"CIBERSEGURIDAD: HACIA UNA RESPUESTA Y DISUASIÓN EFECTIVA"

Cybersecurity: Towards an Effective Response and Deterrence

Recibido: 10 / 04 / 2019 Aprobado: 31 / 10 / 2019

Coronel
Javier Candau
España

El autor es Coronel de Artillería. Ingeniero Industrial con especialidad en electrónica y automática. Actualmente se desempeña como Jefe del Departamento de Ciberseguridad del Centro Criptológico Nacional y responsable de la Capacidad de Respuesta ante Incidentes gubernamental (CCN-CERT). Es Especialista criptólogo. Dispone de diversas certificaciones de especialización en seguridad de las TIC (ISS, SANS, CRAMM, Curso de Auditoría del INAP, Cursos CCN-STIC, etc.). Los principales cometidos de su actividad son la formación del personal especialista en seguridad de la Administración, el desarrollo de normativa del CCN (elaboración de políticas, directrices y guías de seguridad de las TIC para la Administración Pública - Series CCN-STIC), desarrollo de la herramienta de análisis de riesgos PILAR, la supervisión de acreditación de sistemas y la realización de auditorías de seguridad. Tiene más de 18 años de experiencia en todas estas actividades.

RESUMEN

Garantizar e implementar la seguridad en el ciberespacio es un reto extraordinario que exige mejorar las capacidades de detección, monitorización y vigilancia, y conocer las vulnerabilidades y las amenazas a las que se enfrenta la tecnología, con el fin de ofrecer una respuesta oportuna a los nuevos desafíos. La adaptación a este escenario tiene una meta clara: convertir a las organizaciones en objetivos cada vez más difíciles de atacar.

Palabras clave:
Ciberseguridad, ciberamenaza, prevención, detección, respuesta, ciberespacio.

ABSTRACT

Ensuring and implementing cyberspace security is an extraordinary challenge that requires improving detection, monitoring and surveillance capabilities, and knowing the vulnerabilities and threats that technology faces, to offer a timely response to the new challenges. Adapting to this scenario has a clear goal: to turn organizations into increasingly difficult targets to attack.

Keywords:
Cybersecurity, cyberthreat, monitoring, cyberspace, surveillance, response, cyberspace,.

INTRODUCCIÓN

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el Art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

EL RETO DE LA SEGURIDAD EN EL CIBERESPACIO

El avance de las Tecnologías de la Información y la Comunicación (TIC) presenta un nuevo paradigma. La expansión de internet, con más de 4.000 millones de usuarios en todo el mundo, ha impulsado una profunda transformación de las estructuras mundiales. Los servicios públicos, la educación, el ocio, el transporte, la cultura o las relaciones personales han experimentado un proceso de cambio absoluto, debido a la influencia que la tecnología ejerce sobre la sociedad. Tanto es así que existe incluso una nueva realidad: el ciberespacio.

Este entorno global plantea un escenario de oportunidades económicas y sociales de gran alcance. Sin embargo, también conlleva una serie de riesgos, que se incrementan día a día. Las amenazas del ciberespacio, favorecidas por la rentabilidad económica o política, el bajo coste de las herramientas empleadas y la posibilidad de actuar desde cualquier lugar del mundo de manera anónima, se dirigen y afectan transversalmente a los sectores públicos y privado, así como a los ciudadanos.

En este contexto, los ciberdelincuentes, los hacktivistas o los propios Estados, son capaces de explotar las vulnerabilidades tecnológicas con el objetivo de recabar información, sustraer activos de gran valor y amenazar servicios básicos para el normal funcionamiento de un país. Asimismo, la utilización de las técnicas de aprendizaje automático (machine learning) o el uso de modelos de inteligencia artificial (IA) son cada vez más frecuentes y sofisticados, evidenciando un creciente potencial para amplificar los riesgos existentes o crear nuevos riesgos; especialmente cuando Internet de las Cosas (IoT) es capaz de conectar cientos de millones de dispositivos.

Así pues, garantizar e implementar seguridad en el ciberespacio, al tiempo que se respeta la privacidad y la libertad, se ha convertido en una de las prioridades estratégicas de los países más desarrollados, debido a su impacto directo en la seguridad nacional, en la competitividad de las empresas y en la prosperidad de la sociedad en su conjunto. El mundo ciber exige un compromiso constante ante la evolución tecnológica y la creciente sofisticación de los ataques.

