BID

FUNDAMENTOS DE COMERCIO DIGITAL

MÓDULO 6

LA CIBERCRIMINALIDAD EN EL COMERCIO ELECTRÓNICO

Autor del curso

Banco Interamericano de Desarrollo (BID) (www.iadb.org), a través de su Sector de Integración y Comercio (INT).

Coordinador del curso

Banco Interamericano de Desarrollo (BID) (www.iadb.org), a través de su Sector de Integración y Comercio, el Instituto para la Integración de América Latina y el Caribe (INTAL) (www.iadb.org/es/intal), el Instituto Interamericano para el Desarrollo Económico y Social (INDES) (www.indes.org), así como el Consejo Suramericano de Infraestructura y Planeamiento (COSIPLAN) de la UNASUR.

Autor del módulo

Cynthia Gabriela Solís Arredondo

Coordinación pedagógica y de edición

El Instituto Interamericano para el Desarrollo Económico y Social (INDES) (www.indes.org), en colaboración con la Fundación Centro de Educación a Distancia para el Desarrollo Económico y Tecnológico (CEDDET) (www.ceddet.org).

Los presentes materiales han sido revisados a la luz de las decisiones ministeriales tomadas en el marco de la Novena Conferencia Ministerial de la Organización Mundial del Comercio celebrada en Bali, Indonesia, en diciembre de 2013. Los ajustes fueron realizados con la finalidad de reflejar un mayor alineamiento entre la temática del curso y las prioridades identificadas en la Declaración Ministerial y decisiones de Bali, en la que participaron todos los miembros del BID.

Declaración de Bali

Tabla de contenidos

Índice de figuras

Índice de tablas

Glosario de términos y acrónimos

A) GLOSARIO DE CONCEPTOS BÁSICOS

- Antivirus: Es un programa que monitorea un equipo o una red para detectar la mayoría de los programas maliciosos para evitar daños a los sistemas y a la información; normalmente lo llevan a cabo removiendo el código malicioso o neutralizándolo.
- Ataque informático: Es un atentado para tener acceso no autorizado a los sistemas, recursos o información para comprometerla o comprometer la seguridad e integridad de los sistemas.
- Certificado SSL: Las siglas SSL responden a los términos en inglés (Secure Socket Layer), el cual es un protocolo de seguridad que hace que los datos viajen de manera íntegra y segura, es decir, la transmisión de los datos entre un servidor y usuario web, y en retroalimentación, es totalmente cifrada o encriptada.
- Cibercrimen: El Cibercrimen o "Ciberdelito" es un término genérico que hace referencia a la actividad delictiva llevada a cabo mediante equipos informáticos o en contra de ellos, generalmente a través de Internet. El ciberdelito puede hacer uso de diferentes métodos y herramientas, como el phishing, los virus, spyware, ransomware o la ingeniería social, normalmente con el objetivo de robar información personal o de realizar actividades fraudulentas. El concepto general puede variar de legislación a legislación o en normativa o estándares internacionales.
- Ciberseguridad: La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberespacio.

- Contraseña: Una contraseña o password es una serie de caracteres alfanuméricos que sirven como llave de acceso para asegurar cuentas de usuarios a sistemas y programas de cómputo.
- Cracker: El cracker es el individuo que vulnera voluntariamente y con intenciones maliciosa, la seguridad de un sistema informático, generalmente con la finalidad de obtener un lucro indebido.
- Cracking: El término "cracking" hace referencia a la práctica que consiste en atacar sistemas informáticos y software con intención maliciosa.
- Dispositivos informáticos: Es un aparato o mecanismo que desarrolla determinadas acciones, en este caso particular, se utiliza para nombrar a los periféricos y otros sistemas vinculados al funcionamiento de las computadoras.
- Dispositivos móviles: Es un tipo de computadora de tamaño pequeño, con capacidades de procesamiento, con conexión a Internet, con memoria, diseñado específicamente para una función, pero que pueden llevar a cabo otras funciones más generales. Por ejemplo: un teléfono inteligente, una tableta, cámaras digitales, relojes inteligentes.
- Firewall: Se trata de un dispositivo de hardware o un software programado para limitar el tráfico de una red de acuerdo con ciertas reglas de acceso.
- Hacker: Este es un concepto bastante incomprendido ya que depende de las intenciones de una persona más que de sus conocimientos y capacidades, por ejemplo: mientras que un hacker es simplemente un programador inteligente, experto en manipular o modificar un sistema o red informática, un hacker malicioso es alguien que utiliza sus conocimientos de informática para obtener acceso no autorizado a datos tales como información de tarjetas de crédito o imágenes personales, ya sea para diversión, beneficio, para causar daño o por otras razones.
- Redes informáticas: Una red informática son dos o más computadoras conectadas entre sí y que comparten recursos, ya sea hardware (periféricos, sistemas de almacenamiento…) o software (archivos, datos, programas, aplicaciones…). Una red informática permite que varios usuarios puedan intercambiar

información, pasar archivos, compartir periféricos como las impresoras e incluso ejecutar programas en otras computadoras conectadas a la red.[1]

- Sistema informático: Es el conjunto de partes interrelacionadas, hardware, software y usuarios, que permite almacenar y procesar información.
- Sistema operativo: Es el programa de cómputo principal (software principal), que gestiona o administra los recursos del hardware y proporciona servicios y funcionalidades al software aplicativo o programas aplicativos diseñados para ejecutar funciones puntuales.
- Vulnerabilidad (informática): Se le llama así, a la característica de debilidad que vuelve susceptible a un sistema o un programa de cómputo para permitir accesos o modificaciones no autorizadas.

