CUADERNOS DE SEGURIDAD

NÚM. 366 | SEP/OCT 2022 | 12€

cuadernosdeseguridad.com

Edita **Peldaño**

GRANDES EVENTOS Y CENTROS DE OCIO

Seguridad, un trabajo de todos

PROTECCIÓN CONTRA INCENDIOS

Retos y claves de futuro

ROBO E INTRUSIÓN

Tecnología e innovación

LA TRANSFORMACIÓN DIGITAL EN SEGURIDAD CORPORATIVA (V)

La Ciberseguridad

JOSÉ JULIÁN ISTURITZ.
DOCTOR EN DERECHO PÚBLICO. EXPERTO EN SEGURIDAD CORPORATIVA. UNIVERSIDAD ISABEL 1.

NAIARA ISTURITZ LOINAZ.
GRADO EN ENFERMERÍA. MÁSTER EN GESTIÓN SANITARIA. POSTGRADO EN CUIDADOS INTENSIVOS. SEGURIDAD DEL PACIENTE.

Vivimos en una sociedad que está cada vez más digitalizada ya que las nuevas tecnologías han revolucionado nuestros comportamientos y costumbres pero también han cambiado los procesos, tanto organizativos como operativos.

Además de digitalizarse la manera de trabajar, también se ha digitalizado la manera de delinquir, apareciendo nuevos delitos de naturaleza informática con nuevos riesgos de ámbito corporativo.

CIBERESPACIO

Estamos acostumbrados a entender un espacio o territorio como algo tangible. Pues bien, el ciberespacio es aquel territorio virtual en el que concurren y circulan datos de carácter informativo, de forma que no es un espacio tangible, sino intangible, y es más que un espacio común global.

Las actividades que se efectúan en este ciberespacio tienen que ver con la tecnología, carecen de espacio físico como tal y sobrepasan las fronteras convencionales.

Viene a ser lo que muchas veces llamamos «la nube» para referirnos a aquel lugar por donde concurren o se almacenan datos que permiten obtener determinadas informaciones.

En este espacio, como en cualquier otro, ocurren fenómenos ordinarios y otros anormales que buscan diferentes intereses, legítimos o no, y por lo tanto, es un elemento vulnerable sometido a diversos riesgos que hay que gestionar.

CIBERSEGURIDAD

Entendemos por ciberseguridad a las medidas de prevención y protección de los riesgos y ataques que utilizan como vehículo elementos informáticos y se desarrollan en el ciberespacio.

Para Kaspersky (2021)[1], la ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil.

Para el Ministerio del Interior (2019)[2], la ciberseguridad es un objetivo estratégico de la política de seguridad nacional y pretende mejorar las capacidades de los órganos del Ministerio para detectar, prevenir y perseguir la ciberdelincuencia y generar un nuevo impulso operativo y técnico eficaz que garantice la protección de los derechos y libertades y la seguridad ciudadana. De aquí que, el Instituto Nacional de Ciberseguridad (INCIBE)[3] del Ministerio de Asuntos Económicos y Transformación Digital, edite constantemente información útil en ciberseguridad y haya editado junto con el Boletín Oficial del Estado el Código de Derecho de la Ciberseguridad (BOE, 2021)[4] que contiene el conjunto de normas aplicables en esta materia.

«Estamos ante un entorno donde el trabajo colaborativo en red entre distintos profesionales es crucial para la gestión de este tipo de riesgos»

Por lo tanto, la seguridad de las aplicaciones se enfoca a mantener el software y los dispositivos libres de amenazas.

IMPACTO

Según el Ministerio del Interior (2021), la cibercriminalidad experimenta en todo el mundo un fuerte crecimiento paralelo al incremento del desarrollo y uso de las tecnologías de la información y las comunicaciones en todos los ámbitos públicos y privados. Según estimaciones de la Comisión Europea, el costo de la ciberdelincuencia para la economía global en el año 2020 fue de 5,5 billones de euros, lo que representa la mayor transferencia ilícita de riqueza, superior a la que se deriva del tráfico global de drogas.

En 2015, se conocieron un total de 83.058 hechos relacionados con la cibercriminalidad, cifra que ha ascendido a 218.302 a finales de 2019, lo que supone un incremento del 162,8 % en apenas cinco años. Si en 2015 la ciberdelincuencia representó el 4,1% de la criminalidad conocida, a finales de 2019 aumentó hasta el 9,9%.