La adaptación a este escenario pone de manifiesto la necesidad de implementar seguridad, a través de la mejora de las capacidades de prevención, detección y respuesta ante las posibles amenazas.

PREVENCIÓN: NECESIDAD DE IMPLEMENTAR CIBERSEGURIDAD

La ciberseguridad, con el paso de los años se ha introducido entre las prioridades de un gran número de gobiernos, considerada ahora un asunto de seguridad nacional y eje fundamental de la sociedad y de sus sistemas económicos.

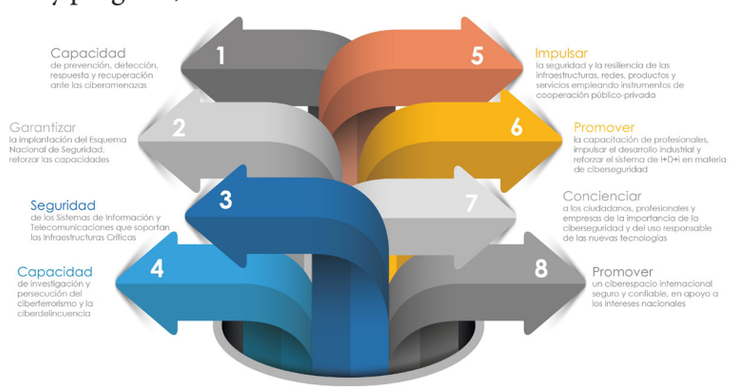
El desarrollo de un marco regulatorio y reglamentario posibilita, el establecimiento de una normativa y legislación en materia de ciberseguridad son el pilar fundamental de la prevención, pues actúan como catalizadores del sector y favorecen la creación, el crecimiento y el fortalecimiento de la actividad.

Todo eso ha justificado la necesidad de disponer de estrategias de ciberseguridad nacionales que permiten enmarcar los objetivos y las medidas para alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información de los Estados.

En Estados Unidos, en el 2009 el Departamento de Defensa creó el US Cyber Command (CYBERCOM) para controlar las capacidades de ciberdefensa y ciberguerra del Ejército y, en el 2011 publicó su Estrategia. En Europa, la Agencia Europa de Ciberseguridad (ENISA) elaboró una Guía de Buenas Prácticas en Estrategias Nacionales de Ciberseguridad.

Del mismo modo, la Organización de Estados Americanos (OEA) desarrolló varios programas para promover la Estrategia Iberoamericana con el objetivo de combatir las Amenazas de la Seguridad Cibernética, y en el 2011 Colombia presentó su Estrategia de Ciberseguridad y Ciberdefensa del Estado Colombiano.

Así pues, en España también se hizo evidente la necesidad de desarrollar un sistema nacional de ciberseguridad que fomentara la integración de todos los actores e instrumentos públicos y privados, con el fin de preservar el ciberespacio de todo tipo de riesgos y ataques, por tanto, defender los intereses nacionales y contribuir al desarrollo de la Sociedad Digital. Un modelo de ciberseguridad integrado que dirigido por el gobierno, garantizara al país su seguridad y progreso, a través de la adecuada coordinación de todas las



Administraciones Públicas entre sí, con el sector privado y con los ciudadanos; y que canalizase las iniciativas y esfuerzos internacionales en defensa del ciberespacio.

De este modo, y después de varios años de intenso trabajo a través de diferentes grupos y organismos, en diciembre de 2013 se publicó en España la Estrategia de Ciberseguridad Nacional (actualizada en 2017).

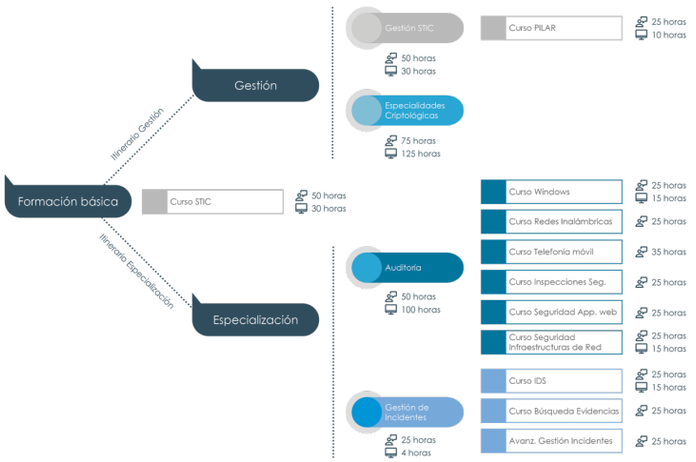
El cuerpo de leyes, decretos, órdenes ministeriales y reglamentos por los que se gobierna en materia de ciberseguridad debe ser ágil y aprovechar las situaciones existentes para conseguir un ciberespacio más seguro y confiable.