B) GLOSARIO DE ATAQUES INFORMÁTICOS

- Ataques de DoS y DDoS: Un ataque de denegación de servicio, o un ataque distribuido de denegación de servicio consiste en la saturación del ancho de banda de un servidor para dejarlo inaccesible impidiendo el tráfico legítimo.
- Backdoor: Un ataque de backdoor o de puerta trasera consiste en la instalación de código en los sistemas, programas o aplicaciones ya sea de fábrica o posteriormente, mediante el cual se puede acceder a éstos sin conocimiento del usuario y con fines maliciosos.
- Bomba Lógica: Del término en inglés LogicBomb. Una bomba lógica es un programa informático que se instala en una computadora y permanece oculto hasta cumplirse una o más condiciones preprogramadas para entonces ejecutar una acción. A diferencia de un virus, una bomba lógica jamás se reproduce por sí sola. Ejemplos de condiciones predeterminadas: día de la semana, hora, pulsación de una tecla o una secuencia de teclas, levantamiento de un interfaz

[1] Red informática en: http://www.apser.es/blog/2015/06/20/las-redes-informaticas-que-son-tipos-topologias/

de red, etc. Ejemplos de acciones: borrar la información del disco duro, mostrar un mensaje, reproducir una canción, enviar un correo electrónico.[2]

- Exploit: Técnica que permite explotar las vulnerabilidades de un sistema o un programa informático.
- Hoax: Es un mensaje que alerta a los usuarios acerca de virus o ataques apócrifos o inexistentes para que los usuarios propaguen estos mensajes y el atacante pueda allegarse de direcciones de correo para posteriormente enviar SPAM o esparcir un virus.
- «Malware» o código malicioso: Se trata de un tipo de software malintencionado dañino para un equipo que tiene el objetivo de infiltrarse en éste para dañarlo o extraer información sin el consentimiento del usuario.
- Pharming: Modalidad de estafa online que aprovecha las vulnerabilidades de los servidores DNS (Domine Name Server) para redireccionar el tráfico hacia un sitio apócrifo, podría considerarse una modalidad de phishing.
- Phishing: Es una forma de engaño utilizada para que las personas caigan en estafas y proporcionen información personal y/o confidencial, en la mayoría de los casos ese ataque se usa para cometer delitos financieros
- «Ransomware» o secuestro de información: Se trata de un programa de cómputo que de alguna manera vuelve inaccesible la información contenida en un sistema, generalmente cifrándola y exige al dueño del dispositivo un rescate para liberarlo.
- SMiShing: Es una variante del phishing, que utiliza los mensajes a teléfonos móviles, en lugar de los correos electrónicos, para realizar el ataque.
- Spam: Consiste en el envío masivo de mensajes no solicitados, con contenido generalmente publicitario, que se realiza a través de distintos medios como: foros, mensajería instantánea, blogs, etc. aunque el sistema más utilizado es el correo electrónico.

[2] Bomba Lógica en: https://www.seguridad.unam.mx/glosario/bomba-lógica

- Spyware o Programa Espía: Es un tipo de programa cuyo objetivo es recopilar información del usuario del sistema en el que se instala. Los datos que se recogen suelen estar relacionados con los hábitos de navegación del usuario y se utilizan con fines publicitarios.
- Virus: Se trata de un programa que tiene la capacidad de replicarse él mismo, infecta a las computadoras sin el conocimiento ni el consentimiento del usuario con el fin de infectar otras computadoras y propagarse.
- Vishing: Fraude que persigue el mismo fin que el Phishing, pero se lleva a cabo a través de llamadas telefónicas de forma manual o automatizada.

Presentación del módulo

"El único sistema seguro es aquél que está apagado en el interior de un bloque de hormigón protegido en una habitación sellada rodeada por guardias armados"

-- Gene Spafford

Desde hace varios siglos, la seguridad de la información ha sido fundamental para los gobiernos y las economías; y desde luego para los seres humanos en general, sólo que estos últimos hasta hace una década no se habían percatado de la pieza fundamental que juegan.

Dentro de este concepto base denominado seguridad de la información, en el que profundizaremos más adelante, se encuentra el término seguridad informática o ciberseguridad.

La **ciberseguridad,** se ha convertido en la última década en un asunto prioritario, sin embargo, a consecuencia de los ataques a infraestructuras críticas (hospitales, transportes, plantas nucleares, agencias gubernamentales) y entidades financieras, su relevancia se ha incrementado aún más.

El comercio digital es una interesante fuente de ingresos y desarrollo para las economías contemporáneas, sin embargo, tal y como lo hicimos con los modelos de negocio tradicionales, es importante implementar las medidas de seguridad mínimas en cada uno de los puntos de contacto de comerciantes, clientes, proveedores e intermediarios, para garantizar transacciones seguras y prevención de riesgos.

Existen temas básicos para la comprensión de este módulo, por lo tanto, se presentan los siguientes tópicos:

- Conceptos básicos de cibercriminalidad y ciberseguridad.
- Un glosario de terminología básica
- Abreviaturas de normas, estándares y organizaciones internacionales clave
- Normativa internacional contra la cibercriminalidad.
- Entidades u organizaciones internacionales relevantes en el tema.
- Normativas son aplicables en nuestra región, nuestro país o nuestra organización.
- Políticas en materia de seguridad informática o estrategia de ciberseguridad gubernamental y corporativa.
- Casos de Ciberataques en organizaciones económicas mundiales
- Análisis del impacto económico de los ciberataques en el comercio digital y las medidas aplicables para disminuirlo.

A lo largo de este módulo nos desplazaremos desde el concepto base de ciberseguridad, pasando por su antagónico que es la cibercriminalidad, la metodología de análisis y prevención de riesgo, hasta los procesos de obtención de evidencia digital.

Objetivo general del módulo

Al concluir este módulo el alumno será capaz de distinguir y diferenciar los conceptos básicos de la **Ciberseguridad** y la **cibercriminalidad,** además entenderá su responsabilidad individual y social para la preservación de la seguridad informática, teniendo

como resultado final la mejora en la aplicación de medidas de seguridad en su vida diaria, en sus organizaciones y en general en sus actividades económicas.

Preguntas orientadoras de aprendizaje

- ¿Cuál es la diferencia entre ciberseguridad y cibercriminalidad?
- ¿Cuál ha sido el impacto económico global de la cibercriminalidad en la última década?
- ¿Cuáles son los estándares internacionales en seguridad de la información más populares?
- ¿Cuál es el nombre de la Convención internacional en materia de cibercriminalidad más importante del mundo?
- ¿Los países latinoamericanos cuentan con legislación en materia de cibercriminalidad?

UNIDAD I
CONCEPTOS BÁSICOS Y ESTADÍSTICA

Objetivos de aprendizaje

- Conocer los conceptos básicos en materia de ciberseguridad y cibercriminalidad.
- Conocer los ataques informáticos más comunes a nivel internacional.
- Tener acceso a cifras actualizadas de la cibercriminalidad en las economías mundiales.

Al término de este módulo, el participante conocerá y manejará clara y oportunamente los conceptos clave de la cibercriminalidad en el entorno económico del ciberespacio.

