El CCN-CERT actualiza su catálogo de productos de seguridad TIC para manejar información clasificada y sensible

La adquisición de un producto de seguridad TIC, que va a manejar información nacional clasificada o información sensible por parte de la Administración Pública, conlleva un proceso de comprobación exhaustivo de sus mecanismos de seguridad. Para facilitar la elección, el **Centro Criptológico Nacional** (**CCN**) ha publicado la 'Guía CCN-STIC 105. Catálogo de Productos de Seguridad de las Tecnologías de la Información y Comunicación'. En esta guía, de casi 120 páginas, el organismo actualiza, por un lado, el listado de Productos Aprobados para manejar información nacional clasificada y, por otro, el de los Productos Cualificados de Seguridad TIC, para entornos sensibles y capacitados para ser utilizados en sistemas de Categoría Alta en aplicación del Esquena Nacional de Seguridad (ENS).

Para la evaluación y certificación de cada uno de estos productos de seguridad –y su posterior inclusión en este catálogo–, el CCN ha tenido en cuenta criterios como la clasificación de la información que puede manejar –Difusión Limitada, Confidencial, Reservada y Secreta–, sus características de seguridad, la categoría del sistema de información en la que puede emplearse según lo definido en el ENS –alta, media, básica–, las certificaciones aportadas o el entorno donde se vaya a emplear.

Clasificación de los productos

La guía –descargable en www.ccn-cert.cni.es– recoge seis categorías para los productos cualificados: Control de Acceso; Explotación de la Seguridad; Monitorización de la Seguridad; Protección de las Comunicaciones; Protección de la Información y Soportes de Información; así como, Protección de equipos y servicios. Y, repartidas en dichas categorías, se incluyen 36 familias, contemplando desde dispositivos biométricos hasta *single sign-on,* servidores de autenticación, protección de puntos finales, cortafuegos, etc.

Para los productos aprobados, el CCN ha establecido cuatro categorías: Seguridad de la Información; Protección de las Comunicaciones; Protección de la información y Soportes de Información; y, *Tempest* –de periféricos–. Y, las componen 10 familias como dispositivos para gestión de claves criptográficas, herramientas para comunicaciones móviles seguras, cifrado *off line*, entre otras.

Entre las más recientes incorporaciones al Catálogo de Productos STIC figuran la española **Open Cloud Factory** (con su solución para controlar todos los activos conectados en las redes corporativas de las compañías, openNAC, permitiéndolas obtener una visibilidad real y control de las mismas), que cumple con sus exigentes criterios para Enterprise. Y también **Forcepoint** con su NGFW, ha recibido la cualificación del CCN, lo que les ha permitido entrar a formar parte del CPSTIC en noviembre 2018. Con este reconocimiento se acredita ofrecer la seguridad exigida por los sistemas TIC pertenecientes a Organismos Públicos afectados por el ENS (Esquema Nacional de Seguridad)

Junto a estos fabricantes otras compañías que poseen una o varias de sus soluciones certificadas por el CCN son: **Alcatel Lucent**, **Aruba**, **Autek Ingeniería**, **CA Technologies** (hoy **Broadcom)**, **Check Point**, **Cisco**, **Dell**, **Epicom**, **EraseIT**, **Extreme Networks**, **FireEye, Forcepoint**, **Fortinet**, **Indra**, **Istria Soluciones de Criptografía**, **Juniper Networks**, **McAfee**, **Palo Alto Networks**, **Panda Security**, **Rubrik**, **Safelayer**, **Sophos**, **SonicWall** y **Symantec**.

Nombrada la nueva Junta Directiva hasta 2020 de ISACA MADRID

Durante la Asamblea General del pasado 22 de noviembre, fue elegida la Junta Directiva de **ISACA Madrid**, para el periodo 2018-2020. **Ricardo Barrasa** ha sido renovado como Presidente. Junto a él, forman la nueva Junta **Antonio Ramos** (Vicepresidente), **José Miguel Cardona** (Secretario), **Ana Belén Soriano** (Tesorera), **Vicente Chiva** (Vocal responsable de Formación y Relaciones académicas), **Joaquín Castillón** (Relación con los asociados, Comunicación y Marketing), **Pablo Blanco** (Eventos), **Vanesa Gil Laredo** (Auditoría & GRC), **Fernando Hervada** (Relaciones con la Admon. Pública y las Empresas privadas), **Eduardo Solís** (Seguridad Lógica) y **Erik de Pablo Martínez** (Director de Investigación).

Cobit 2019

De forma paralela, Isaca publicó en noviembre las novedades de COBIT, el *framework* que ayuda a conseguir un gobierno de las TIC más eficaz. Este marco de trabajo ha sido actualizado a la versión 2019. En la web de Isaca –www.isaca.org– se encuentran publicados cuatro documentos que proporcionan la base para crear un programa de un gobierno personalizado: *Introduction and Methodology*; *Governance and Management Objectives*; *Designing an Information and Technology Governance Solution*; e *Implementing and Optimizing an Information and Technology Governance Solution*.

CHECK POINT analiza sus 25 años ciberprotegiendo el mundo frente a ataques cada vez más sofisticados

Mario García, Director General Check Point España Portugal

Nacida en Israel, uno de los países que más apuestan por la seguridad y la defensa –también ciber–, en sólo un cuarto de siglo **Check Point** ha pasado de ser una compañía de cortafuegos y soluciones VPN a una empresa global que ofrece una arquitectura de protección multinivel de la información que discurre por la nube, las redes corporativas y los dispositivos móviles.

Para ello ha basado su crecimiento en una estrategia unificada y sólida. "Los ataques y amenazas han evolucionado, y cada vez son más sofisticados, obligando también a los actores del mundo de la ciberseguridad como Check Point a reinventarse", destacan sus responsables. "Desarrollar y ofrecer nuevas formas de protección contra todo tipo de amenazas ha sido un desafío constante para Check Point. Un reto que continúa y que exige disponer, cada vez más rápido, de nuevos sistemas" afirmó el Director General de Check Point para España y Portugal, **Mario García**, durante la celebración del 25 aniversario de la compañía.

Para el directivo, "hasta ahora, el panorama no ha sido tan sombrío, pero en los últimos meses se han producido muchos incidentes de gran interés, como las brechas en **British Airways, UnderArmour** y **Ticketmaster**". Y la realidad es que este tipo de situaciones no van a cesar porque los ciberataques dirigidos a empresas –y ciudadanos– se están profesionalizando e industrializando, ya que cada vez más ciberdelincuentes tienen acceso a las herramientas que los facilitan.

Para contrarrestarlo, Check Point considera necesario implementar medidas drásticas, "un antivirus no va a ser efectivo por sí solo, hay contar con tecnologías adicionales que se ajusten a las amenazas actuales, donde la prevención es también un elemento fundamental".