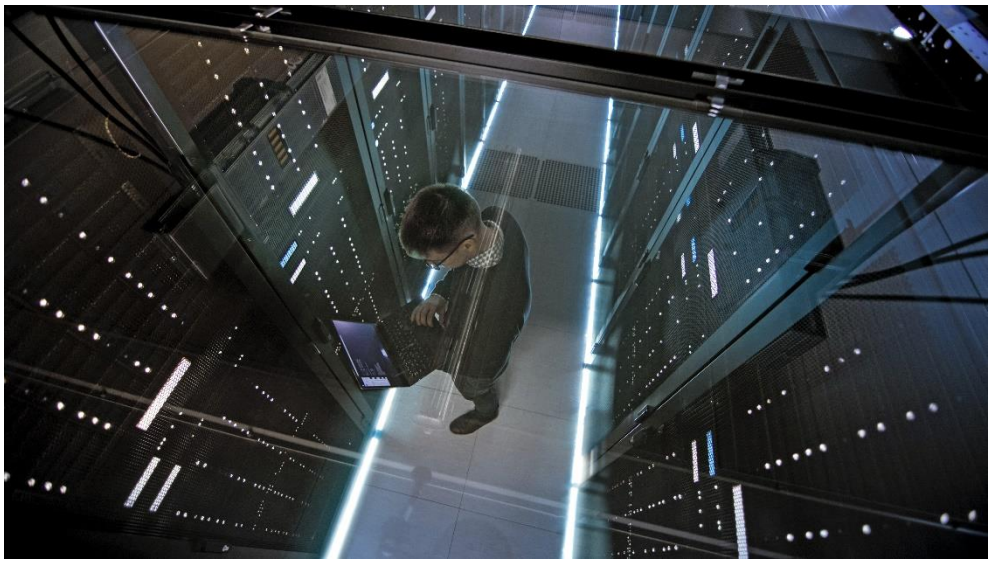
CONTRAATAQUES A LA CIBERSEGURIDAD

Por Ann Brady

Los ciberataques son costosos, disruptivos y una creciente amenaza para las empresas, los gobiernos y la sociedad por igual. Afortunadamente, contar con un arsenal de normas nos ayuda a llevar la delantera.

Los ciberdelitos no hacen sino aumentar, y a medida que avanzamos por la era digital, la era de la llamada Cuarta Revolución Industrial, estos son cada vez más avanzados y graves, con serias consecuencias. Los ciberdelincuentes cada vez son más hábiles, de modo que los ciberdelitos han afectado todas nuestras vidas de una forma u otra.

Los ciberataques pueden darse en forma de hackeos de sistemas y redes sociales, ataques de phishing, software malicioso incluido el ransomware, robo de identidad o ataques de ingeniería social y denegación de servicio. Resulta desagradable a nivel tanto personal como económico, provoca daños y destrucción incalculables y, además, deja a las personas y la sociedad en una posición vulnerable. Según McAfee, la empresa de software de seguridad informática, el costo de estos ciberataques no deja de aumentar, llegando casi al billón de dólares estadounidenses en 2020.



Un riesgo global cada vez mayor

Dado que la pandemia de COVID-19 ha arraigado aún más nuestra creciente dependencia de sistemas digitales, no es de sorprender que el *Informe Global de Riesgos de 2022* haya vuelto a incluir la amenaza a la ciberseguridad como uno de los riesgos crecientes a los que se enfrenta el mundo. Indica que los fallos de ciberseguridad han empeorado considerablemente y amenazan la prosperidad a largo plazo.

Pero ¿cómo podemos adelantarnos? El desarrollo de un buen sistema de ciberdefensa y la previsión de amenazas son

elementos clave de la lucha contra los ciberdelitos, pero ni la resiliencia ni la gobernanza son posibles sin unos planes de gestión de riesgos de ciberseguridad que sean creíbles y sofisticados. «Los ciberdelitos son acontecimientos nacionales e internacionales que se propagan a gran velocidad, afectando así a empresas, gobiernos y la sociedad en general. La escala y complejidad de esta actividad delictiva tienen consecuencias profundas y perjudiciales y la situación es algo confusa, ya que los ciberdelincuentes operan traspasando las fronteras nacionales, haciendo uso de infraestructura técnica», afirma el Dr. Edward Humphreys, experto en ciberseguridad.