I.1. Cibercriminalidad y la ciberseguridad

La cibercriminalidad y la ciberseguridad son conceptos que se encuentran estrechamente ligados ya que no puede existir el uno sin el otro, sólo que son antagónicos; es decir, a mayor sea el grado de ciberseguridad, la incidencia de la cibercriminalidad será menor o podrá contenerse.

La cibercriminalidad como concepto, es ciertamente abstracto, ya que, de manera genérica a nivel internacional, se ha utilizado para definir y englobar todas las conductas ilícitas llevadas a cabo a través de las tecnologías de la información y la comunicación, o en contra de éstas; encontrando en esta categoría ilícitos administrativos, civiles y penales.

Por ejemplo: el uso y divulgación no autorizados de contenidos protegidos por el derecho de autor (de naturaleza administrativa), la afectación a la propia imagen (comúnmente regulado por el derecho civil) y el acceso ilícito a sistemas de cómputo (contemplado como delito).

La primera generación de la cibercriminalidad en la que lo característico era el uso de computadoras para la comisión de delitos, le ha sucedido una segunda época en la que la característica central es que el delito se comete a través de Internet, y, una tercera en la que los delitos están absolutamente determinados por el uso de Internet y las TIC.

Figura 1. Ilícitos en la cibercriminalidad.

Fuente: Elaboración propia

Cabe destacar que la palabra cibercriminalidad es heredada del término anglosajón *cybercrime*, pero en un contexto de derecho continental al que pertenece toda Latinoamérica, lo correcto es hablar de **delitos informáticos,** aunque para efectos prácticos y no jurídicos, de manera genérica estaremos usando el término **cibercriminalidad.**

Por otro lado, el término **ciberseguridad** es una especie del género conocido como seguridad de la información, a su vez, la **seguridad de la información** es la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y los esquemas normativos, que nos exigen niveles de aseguramiento de procesos y de tecnología para elevar el nivel de confianza en la creación, utilización, almacenaje, transmisión, recuperación y disposición final de la información.

Los **activos de información** son los elementos que la **Seguridad de la Información** debe proteger. Por lo que son tres elementos lo que forman los activos:

Figura 2. La triada de la seguridad de la información.

Fuente: Elaboración propia

Ahora bien, dentro de todo lo que comprende la seguridad de la información, se encuentra la ciberseguridad.

Figura 3. El hiperónimo Seguridad de la Información
y la ciberseguridad como parte de esta.

Fuente: Elaboración propia

La ITU define a la **ciberseguridad** como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno.

Cuando una organización comprende correctamente los riesgos que existen respecto de la información y los medios que posee, es capaz de establecer correctas medidas que garanticen la seguridad de la información, lo que forzosamente reducirá

sus vulnerabilidades frente a los cibercriminales. Similar a lo que sucede en una casa, cuando conocemos claramente los accesos que existen, ya sea puertas, ventanas, entradas traseras, chimeneas, etc. estaremos en aptitud de poder diseñar e implementar medidas de seguridad para impedir la entrada a personas ajenas no autorizadas.

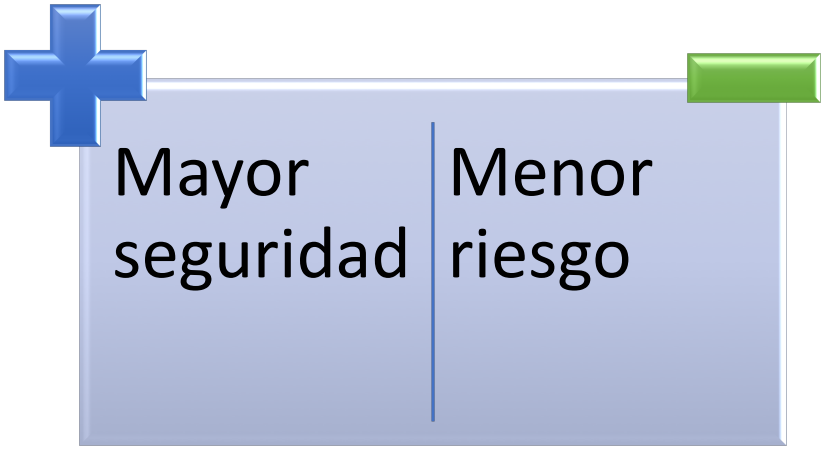

Figura 4. Equilibrio entre seguridad y riesgo.

Fuente: Elaboración propia

I.2. Tipos de ataques informáticos

Un **ataque informático** se puede describir como una actividad hostil contra un sistema, un dispositivo, una aplicación o un objeto que tenga un componente informático. Es una actividad que aspira a conseguir un beneficio para el atacante a costa del atacado. Existen diferentes **tipologías de ataque informático** que dependen de los objetivos que se quieren alcanzar, de los escenarios tecnológicos y de contexto.

Existen ataques que impiden el correcto funcionamiento de un sistema, ataques que buscan comprometer los sistemas, otros que se gestan para obtener datos personales, ya sea que se encuentren contenidos en un sistema de una empresa o bien, a través de técnicas de ingeniería social; y los de ciberactivismo que sostienen causas sociales. Entre los ataques más comunes se encuentran los que pretenden robar datos de tipo financiero y la suplantación de identidad.

Usualmente los ataques informáticos solían ser cometidos de forma aislada por delincuentes conocidos de forma genérica como **hackers,** sin embargo, en los últimos cinco años este tipo de ataques son los menos comunes, ya que la cibercriminalidad se ha convertido en un problema de delincuencia organizada, donde estos ciberdelincuentes que incluso perciben un salario o contraprestación por llevar a cabo estos ataques, o bien, bandas de delincuencia organizada dedicadas comúnmente a delitos como narcotráfico o trata de personas, ahora migran a utilizar los medios electrónicos como mecanismos alternos para delinquir, o bien, para facilitar sus actividades ilícitas.

No existe una clasificación de los ciberataques mundialmente aceptada o estandarizada, sin embargo, los ciberataques de forma genérica podrían catalogarse de la siguiente manera:

Figura 5. Clasificación de ciberataques.

Fuente: Elaboración propia

Como todos los delitos, los ciberataques siempre tienen un móvil, que en ocasiones es más evidente que otras; por ejemplo: el incremento del robo de contraseñas o información confidencial de carácter financiero persigue claramente el objetivo de enriquecerse o hacerse ilícitamente de recursos, y por eso las diferentes modalidades de ciberataques de índole financiero han ido a la alza; pero hay otros, como los ciberataques que tienen como objetivo dañar la infraestructura crítica de un país, en los que no se tiene claro el móvil o el autor intelectual, que puede ser desde un disidente hasta un país enemigo.

