experiencias y buenas prácticas, pero con poca madurez. Desde un punto de vista nacional, lo más complejo fue dar a conocer fuera del ámbito técnico a los CERTs / CSIRTs, así como conseguir ciertas atribuciones para ellos dentro de las organizaciones o las administraciones públicas. Aún queda mucho camino por recorrer, pero la aparición de los mismos en la legislación ha sido un reto conseguido de mucha importancia.

En cuanto a su evolución, la comunidad de CSIRTs en España ha crecido de una forma muy adecuada y, considerando FIRST como el foro de referencia mundial, somos el tercer del país del mundo con mayor número de miembros, algo que demuestra la madurez de nuestro mercado de ciberseguridad y la importancia que le dan a la misma las principales empresas de nuestro país y el sector público a todos los niveles, no solo estatal. El posicionamiento actual de los CERTs / CSIRTs españoles es muy bueno y debemos ser considerados como un caso de éxito por las capacidades construidas como comunidad y la colaboración existente en la misma a nivel nacional.

Ahora, el reto es continuar fortaleciendo estas redes de CERTs / CSIRTs, la colaboración entre ellos. Y la compartición de información dentro de las mismas es clave para continuar incrementando el nivel de madurez de cada equipo y la comunidad nacional e internacional que forman".

mente INCIBE), en el que trabajó durante más de 10 años. SIC les ha preguntado por los retos a los que se tuvieron que enfrentar cuando acometieron la puesta en marcha de los primigenios Equipos y, también, qué queda aún por hacer al cabo de más de una década.

FRANCISCO MONSERRAT
Técnico Senior en IRIS CERT

"Llegué al IRIS-CERT a principios de 1999. El equipo de seguridad ya estaba formado desde el año 1995 gracias a la labor de **Rubén Martinez**, aunque desde que se creó Red IRIS por el año 1990 se venía viendo la necesidad de coordinar las iniciativas de seguridad. Por entonces, el concepto de CERT todavía no estaba muy bien definido. Lo que se buscaba, sobre todo, era tener un 'punto de contacto' en otro lugar del mundo, aunque muchas veces éste no tuviera ninguna autoridad real. Por entonces, Manel Medina, ya estaba creando en España esCERT. Así, en 1997, IRIS-CERT se hizo miembro de FIRST y en 2001 o 2002 patrocinamos a la membresía del esCERT-UPC en FIRST.

Hasta el año 2005, los CERTs fueron, por un lado, muy activos, ya que había demasiadas cosas que hacer, pero por otro, muy solitarios. Veíamos como en otros países empezaban a aparecer CERTs de diferentes sectores (gobierno, empresas privadas, etc.) pero en España solamente estábamos dos equipos de seguridad, lo que hacía que muchas veces actuáramos como punto de contacto desde el exterior con incidentes que no eran de nuestro ámbito de actuación.

De lo que nos podemos sentir más orgullosos es de los grupos de coordinación que se crearon, inicialmente solo con los ISP y Fuerzas de Seguridad, y que después dieron lugar al foro de CSIRTs españoles, que ha servido para fomentar la creación de los más de 30 equipos que hay en la actualidad.

Lo más complicado fue la falta de claridad entre los servicios, la notificación de incidencias a las instituciones y, por otro lado, con el equipo de seguridad en su conjunto y los problemas de perder personal que tuvimos cuando el servicio de notificación se separó de las funciones del equipo de seguridad.

En cuanto a su evolución, los CSIRTs han pasado de ser un organismo externo en muchas organizaciones (el ente al que se le envía información y de la que se reciben notificaciones), a ser un concepto que está interiorizado en muchas organizaciones, no solo como servicio hacia otras organizaciones, sino también a nivel interno de estas; ha ayudado mucho a ello el ENS y los CSIRTs nacionales, sobre todo CCN-CERT e INCIBE-CERT. Ahora, el principal reto de los CSIRTs es la cooperación con otros CSIRTs y organizaciones para el intercambio de información eficaz que ayude a proteger a sus entidades".