FORMAS DE INCORPORAR LA RESILIENCIA CIBERNÉTICA A SU NEGOCIO

Por Ann Brady

En una era cada vez más digital, y marcada por la desinformación y los bulos, el gran desafío radica en instaurar la confianza en la propia tecnología.

Hoy en día, pocos de nosotros ignoramos la importancia de la ciberseguridad y de las amenazas de los ciberataques a nuestras computadoras, smartphones y otros dispositivos. Se nos recuerda constantemente que jamás debemos revelar nuestras claves y que debemos permanecer alerta ante correos electrónicos no deseados y de phishing que intentan manipularnos para revelar información personal, como dichas claves, datos bancarios, datos de la Seguridad Social o información médica.

Esta forma de robo de identidad, alarmante de por sí, se vuelve aún más siniestra cuando está dirigida a gobiernos y otras instituciones importantes. «Ver es engañar» es el mensaje de una popular serie de BBC TV, The Capture, que explora el impacto de la tecnología deepfake –descrita como la respuesta del S. XXI al uso de Photoshop– que amenaza la seguridad nacional, hace tambalear los cimientos del estado, destruye la confianza y nos hace dudar de la realidad.

> El costo global de los ciberdelitos alcanzará los 10,5 billones de USD al año para 2025.

Quizá sea descabellada en muchos aspectos, pero a medida que nos adentramos en la era de la Cuarta Revolución Industrial, esta serie pone de relieve los riesgos y amenazas potenciales de unas tecnologías que cambian rápidamente y son cada vez más sofisticadas.

Priorizar el riesgo

Según el informe Perspectivas globales de ciberseguridad en 2022 del Foro Económico Mundial, la ruptura de infraestructuras como resultado de un ciberataque es la principal preocupación de los líderes en cibernética, por

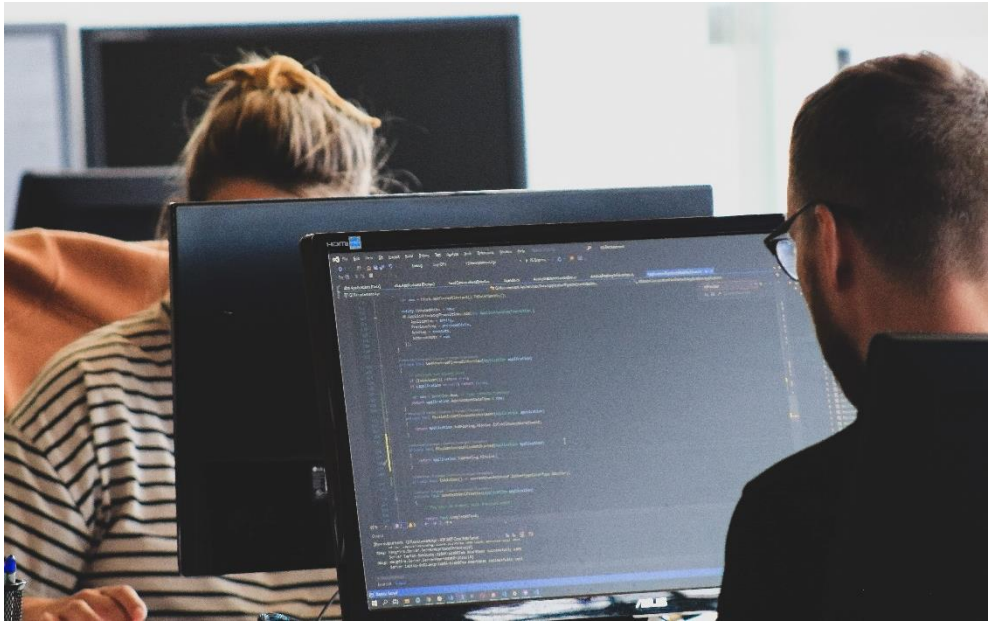
delante del robo de identidad. Este informe también señala que, si bien el 85 % de los líderes en cibernética coinciden en que la resiliencia cibernética es una de las prioridades de sus organizaciones, obtener el apoyo de los responsables de la toma decisiones a la hora de dar prioridad a dichos riesgos frente a otros sigue siendo todo un desafío. Desafío que no debemos tomar a la ligera. La revista CyberCrime afirma que los ciberataques podrían deshabilitar la economía de una ciudad, un estado o todo un país, y sostiene que el costo global de los ciberdelitos alcanzará los 10,5 billones de USD al año para 2025.

> Para tener éxito en el mercado,
> hay que ganarse la confianza
> de los consumidores.