En los últimos años los ciberataques más comunes y rentables han sido el popular **phishing,** el **ransomware** y la **suplantación de identidad;** sin embargo, también el robo y la comercialización ilegal de bases de datos personales en el mercado negro han ido al alza.

Los citados delitos son altamente comunes en el comercio electrónico y muchas veces se interrelacionan entre sí; por ejemplo: un cibercriminal a través del uso de la **ingeniería social.** La Ingeniería Social se sustenta en un sencillo principio: "el usuario es el eslabón más débil". Dado que no hay un solo sistema en el mundo que no dependa de un ser humano, la Ingeniería Social es una vulnerabilidad universal e independiente de la plataforma tecnológica.

Entonces, el atacante analiza con detenimiento a su víctima, ya sea una persona física o una organización, y encuentra sus vulnerabilidades, de tal suerte que pueda hallar ese eslabón débil.

Luego de hallar ese eslabón, genera algún tipo de contenido que sea atractivo para la víctima y lanza el anzuelo, lo que se conoce como **phishing.** Si la persona es atrapada por el anzuelo, es capaz de entregar información confidencial creyendo que el remitente es confiable, posteriormente el atacante, con la información obtenida comete otros ilícitos, que pueden ir desde la venta de la información en el mercado negro, hasta la comisión de fraudes o la **suplantación de identidad** para penetrar en una organización y realizar algún otro ataque más profundo.

I.3. Estadísticas internacionales de impacto de la cibercriminalidad en la economía

Hoy en día es muy difícil estimar las cifras exactas del cibercrimen a nivel mundial, los números aproximados se obtienen de las consecuencias económicas que se han sufrido a nivel internacional, pero la falta de una cultura de denuncia o el desconocimiento de la legislación vigente en los países y los mecanismos de lucha contra la ciberdelincuencia, vuelven difícil la tarea estadística.

Tanto los gobiernos de diversas naciones del mundo como empresas de seguridad informática y asociaciones civiles se han dado a la tarea de documentar los efectos nocivos del cibercrimen, pero es un hecho que lo que conocemos es apenas la capa más superficial del problema.

Un estudio publicado en 2018 estimó algunas cifras basadas en los reportes de los cibercrímenes más comunes y es de destacar que el mercado ilegal en línea es uno de los negocios más rentables para los atacantes (860 billones de dólares) siendo lo que más pérdidas económicas genera. Con lo anterior, sumando otro tipo de ilícitos como el robo de propiedad intelectual (500 billones de dólares), el trading de datos (160 billones de dólares) y el *ransomware* o cibercrimen como servicio (entre 1 y 1.6 billones de dólares), el reporte concluye que las ganancias de los cibercriminales alcanzaron los 1.5 trillones de dólares[3].

Caso Wannacry

- Fecha: 12 al 16 de mayo de 2017
- Tipo: Ransomware
- Objetivo: solicitar bitcoins para permitir acceder a los archivos
- Alcance: 360.000 ordenadores afectados en más de 180 países
- Servicios afectados: Salud, transporte, energía o finanzas

[3] "The Web of Profit", Reporte de Bromium elaborado por el investigador en criminología Dr. Mike McGuire, https://learn.bromium.com/rprt-web-of-profit.html, consultado el 13 de noviembre de 2018.

- Países más afectados: China, Rusia, EE. UU. y Reino Unido
- Rescates pagados: Más de 300 transacciones rastreadas y más de 100.000 dólares acumulados en total
- Costo por inactividad mundial: +100 millones de dólares

Fuente: Datos obtenidos del Reporte ¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía?, Deloitte (2017)[4]

No es de extrañar que las empresas de seguridad informática frecuentemente son las que cuentan con métricas más exactas, simplemente porque no todos los ataques se hacen del conocimiento de las autoridades, a veces por desconocimiento y otras más por cuidar la reputación de las organizaciones.

Cuando una empresa sufre un ataque, lo más importante para ellos es la continuidad del negocio y a nadie le interesa que se hagan públicas sus vulnerabilidades, sin embargo, como deben parar los ataques y remediar los eventuales daños, recurren a los consultores privados y a fabricantes de soluciones informáticas para contener los daños, por eso es por lo que muchas veces son estos últimos quienes cuentan con un panorama más objetivo o por lo menos más claro.

Algunos fabricantes tienen mapas en tiempo real que nos pueden ilustrar las rutas de los ataques, es decir, de dónde provienen y el objetivo final.

- Con datos de Kaspersky Lab[5], podemos señalar que el país más atacado en el mundo es Rusia, seguido por Francia en el tercer lugar, Alemania en el cuarto, Estados Unidos en el quinto, y de América Latina, Brasil ocupa el sexto lugar seguido de México en el noveno.
- Para visualizar las ciberamenazas se puede visitar el portal de la empresa Kaspersky Lab, en él se presenta un mapa global con la facilidad de observar la

[4] http://perspectivas.deloitte.com/hubfs/Campanas/WannaCry/Deloitte-ES-informe-WannaCry.pdf
[5] Kaspersky Lab. https://cybermap.kaspersky.com/es/stats/

situación por país. [6] En las imágenes, se muestran datos en tiempo real de ciberamenazas para: OAS- On Acces Scan; ODS – On Demanda Scan; MAV- Mail Anti-virus, WAV – Web Anti-Virus; IDS – Intrusion Detection Scan; VUL – Vulnerability Scan; Kaspersky Anti-Spam; BAD - Botnet Activity Detection.

Las cifras del cibercrimen van mutando día con día y debemos estar monitoreando el estado actual no sólo de nuestra región y país, sino de nuestras organizaciones.

Los riesgos inherentes al cibercrimen van estrechamente ligados a los hábitos de los internautas, ya que el tipo de conexiones y los dispositivos desde los que se conectan a Internet pueden volverlos más susceptibles a ciertos ataques, por ejemplo: una persona que se conecta a Internet a través de una red pública corre el riesgo de sufrir un **ataque de intermediario.**

- La Asociación de Internet MX en su estudio de hábitos de consumo 2017, reveló que el 26% de los usuarios utiliza redes públicas para tener acceso al servicio de Internet, comúnmente parques, plazas públicas, cafés, restaurantes, etc. Aunque el Internet de casa y el del trabajo siguen siendo las conexiones por excelencia.