En el caso de España, existe el Código de Derecho de la Ciberseguridad, publicado en el Boletín Oficial del Estado, que cita las principales normas a tener en cuenta con relación a la protección del ciberespacio y para velar por la mencionada ciberseguridad. Del mismo modo, la Ley 11/2002 del 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos estableció el Esquema Nacional de Seguridad que, aprobado mediante Real Decreto 3/2010, del 8 de enero, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en el sector público. Su mandato esencial es que todo el sector disponga de una política que garantice el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de datos e informaciones, sentando las bases necesarias para promover la confianza de los ciudadanos en la utilización de los medios electrónicos.

Asimismo, para implementar ciberseguridad de una manera más clara y como medida de fortalecimiento de las capacidades de prevención, es necesario analizar los procedimientos y medidas de seguridad aplicadas a los sistemas de información de organismos, entidades y organizaciones. Para ello, resulta conveniente realizar auditorías de seguridad, que tienen como fin la obtención de evidencias y su evaluación de modo que se pueda determinar el grado de conformidad con la política de seguridad del sistema de información auditado y las necesidades de mejora y corrección de este. Para desarrollar estas acciones preventivas es imprescindible fomentar y desarrollar perfiles profesionales cualificados, así como concienciar y sensibilizar a los ciudadanos de los riesgos derivados de este nuevo paradigma. La prevención de los riesgos solo es

posible si la sociedad es consciente de las consecuencias derivadas de un incidente de seguridad.

Ante esta necesidad, el Centro Criptológico Nacional ha desarrollado un Plan de Formación adaptado a las tendencias en la gestión de incidentes y a la evolución de la superficie de exposición ante las posibles deficiencias de los requerimientos establecidos por la política de Seguridad de los Sistemas. Este nuevo escenario ha quedado reflejado en un diseño curricular, que da respuesta a las necesidades planteadas por su comunidad de referencia.



DETECCIÓN, LA CLAVE DE LA ACCIÓN PREVENTIVA

Para garantizar un nivel de seguridad adecuado en los sistemas, es necesario actuar antes de que produzca un incidente o, por lo menos, reducir su impacto y alcance una vez se ha detectado.

Por este motivo, desde el año 2008 el CCN-CERT ha desarrollado un Sistema de Alerta Temprana (SAT) para la detección rápida de incidentes y anomalías, que permite realizar acciones preventivas, correctivas y de contención. Su principal función, por lo tanto, es la detección temprana de un incidente para que puedan aplicarse las medidas necesarias de eliminación de la amenaza y poder evitar que el intento de ataque sea fructífero o, en su caso, minimizar el posible impacto.

Este sistema cuenta con tres (3) vertientes: SAT-SARA, monitorización de la Intranet de la Administración; SAT-INET, monitorización de las salidas de internet de los organismos adscritos al servicio; y SAT-ICS, para la detección en tiempo real de las amenazas e incidentes existentes en las redes de control y supervisión industrial del organismo adscrito.

A través de este servicio, el organismo adscrito tiene capacidad de detectar multitud de tipo de ataques, evitar su expansión, responder de forma rápida ante el incidente detectado y generar normas de actuación que eviten futuros incidentes. Al mismo tiempo y gracias al almacenamiento de un número progresivo de eventos, es posible contar con una panorámica completa y veraz de la situación de los sistemas, que posibilita una acción preventiva frente a las amenazas que sobre ellas se ciernen.

El Sistema de Alerta Temprana permite automatizar y reducir los tiempos de respuesta ante ataques e incidentes de todo tipo, incluida la detección avanzada interdominio, es decir, la detección temprana de un incidente replicado en otros dominios monitorizados. En este sentido, la integración de las capacidades de Security Information and Event Management (SIEM), notificación de incidentes y ciberinteligencia se hacen especialmente necesarias para la mejora de las técnicas de correlación compleja de eventos y gestión de incidentes.

HACIA UNA RESPUESTA Y DISUASIÓN EFECTIVA

En 1988, y ante lo que se consideró el primer gran ataque de la historia conocido como el gusano Morris, el Departamento de Defensa de Estados Unidos encargó a la Universidad Carnegie Mellon, en Pittsburg, la creación de un equipo capaz de hacer frente a este nuevo tipo de amenazas. El resultado fue la constitución del denominado Computer Emergency Response Team (CERT).