Sfio Cracho/Shutterstock

TIPOS DE RIESGOS O CIBERAMENAZAS

Los tipos de amenazas que afectan a la ciberseguridad pueden ser:

a) El delito cibernético, que incluye aquellos agentes individuales o grupos que atacan a los sistemas para obtener beneficios financieros o causar interrupciones.

b) Los ciberataques, que normalmente pretenden la recopilación de información con fines empresariales y/o políticos.

c) El ciberterrorismo que tiene como objetivo debilitar los sistemas electrónicos para causar pánico o temor.

LA CIBERSEGURIDAD EN EL MARCO DE LA SEGURIDAD CORPORATIVA

Como ya se ha afirmado desde hace décadas por diferentes autores (Fernandez Pereira, 2005; Ballbé, 2007; Curbet, 2010; entre otros), la seguridad corporativa tiene un carácter integral e integrado, es decir, integral en tanto en cuanto es global, e integrada en cuanto a que está introducida en el tejido social de la corporación (Isturitz, 2013).

Por lo tanto, la ciberseguridad no es más que uno de los múltiples riesgos que pueden existir en una organización y así debe ser tratado en el marco de esta visión integral del fenómeno de la in/seguridad.

De ahí que resulta un error entender la seguridad como una parte de la informática empresarial, ya que ésta es el instrumento que los agresores utilizan para producir un daño y, como tal, tiene que ser previsto y protegido, mientras que la seguridad es más que eso.

Solarseven/Shutterstock

EL DIRECTOR DE SEGURIDAD Y LA CIBERSEGURIDAD

El director de Seguridad, como profesional regulado, tiene un papel relevante, también en materia de ciberseguridad, pero probablemente es un ámbito en el que debe poner más esfuerzo en el trabajo colaborativo en red a tener que trabajar con otros profesionales más especializados. En este caso, con los técnicos y servicios de informática de la corporación ya que estos son los verdaderamente expertos en los instrumentos informáticos.

Es similar a las relaciones existentes entre los departamentos de Ingeniería y los de Prevención de Riesgos Laborales, por lo que es muy sustantivo abundar en el talante, la búsqueda de consenso y complicidad del director de Seguridad Corporativo.

Puede desarrollar las siguientes funciones específicas relacionadas con la ciberseguridad:

-Protege las contraseñas

Para ello debe elaborar y controlar un protocolo sobre los accesos, sus filtros y jerarquías.

-Vela por el acceso a la información

Establece la jerarquía de valores en cuanto a la capacidad de acceso a los datos y la información que generan, en función del rol que cada persona tenga en la organización.

-Continuidad de negocio

Garantiza que exista una copia de seguridad de los datos y que estos pueden permanecer operables incluso en situaciones críticas.

-Identificación de los usuarios

Identifica usuarios para permitir el acceso y además, para poder saber qué, cuándo y para qué consulté un dato determinado.

-Revisa las conexiones

Controla las redes inalámbricas, tanto para acceso a internet como interconexiones de videocámaras, audio, radiocomunicaciones y similares.

Por lo tanto, es el responsable de planificar y dirigir aquellos aspectos que dan mayor seguridad y fiabilidad a un negocio o ámbito organizacional.

CONCLUSIONES

El ciberespacio es un lugar virtual en el que, como en cualquier otro, se cometen actos delictivos que deben ser gestionados.

Estamos ante un entorno donde el trabajo colaborativo en red entre distintos profesionales es crucial para la gestión de este tipo de riesgos.

La figura del director de Seguridad en materia de ciberseguridad precisa de una especial sensibilidad, consenso y complicidad con otros profesionales como son los técnicos informáticos de la corporación. ✱

Referencias bibliográficas

1.- Kaspersky. (2021). ¿Qué es la ciberseguridad? https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security.

2.- Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. «BOE» núm. 103, de 30/04/2019. https://www.boe.es/buscar/act.php?id=BOE-A-2019-6347.

3.- Incibe. (2021). https://www.incibe.es/.

4.- BOE. (2021). Código de Derecho de la Ciberseguridad. https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=173_Codigo_de_Derecho_de_la_Ciberseguridad&modo=1.system explosion – Arizona, 28 de julio de 2020, Mark B. McKinnon et al. [Consultado el 17 de diciembre de 2020].