Cabe destacar que los ciberataques también van mutando y sofisticándose, por ejemplo:

- Los consumidores que han sido víctimas del cibercrimen a nivel global han perdido 172 billones de dólares (Symantec, 2018)
- El 53% de los consumidores han sufrido un cibercrimen o conocen a alguien que lo ha experimentado (Symantec, 2018).
- En 2017, 978 millones de adultos en 20 países experimentaron un cibercrimen. De ellos, 352.7 millones están ubicados en China, 186.44 millones en India y 62.21 en Brasil (Symantec 2018)

[6] Idem

- El 76% de las empresas sufrieron ataques de phishing en 2017, pero los datos muestran que el **smishing (phishing** por SMS) es una amenaza emergente, ya que el 45% de los profesionales de seguridad experimentaron **phishing** a través de llamadas telefónicas (**vishing**) y **smishing.**
- De los 40 millones de ataques de phishing en América Latina sucedidos en los primeros 8 meses del 2018, el 23% sucedieron en Brasil, 17% en Venezuela y 16% en Argentina (Kaspersky Lab)
- Se registraron más de 746 mil ataques de malware diarios durante los últimos 12 meses en América Latina, lo que significa un promedio de 9 ataques de malware por segundo (Kaspersky Lab).

SÍNTESIS DE LA UNIDAD

La cibercriminalidad y la ciberseguridad son conceptos que se encuentran estrechamente ligados.

Como todos los delitos, los ciberataques siempre tienen un móvil, que en ocasiones es más evidente que otra. Un ataque informático se puede describir como una actividad hostil contra un sistema, un dispositivo, una aplicación o un objeto que tenga un componente informático.

Como podemos observar, las cifras que miden las ciberamenazas son dinámicas y van preocupantemente al alza, lo importante es darnos cuenta del nivel de riesgo personal y organizacional para establecer medidas preventivas eficaces.

UNIDAD II

NORMATIVA INTERNACIONAL EN MATERIA DE CIBERCRIMINALIDAD

Objetivos de aprendizaje

El objetivo de esta unidad es distinguir la normativa internacional en materia de cibercriminalidad. Para ello, se revisarán tratados internacionales convenciones y directivas europeas; leyes y reglamentos nacionales; así como, estándares internacionales en materia de seguridad de la información.

Al término de esta unidad el lector será capaz de:

- Identificar el referente legislativo internacional en materia de ciberdelincuencia
- Identificar el avance en la normativa local en materia de cibercriminalidad a nivel internacional.

II.1. Tratados internacionales

Existe un gran mito en torno a la inexistencia de regulación del entorno digital y tecnológico; sin embargo, casi todos los países de los cinco continentes cuentan con regulación en la materia, desde el ámbito civil, el mercantil, el de innovación y protección a la propiedad intelectual, hasta el ámbito penal.

Un estudio realizado por la ONU encontró que *"las divergencias en el alcance de los poderes procesales y las disposiciones sobre cooperación internacional pueden hacer surgir 'racimos' de cooperación nacional que no siempre corresponden de la mejor manera a la naturaleza global del delito cibernético".*[7]

El referente legislativo internacional en la materia es el **Convenio sobre la Delincuencia** del Consejo de Europa (CETS No.185), mejor conocido como **Convenio de Budapest.** Este Convenio fue signado en el año 2001 con el fin de incrementar la eficacia de las investigaciones y procedimientos penales informáticos, así como permitir la obtención de pruebas electrónicas[8]. Este documento sirve a su vez, como una guía a los países para poder desarrollar sus propias legislaciones en la materia, y como un marco de referencia que facilita la cooperación entre los países que se adhieren.

La Red del Convenio de Budapest suma a 61 países, entre aquellos signatarios y los observadores. Entre los países latinoamericanos que participan, se pueden señalar: Argentina, Chile, Costa Rica, Panamá, Paraguay, Colombia, México y Perú.[9]

El convenio consta de 48 artículos, agrupados en cuatro capítulos[10]:

- Capítulo I – Terminología,

[7] Estudio Exhaustivo sobre el delito cibernético, UNODC (2013), https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf

[8] Convenio de Ciberdelincuencia, https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

[9] Países participantes en el Convenio de Budapest, https://www.coe.int/en/web/cybercrime/parties-observers, consultado el 13 de noviembre de 2018.

[10] Para descargar el Convenio de Budapest se puede consultar: https://www.coe.int/en/web/cybercrime/the-budapest-convention

- Capítulo II – Medidas que deberán adoptarse a nivel nacional
    - Sección 1 – Derecho Penal sustantivo
    - Sección 2 – Derecho procesal
    - Sección 3 – Jurisdicción
- Capítulo III – Cooperación Internacional
    - Sección 1 – Principios generales
    - Sección 2 – Disposiciones específicas
- Capítulo IV- Cláusulas finales

Dentro del Capítulo III, referente a la cooperación internacional, se habla sobre la **Red 24/7** y para su conformación se establece que cada parte debe designar un punto de contacto localizable las 24 horas del día para poder dar asistencia inmediata a las investigaciones.

Para facilitar la implementación del Convenio de Budapest se cuenta con el Comité de la Convención del Cibercrimen (T-CY, por sus siglas en inglés) así como con programas de capacitación.

II.2. Convenciones y directivas europeas

Como se mencionó en el apartado anterior, el **Convenio sobre la Cibercriminalidad** fue de origen elaborado por el Consejo de Europa.

Los trabajos para su elaboración comenzaron en 1996, al crear un grupo de expertos para poder lidiar con temas de cibercrimen. Las temáticas de interés fueron:

- Delitos cibernéticos
- Leyes penales y su vínculo hacia la cooperación internacional
- Fuerza coercitiva en un espacio transfronterizo en un ambiente tecnológico
- Jurisdicción de delitos basados en tecnologías de información
- Cooperación internacional cercana para las investigaciones de ciberdelitos

Tras los trabajos realizados, en el año 2001 se tuvo una versión final cuyo principal propósito era: 1) Harmonizar leyes nacionales en materia penal de cibercrimen; 2) establecer las facultades del derecho procesal penal interno necesarias para la investigación y el enjuiciamiento de dichos ciberdelitos; y 3) establecer un régimen rápido y efectivo de cooperación internacional.[11]

Actualmente todos los países europeos miembros del Consejo de Europa cuentan con normativa acorde con el Convenio de Budapest, no sólo leyes sustantivas y adjetivas sino también medidas de cooperación internacional para la persecución de los ciberdelincuentes y por ende la disminución de los cibercrímenes.