Bajos estas mismas siglas comenzaron a formarse otros grupos en distintas universidades norteamericanas, encargados de estudiar la seguridad de las redes y ordenadores para proporcionar servicios de respuesta ante incidentes víctimas de ataques, publicar alertas relativas a amenazas y vulnerabilidades y ofrecer información que ayudara a mejorar la seguridad de estos sistemas.

Teniendo en cuenta el continuo incremento de las amenazas y vulnerabilidades sobre los sistemas de información de todo el mundo, en el año 2004 se afianzó lo que sería el CERT Gubernamental Na-

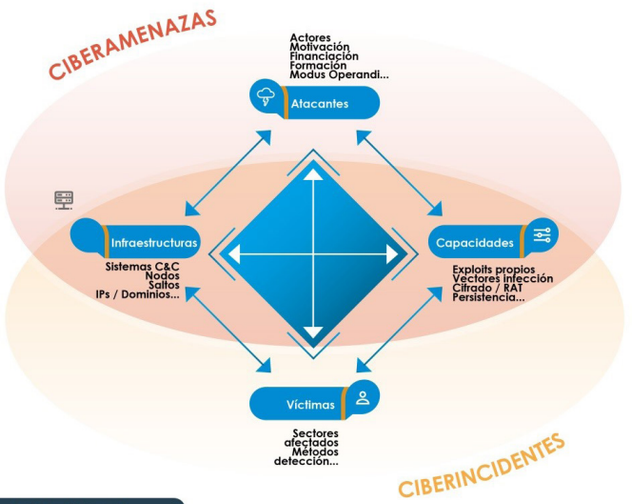
cional español. Así, y tras dos años de intenso trabajo, se presentó la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, (CCN-CERT), organismo cuya misión es contribuir a la mejora del nivel de seguridad de los sistemas de información de las Administraciones Públicas españolas y que coopera y ayuda al sector público a responder de forma rápida y eficiente a los incidentes de seguridad que pudieran surgir, para afrontar de forma activa las nuevas amenazas.

Estas amenazas han demostrado ser globales y su resolución solo puede llevarse a cabo mediante una respuesta conjunta, que debe implicar un mayor grado de coordinación y cooperación. Por un lado, a nivel nacional, entre los niveles de la Administración del Estado y las empresas privadas; y por otro, a nivel internacional, con otros países y organizaciones multilaterales.

Cualquier mecanismo utilizado para la gobernanza será verdaderamente eficaz si todos los participantes disponen de información fidedigna que les permita actuar. Esta capacidad de actuación es especialmente relevante en el caso de los gobiernos, a los que compete garantizar la seguridad y el bienestar de los ciudadanos.

En el ámbito nacional resulta imprescindible disponer de un modelo basado en el intercambio de información entre organismos públicos y privados, proveniente tanto del análisis de ciberamenazas como de ciberincidentes, con el objetivo de mejorar y agilizar la detección y actuación frente a los ataques.

Este intercambio siempre es más efectivo a través de la confianza entre las partes que por imposición normativa. Dicha confianza permitirá que todos los agentes implicados consideren beneficioso invertir su tiempo en foros y sistemas de intercambio y, asimismo, que se produzca una actuación recíproca en la que la información aportada esté a la par que la obtenida para optimizar sus defensas. Para que este modelo funcione, las aportaciones respecto a ciberamenazas y ciberincidentes deben estar compensadas, pues es necesaria tanto la información del atacante, relativo a sus capacidades e infraestructuras, como la de la víctima, en relación con el procedimiento de ataque, el impacto sufrido y las técnicas de detección y resolución. De este modo, se podrán cubrir todos los vértices del modelo de diamante y conocer las técnicas, tácticas y procedimientos (TTP) del atacante.



Modelo diamante

La industria de la ciberseguridad nacional debe actuar como catalizador de esta compartición de información de valor, con especial énfasis en el factor humano y a la formación de un equipo de analistas e investigadores, que aporten conocimiento y sean capaces de interpretar la información.

En esta tarea, el CCN-CERT ofrece dos de sus soluciones más destacadas: LUCÍA y REYES. La primera de ellas, para la notificación de incidentes y contextualización de la amenaza; la segunda, para el conocimiento y parametrización de la amenaza, permitiendo la elaboración de ciberinteligencia.