> Los fallos de ciberseguridad
> han empeorado considerablemente.

Por ello, agrega, la colaboración internacional es fundamental y las Normas Internacionales son imprescindibles para la protección global. El Dr. Humphreys habla a partir de sus muchos años de experiencia en el mundo de los negocios. También es investigador senior especializado en ciberriesgo, seguridad y ciberpsicología y estudios de innovación en SGSI, además de coordinador del grupo de trabajo responsable de la gestión, el desarrollo y el mantenimiento de ISO/IEC 27000, una familia de normas sobre sistemas de gestión de la seguridad de la información (SGSI).

Soluciones y controles

Las Normas Internacionales aportan soluciones, afirma, al permitir a las organizaciones establecer marcos y sistemas para evaluar y gestionar la situación, con el objetivo de

proteger la información, las aplicaciones, servicios y la infraestructura nacional.

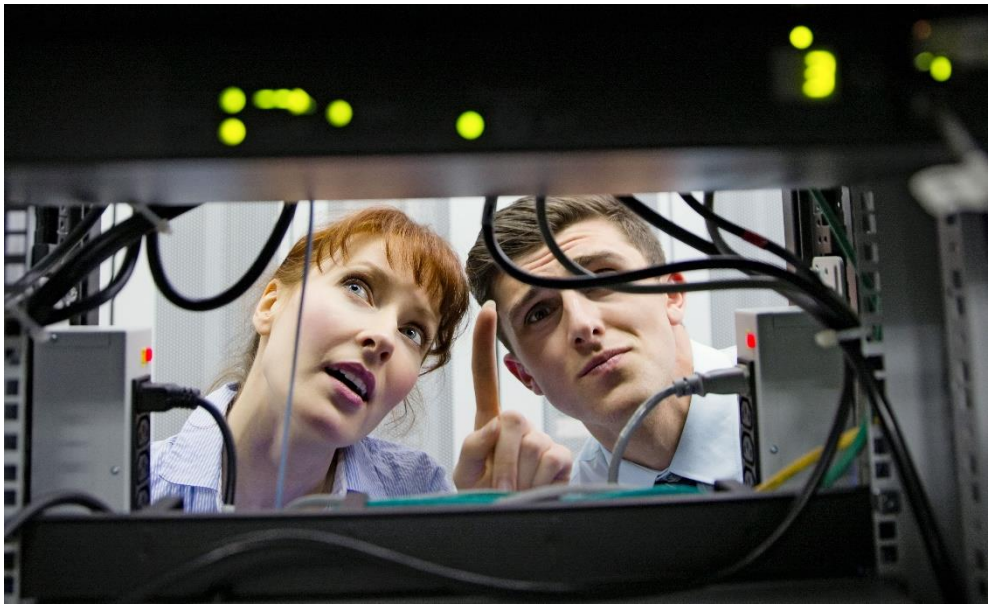
El primer paso para abordar los ciberdelitos consiste en conocer los riesgos a los que estamos expuestos, para después decidir los controles que se deben implementar para mitigarlos. Humphreys señala a las normas como la familia ISO/IEC 27000, desarrollada por ISO y la Comisión Electrotécnica Internacional (IEC), como la opción obvia para toda organización que desee desarrollar soluciones sólidas contra los ciberdelitos. El conjunto de Normas Internacionales especifica un sistema de gestión que ahonda en el proceso de la gestión de riesgos a cargo de evaluar los riesgos y, después, determinar los controles necesarios para tratarlos.

«Numerosas normas complementan a ISO/IEC 27001, como ser ISO/IEC 27005 sobre gestión de riesgos de seguridad de la información e ISO/IEC 27003 sobre directrices de implementación», afirma. «Además, existen otras muchas normas que ofrecen apoyo técnico a ISO/IEC 27001, por ejemplo, para proteger las redes e integrar características de seguridad en tecnologías, servicios y aplicaciones».