II.3. Leyes y Reglamentos nacionales

- La ONU ha identificado que las Leyes nacionales se concentran en establecer figuras delictivas específicas para los principales actos del delito cibernético. La tendencia ahora es abordar medidas investigativas, la jurisdicción, la evidencia electrónica y la cooperación internacional.[12]
- La UNCTAD[13] identifica que el 72% de los países cuentan con legislación en materia de Cibercrimen, un 9% cuenta con proyectos borradores, 18 % no cuentan con ella, y sobre 1% no se dispone de información.
- En el caso de América las cifras no varían de forma relevante, la UNCTAD identifica que 26 países (74%) cuentan con legislación, 3 países (9%) tienen borradores y 6 países (17%) no cuentan con legislación en la materia (Suriname, Guyana, Honduras, Haití, Belice y Honduras).

[11] Reporte Explicativo del Convenio de Cibercrimen, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b

[12] Estudio Exhaustivo sobre el delito cibernético, UNODC (2013), https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf

[13] El Repositorio de Cibercrimen puede ser consultado en: https://sherloc.unodc.org/cld/v3/cybrepo/

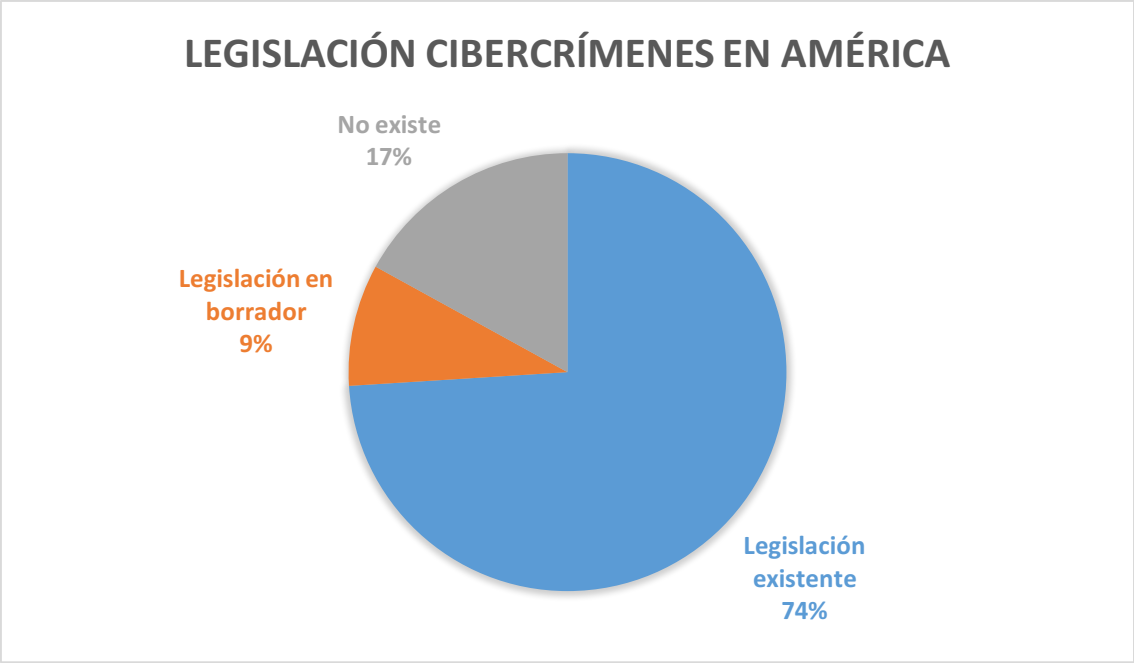

Figura 6. Legislación de Cibercrímenes en América.

Fuente: Elaboración propia con información de UNCTAD.

- La siguiente tabla resume la legislación nacional de los países de América Latina y el Caribe. A su vez, se señalan los delitos que tal regulación contempla.

País	Ley que lo contempla delitos informáticos	Delito contemplado
Antigua y Barbuda	Ley de Uso Indebido de las Computadoras	• Aseguramiento ilícito de programas o datos contenidos en las computadoras • aseguramiento de programas informáticos o datos almacenados de cualquier equipo de cómputo con intensiones maliciosas • Actividades similares al hacking o apropiación por vía remota de información generada y almacenada en computadoras ajenas.
Argentina	Código Penal	• Posesión sin la debida autorización o exceso de la posesión que tenga de un sistema informático de acceso restringido y su punibilidad • Revelación de hechos, actuaciones, documentos o datos que por ley son secretos.

País	Ley que lo contempla delitos informáticos	Delito contemplado
Bahamas	Ley de Uso Indebido de las Computadoras	• Aseguramiento ilícito de cualquier programa o datos contenidos en una computadora o una ofensa derivada de dicho aseguramiento • Aseguramiento ilícito de cualquier programa o datos contenidos en una computadora o una ofensa derivada de dicho aseguramiento • Actividades similares al hacking o apropiación por vía remota de información generada y almacenada en computadoras ajenas.
Barbados	Ley de Uso Indebido de las Computadoras	• Aseguramiento ilícito de cualquier programa o datos contenidos en una computadora o una ofensa derivada de dicho aseguramiento. • Aseguramiento de programas informáticos o datos almacenados de cualquier equipo de cómputo con intensiones maliciosas. • Actividades similares al hacking o apropiación por vía remota de información generada y almacenada en computadoras ajenas.
Bolivia	Código Penal Federal	• Alteración Acceso y Uso Indebido de Datos Informáticos
Brasil	Ley N. 8069	• Distribución, exposición o venta de material pornográfico infantil o adolescente por medios electrónicos
Chile	Ley Relativa a Delitos Informáticos	• Daños que se puedan cometer contra el hardware • Sabotaje informático • Espionaje informático
Colombia	Ley de Protección de la Información y de los Datos	• Acceso abusivo a un sistema informático
Costa Rica	Código de Normas y Procedimientos Tributarios, Ley General de Aduanas y el Código Penal Federal.	• Acceso desautorizado a la información o bases de datos de la Administración Tributaria. • Ley General de Aduanas: establece 4 supuestos que podrán ser considerados como Delitos informáticos y su pena • Código Penal Federal: delito de violación a las comunicaciones electrónicas y su pena.
República Dominicana	Ley 53/07 Contra Crímenes y Delitos de Alta Tecnología	Crímenes y Delito Contra la Confidencialidad, Integridad y Disponibilidad de Datos y Sistemas de Información (artículos del 5 al 11) • Códigos de Acceso • Clonación de Dispositivos de Acceso • Acceso ilícito