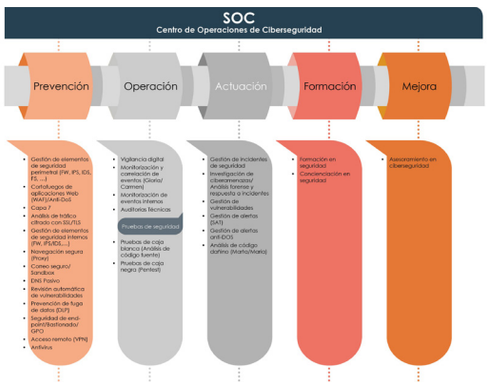
Junto a la cooperación nacional, resulta fundamental que cualquier equipo de respuesta a incidentes mantenga contacto en caso de ataque, con otros equipos del resto del mundo y asegure así las fuentes de información fiables. De ahí, la importancia de participar en los distintos foros internacionales existentes.

Del mismo modo, el constante aumento de los ciberataques, unido a las posibles consecuencias que para un país tendría que un incidente de seguridad afectase a sus sistemas, conlleva la necesidad de incrementar y mejorar las capacidades de prevención, monitorización, vigilancia y respuesta.

Todo ello es posible a través de los Centros de Operaciones de Ciberseguridad (SOC), cuya finalidad es la prestación de servicios

horizontales de ciberseguridad que permiten aumentar la capacidad de vigilancia y detección en la operación diaria de los sistemas de información y comunicación, así como mejorar su capacidad de respuesta ante cualquier ataque.

Su objetivo final es aumentar las capacidades existentes de vigilancia y detección de amenazas en la operación diaria, así como su capacidad de respuesta ante cualquier ataque, siendo prioritarios la monitorización y evaluación de manera continua de las medidas de seguridad, la actuación de manera proactiva ampliando las capacidades de vigilancia y reacción ante incidentes, y la parametrización de la amenaza mediante inteligencia de ciberseguridad, que permita integrar la información, para lo que resulta imprescindible mejorar la notificación de incidentes e incrementar el intercambio sobre la amenaza.



De esta manera, la evaluación continua constituye uno de los objetivos principales que persigue un Centro de Operaciones de Ciberseguridad, al permitir a lo largo del tiempo el seguimiento del grado de exposición a potenciales atacantes.

Asimismo, la cibervigilancia juega un papel primordial al comprender las acciones destinadas a vigilar el ciberespacio. Por tanto, la misión de un sistema de cibervigilancia es emitir informes y alertas sobre amenazas, de forma que la inteligencia obtenida pueda ser empleada para desplegar capacidades de respuesta en pro de desactivar, contener, mitigar o anular la posible acción dañina.

CONCLUSIÓN

El tiempo que media entre la primera acción hostil hasta el compromiso de un activo se mide, frecuentemente, en términos de segundos o minutos. Sin embargo, el plazo para su descubrimiento o detección, que depende en gran medida del tipo de ataque, suele expresarse en días, semanas o meses.

Estos datos reflejan la necesidad de continuar invirtiendo recursos materiales y, sobre todo humanos, para mejorar la protección del ciberespacio ante la imparable evolución de las tecnologías y la creciente sofisticación de los ataques. De igual modo, es necesario incrementar y mejorar las capacidades de inteligencia para la identificación de los atacantes, la determinación de sus objetivos y, sobre todo, la formación y concienciación de las personas para que los mecanismos de protección sean eficientes.

Por eso, el Centro Criptológico Nacional trabaja para dar respuesta al gran desafío que supone preservar el ciberespacio español, mejorando y adaptando sus soluciones a las necesidades presentes y futuras, para afianzar su papel como centro de referencia, tanto a nivel nacional como internacional, en materia de ciberseguridad.

REFERENCIAS

Centro Criptológico Nacional. (2007). *Capacidad de respuesta a incidentes del Centro Criptológico Nacional.* Recuperado de https://www.ccn-cert.cni.es

Centro Criptológico Nacional (2018, junio). *Aproximación española a la ciberseguridad.* Recuperado de https://www.ccn.cni.es/index.php/es/menu-ccn-es/aproximacion-espanola-a-la-ciberseguridad

Centro Criptológico Nacional. (2013). *Estrategia Nacional de Ciberseguridad.* Recuperado de https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf

Europea Union Agency for Network and Information Security. (2016). *NCSS Good Practice Guide*. Recuperado de https://www.enisa.europa.eu/publications/ncss-good-practice-guide

We are social (2018). *Global digital report.* Recuperado de https://digitalreport.wearesocial.com/