La ciberseguridad no es una novedad, pero en nuestro mundo cada vez más interconectado (y fragmentado), los riesgos de los ciberataques para las personas, organizaciones, servicios y sistemas jamás fueron tan grandes. La tecnología se ha vuelto cada vez más sofisticada, al igual que los ciberdelincuentes. La incertidumbre lo copa todo y la confianza adquiere especial importancia. Tener la confianza y seguridad de que nuestros sistemas están a salvo es ahora un requisito básico y hay dos Normas Internacionales – ISO/IEC 15408 e ISO/IEC 18045 para tecnologías de la información– que pueden ayudar a recuperar esa confianza.

Las normas trabajan juntas «como los pedales de una bicicleta», afirma Miguel Bañón, experto en evaluación y certificación de ciberseguridad y coordinador del grupo de trabajo sobre evaluaciones, pruebas y especificaciones de seguridad que opera bajo el patrocinio conjunto de ISO y la

Comisión Electrotécnica Internacional (IEC). ISO/IEC 15408 establece los criterios de evaluación para la seguridad de las TI, mientras que ISO/IEC 18045, el documento de apoyo, define la metodología para la evaluación de la seguridad de las TI. A efectos prácticos, no obstante, son lo mismo.



Revisión oportuna

La reciente revisión de las normas no pudo ser más oportuna, evolucionando para satisfacer las complejas necesidades de nuestro tiempo. «El grupo de trabajo está centrado en la garantía de la tecnología, probando certificaciones y proporcionando las normas para garantizar que la tecnología en sí misma sea segura», afirma Bañón. «Es una parte importante de la solución». Las normas también ayudan a gestionar la información y a adoptar un planteamiento holístico, pero el fundamento básico es que la tecnología es segura.

Para tener éxito en el mercado, hay que ganarse la confianza de los consumidores. Es igual de cierto para la tecnología como para cualquier otro producto. Con una abrumadora variedad de productos que salen al mercado con mucha

rapidez –como es el caso de los vehículos conectados, por ejemplo–, ¿cómo podemos fiarnos de un vehículo conectado que conduce por sí solo si no tenemos la certeza de que va a funcionar como es debido?

Bañón nos cuenta que, con ISO/IEC 15408 e ISO/IEC 18045, «proporcionamos la mejor y única manera, acordada internacionalmente, de probar y evaluar la seguridad de los productos y sistemas». Señala que lo que antes era un nicho de mercado se está convirtiendo en la corriente principal y el propio mercado está poniendo la ciberseguridad como un requisito. Los líderes y los responsables de la toma de decisiones ahora tienen que redoblar sus esfuerzos y priorizar los ciberriesgos.

> El propio mercado está poniendo la ciberseguridad como un requisito.

Construir la resiliencia

A nivel gubernamental, se trata de algo que se está reconociendo cada vez más. Bañón afirma que un resultado positivo de este aluvión de preocupaciones por la ciberseguridad es que ha dado lugar, por ejemplo, a la nueva y próxima legislación de la Unión Europea para reforzar los sistemas de ciberseguridad. «La Ley de Ciberseguridad de la UE ofrece un marco para todos los programas de certificación en Europa. En el pasado, si había que certificar la seguridad de un producto, se podía hacer sobre la base de programas nacionales», comenta. «Ahora, por primera vez, habrá un programa de certificación paneuropeo para los productos, y este nuevo programa está basado en ISO/IEC 15408».

Como él mismo señala, la seguridad de las TI no es nada nuevo y la pasada aplicación de las normas ha tenido un impacto positivo en los productos del mercado. En su opinión: «Productos que normalmente han logrado cumplir las normas, como los sistemas operativos o los dispositivos de red, han evolucionado y mejorado hasta el punto de que los hackers han tenido que dirigirse a productos/superficies de ataque más "fáciles"».

El cumplimiento de ISO/IEC 15408 requiere un alto grado de madurez y de resistencia frente a ataques. Según Bañón, cuando hoy en día nos enteramos de noticias sobre grandes infracciones de la ciberseguridad, existe una alta probabilidad de que estos hackers estén explotando productos que no están certificados ni analizados por esta norma. «En el caso de un hacker, tiende hacia el eslabón más débil de la cadena. A día de hoy, la vía más rápida son los productos que no están certificados con la norma».

Independiente e imparcial

Todo es cuestión de confianza. En palabras de Bañón: «En nuestras normas, la confianza se otorga tras una revisión muy rigurosa, independiente e imparcial de un producto y tras un proceso de evaluación y certificación». Al igual que no es posible comprar (y no querríamos comprar) una lavadora que no cumple con los requisitos de seguridad, el cumplimiento de estas normas, «que están impulsadas por las necesidades del mercado y son la base de los programas de ciberseguridad de mayor éxito en todo el mundo», ofrece protección contra sorpresas desagradables y aporta tranquilidad.