País	Ley que lo contempla delitos informáticos	Delito contemplado
		• Uso de Datos por acceso ilícito • Acceso ilícito para servicio a terceros • Beneficio de actividades de un tercero • Dispositivos fraudulentos • Interceptación e intervención de datos o señales • Daño o alteración de datos • Sabotaje Delitos de contenido • Atentado contra la vida de las personas • Robo mediante la utilización de alta tecnología • Obtención ilícita de fondos • Transferencias electrónicas de fondos • Estafa • Chantaje • Robo de identidad • De la falsedad de documentos y firmas • Uso de equipos para invasión de privacidad • Comercio ilícito de bienes y servicios • Difamación • Injuria pública • Atentado sexual • Pornografía infantil • Adquisición y posesión de pornografía infantil Delitos de la Propiedad Intelectual y afines • Delitos relacionados a la Propiedad Intelectual y fines, contemplados de forma específica en la Ley No.20-00, del 8 de mayo del año 2000, sobre Propiedad Industrial, y la Ley No.65-00, del 21 de agosto del año 2000 Delitos contra las telecomunicaciones • Llamada de retorno de tipo fraudulento • Fraude de proveedores de servicio de información líneas tipo 1-976 • Redireccionamiento de llamadas de larga distancia • Robo de línea • Desvío de trafico • Manipulación ilícita de equipos de telecomunicaciones • Intervención de centrales privadas Crímenes y delitos contra la nación y actos de terrorismo • Crímenes y delitos contra la nación • Actos de terrorismo

País	Ley que lo contempla delitos informáticos	Delito contemplado
Ecuador	Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley No. 2002-67)	• Definición y supuestos de delito informático.
Estados Unidos de América	Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030)	• Pornografía infantil • Infracciones a los Derechos de Autor (distribución comercial por medios electrónicos)
Guatemala	Código Penal Federal	• Definición y pena de interferencia en los datos.
Guyana	Ley de Interceptación de Comunicaciones 2008	• Interferencia de las comunicaciones • Protección de Datos Personales en Posesión de Prestadores de servicios de Telecomunicaciones
Honduras	Código Penal Federal	• Definición y pena de interferencia en los datos.
Jamaica	Ley de Interceptación de Comunicaciones	• Protección de Datos Personales en Posesión de Prestadores de servicios de Telecomunicaciones
México	Código Penal Federal	• Revelación de secretos: definido y sancionado en los artículos del 210 al 211 Bis del Código Penal Federal. • Acceso ilícito a sistemas y equipos de informática: definido y sancionado en los artículos del 211 Bis1 al 211 bis 7 del Código Penal Federal.
Nicaragua	Código Penal Federal	• Delito de Acceso y uso no autorizado de información
Panamá	Código Penal Federal	• Definición de delito informático y pena.
Paraguay	Código Penal Federal	• Violación del secreto de la comunicación • Alteración de datos • Sabotaje de computadoras • Operaciones fraudulentas por computadora • Pornografía relativa a niños y adolescentes. • Alteración de datos relevantes para la prueba

País	Ley que lo contempla delitos informáticos	Delito contemplado
Perú	Código Penal Federal	• Delito Informático • Alteración, daño y destrucción de base de datos, sistema, red o programa de computadoras • Delito informático agravado • Pornografía infantil
San Vicente y las Granadinas	Ley de Transacciones Electrónicas	• Definición y pena para los delitos informáticos.
Suriname	Código Penal Federal	• Alteración, daño y destrucción de base de datos, • Sistema, red o programa de computadoras • Delito informático agravado.
Trinidad y Tobago	Ley de Uso Indebido de las Computadoras	• Aseguramiento ilícito de cualquier programa o datos contenidos en una computadora o una ofensa derivada de dicho aseguramiento, así como su pena.
Venezuela	Ley Especial contra los Delitos Informáticos	Delitos Contra los Sistemas que Utilizan Tecnologías de Información 1. Acceso indebido 2. Sabotaje o daño a sistemas 3. Favorecimiento culposo del sabotaje o daño 4. Acceso indebido o sabotaje a sistemas protegidos 5. Posesión de equipos o prestación de servicios de sabotaje 6. Espionaje informático 7. Falsificación de documentos Delitos contra la Propiedad 1. Hurto 2. Fraude 3. Obtención indebida de bienes y servicios 4. Manejo fraudulento de tarjetas inteligentes 5. Apropiación de tarjetas inteligentes o instrumentos análogos 6. Provisión indebida de bienes o servicios 7. Posesión de equipo para falsificaciones Delitos Contra la Privacidad de las Personas y de las Comunicaciones 1. Violación de la privacidad de la data o información de carácter personal 2. Violación de la privacidad de las comunicaciones 3. Revelación indebida de data o información de carácter personal

País	Ley que lo contempla delitos informáticos	Delito contemplado
		Delitos Contra Niños, Niñas o Adolescentes 1. Difusión o exhibición de material pornográfico. 2. Exhibición pornográfica de niños o adolescentes. Delitos Contra el Orden Económico 1. Apropiación de propiedad intelectual 2. Oferta engañosa
Sin legislación	Belice, Cuba, Granada, Haití, Santa Lucía	

Tabla 1. Legislación sobre delitos informáticos en América Latina y el Caribe.

Fuente: Elaboración propia con información de UNCTAD[14]

II.4. Estándares internacionales en materia de seguridad de la información

Existen diversos estándares técnicos en materia de seguridad de la información. Algunos entes reconocidos por la OCDE son: la Organización Internacional de Normalización (ISO), el Grupo de Trabajo de Ingeniería de Internet (IETF), el World Wide Web Consortium (W3C), la Organización para el Avance de las Normas de Información Estructurada (OASIS).[15] Cabe señalar que los estándares de seguridad de la información tienen un vínculo importante con el manejo de riesgos.