Cómo prepararse

El Dr. Humphreys reitera la necesidad de que las empresas estén preparadas y listas para hacer frente a estos ataques. «Los ciberataques pueden producirse en cualquier momento y lugar, y lo cierto es que estos ataques seguramente

sucedan, pero jamás sabremos con certeza cuándo o dónde», afirma. «Estar listos y preparados es una actividad de negocio básica para la supervivencia. Implica que un negocio disponga de un proceso para poder prever, identificar, detectar y comunicar incidentes, y para analizar dichos incidentes a fin de decidir cómo responder ante ellos». Todo ello se debe hacer de forma rápida y oportuna para limitar el impacto que podría provocar el incidente.



Entonces, ¿cómo pueden las empresas estar mejor preparadas? Una vez que una empresa detecta la presencia de un ataque de código malicioso o ataque de denegación del servicio, cuanto antes responda con medidas de seguridad adecuadas, más probabilidades tendrá de limitar la propagación de estos ataques, así como de limitar el impacto y los daños. Además, el Dr. Humphreys opina que existen normas que ayudan a las empresas a estar listas y a prepararse mejor para responder, como la norma sobre gestión de incidentes (ISO/IEC 27035), la norma sobre gestión de la continuidad del negocio (ISO 22301) y la norma sobre preparación de las TIC (ISO/IEC 27031).

Acción colectiva

En un mundo de por sí incierto, los ciberdelitos pueden tener unas consecuencias financieras devastadoras, provocar disrupciones en las operaciones de negocio y la infraestructura nacional, además de afectar la sociedad y los ciudadanos. Por ejemplo, un ataque en una parte de la cadena de suministro puede propagarse y alterar y dañar otras partes de la cadena. A fin de promover unos sistemas de ciberseguridad más seguros y resilientes, el Dr. Humphreys señala que la gestión de una cadena de suministro es un excelente ejemplo en el que se necesita acción colectiva en todas las partes de la cadena para mantenerla segura.

Agrega: «Una vez más, existen normas que ayudan con la seguridad de la cadena de suministro, como ISO 28000 e ISO/IEC 27036. También se necesita acción colectiva en diversas situaciones que implican relaciones comerciales y comunicación con otras organizaciones. Existe un grupo de normas de gestión que ayudará a desarrollar la resiliencia necesaria para frenar la disrupción del negocio y garantizar la capacidad de supervivencia y el sistema gobernanza. Se trata de ISO 22301 (sistemas de gestión de la continuidad del negocio), ISO/IEC 27001 (sistemas de gestión de la seguridad de la información) e ISO/IEC 27014 (gobernanza de sistemas de seguridad)».

Dados el crecimiento y la dependencia de la conectividad para las empresas, la infraestructura que las sustenta y el uso de Internet y de dispositivos móviles, existe una necesidad aún mayor en cuanto a seguridad y resiliencia del sistema. El Dr. Humphreys reconoce que las normas deben seguir

evolucionando para seguirles el ritmo a los rápidos avances en tecnología. «La tercera edición de ISO/IEC 27002, por ejemplo, se publicó en el primer trimestre de 2022. Esta norma de alto nivel trata los controles de seguridad de la información y se ha actualizado para encajar los avances en tecnología, prácticas y desarrollos de negocio, así como las nuevas leyes y reglamentos».

En 2021, agrega, se produjeron otros muchos desarrollos en normalización, incluidas la seguridad y privacidad de la Internet de las Cosas (IdC), la seguridad y privacidad de los big data, la seguridad y privacidad de la inteligencia artificial y la protección de la información biométrica. Todo ello se suma a recientes especificaciones técnicas tales como ISO/IEC TS 27570, que ofrece pautas para la protección de la privacidad de ecosistemas de ciudades inteligentes, e ISO/IEC TS 27100, que especifica cómo crear o perfeccionar unos cibersistemas sólidos para estar protegidos frente a ciberataques. La familia completa de normas ISO/IEC 27000 y estas especificaciones centradas en tecnología son los cimientos sobre los que construir y gestionar un futuro seguro.