De forma particular, sobresalen los siguientes estándares **ISO:**

- ISO/IEC 31000:2009 - Manejo de riesgos, principios y guías
- ISO Guide 73 –Manejo de riesgos, vocabulario

[14] Información tomada de la base de Legislación en Cibercrímenes de UNCTAD, https://unctad.org/en/Docs/Cyberlaw/CC.xlsx

[15] Digital Security Risk Management for Economic and Social Prosperity, OCDE (2015), http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf

- ISO/IEC 27000 serie – Tecnologías de información – Técnicas de seguridad

Para conocer más ser recomienda:

- Leer documento sobre qué es un Sistema de Gestión de la Seguridad de la Información. http://www.iso27000.es/download/doc_sgsi_all.pdf

Por otra parte, el **NIST** (*National Institute of Standards and Technology* de Estados Unidos) desarrolló un Marco de Referencia para mejorar la infraestructura crítica de seguridad[16]. El uso de este marco de referencia es voluntario para aquellos dueños operadores de infraestructuras críticas, su fin es tener una forma costo-efectiva para establecer y controlar medidas de seguridad informática.

SÍNTESIS DE LA UNIDAD

- **El Convenio de Ciberdelincuencia, también conocido como Convenio de Budapest, favorece la armonización de la legislación en la materia, así como la cooperación internacional.**
- **La legislación local, a nivel mundial y Latinoamérica, muestra un avance importante, si bien aún existen países en América que carecen de ella.**

[16] Marco de Referencia NIST para mejorar infraestructuras de seguridad, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

UNIDAD III

PROCESO PARA DETECTAR Y MEJORAR EL ESTADO DE VULNERABILIDADES MATERIA DE CIBERCRIMINALIDAD

Objetivos de aprendizaje

El objetivo de esta unidad es describir el proceso para detectar y mejorar el estado de vulnerabilidades materia de cibercriminalidad.

Al término de esta unidad el lector será capaz de:

- Describir cómo se evalúan las medidas de seguridad
- Describir cómo se preserva y presenta evidencia digital
- Enunciar cómo se documentan los incidentes de seguridad

III.1. Metodología para el análisis de vulnerabilidades de una organización

Hoy en día, es fundamental para todas las empresas, incluyendo aquellas que se dedican al comercio electrónico o digital, realizar constantemente análisis de vulnerabilidades al interior de su organización para prevenir ciberataques o por lo menos minimizar los riesgos inherentes a éstos, a nivel internacional existen diversos protocolos y estándares diseñados para poder detectar y medir estas vulnerabilidades.

Una vez que se han identificado estas debilidades o fallas en la seguridad de los sistemas internos, es necesario poner en marcha una política y de remediación, así como las tareas a llevar a cabo para disminuir los riesgos encontrados, además de esto existen herramientas tecnológicas de seguridad que pueden auxiliar en el monitoreo y disminución de estos riesgos.

En la siguiente liga podrá encontrar un ejemplo de metodología diseñada por un estudiante de la Universidad Javeriana: http://www.javeriana.edu.co/biblos/tesis/ingenieria/tesis181.pdf

III.2. Atención a incidentes

Los diferentes ataques que sufren los sistemas conectados a Internet son conocidos como incidentes de seguridad informática. Éstos amenazan el buen funcionamiento de cualquier organización y violan implícita o explícitamente las políticas de seguridad.

Internet se ha convertido en el medio de interconexión global por excelencia, gran cantidad de transacciones de negocios se realizan de esta forma, por lo que se requieren mecanismos de respuestas rápidas a incidentes de seguridad para evitar que la organización se exponga a pérdidas irreversibles. Se le denomina un incidente de

seguridad informática a cualquier evento que sea considerado una amenaza para la seguridad de un sistema.

Existen diversos tipos de amenazas y seguirán apareciendo cada vez más. Entre las más conocidas tenemos:

- Instalación de **software malicioso (malware)**
- Acceso sin autorización al sistema o a sus datos
- Interrupciones indeseadas
- Denegación de servicios
- Uso desautorizado de las bases de datos
- Cambio en el hardware, firmware o software del sistema

Es posible clasificar los incidentes de seguridad en dos tipos:

1. Incidentes automáticos
2. Incidentes manuales

Se denominan incidentes automáticos a los incidentes producidos por programas de cómputo tales como virus, gusanos y troyanos. Los incidentes manuales son aquellos incidentes en los que de manera intencional se ataca un sistema utilizando, por ejemplo, escaneo de vulnerabilidades, inyección SQL o **ingeniería social,** aunque bajo ciertas circunstancias, también se pueden realizar de forma automática.

Siempre que sea posible, se deseará evitar que, en primer lugar, se produzcan incidentes de seguridad. No obstante, resulta imposible evitar todos los incidentes de seguridad. Cuando se produce un incidente de seguridad, se debe garantizar que se minimice su repercusión. Para minimizar la cantidad y repercusión de los incidentes de seguridad, debe seguir estas pautas:

- Establecer claramente y poner en práctica todas las directivas y procedimientos. Muchos incidentes de seguridad están provocados accidentalmente por el personal de TI, que no ha seguido o no ha entendido los procedimientos de

administración de cambios, o bien no ha configurado correctamente los dispositivos de seguridad, como pueden ser los firewalls o los sistemas de autenticación. Las directivas y los procedimientos se deben probar exhaustivamente para garantizar que son prácticos y claros, y que ofrecen el nivel de seguridad apropiado.

- Obtener compatibilidad administrativa para las directivas de seguridad y el control de incidentes.
- Evaluar de forma regular las vulnerabilidades del entorno. Las evaluaciones deben ser realizadas por un experto en seguridad con la autoridad necesaria (con derechos de administrador de los sistemas) para llevar a cabo estas acciones.
- Comprobar con regularidad todos los sistemas y dispositivos de red para garantizar que tienen instaladas las revisiones más recientes.
- Establecer programas de formación sobre la seguridad tanto para el personal de TI como para los usuarios finales. La mayor vulnerabilidad de cualquier sistema es el usuario carente de experiencia. El gusano ILOVEYOU aprovechó de forma eficaz esa vulnerabilidad entre el personal de TI y los usuarios finales.
- Se deben enviar boletines de seguridad que recuerden a los usuarios sus responsabilidades y restricciones, junto con la advertencia de que se pueden emprender acciones legales en caso de infracción. Se debe buscar asesoramiento legal para asegurarse de que la redacción de las notificaciones de seguridad es apropiada.
- Desarrollar, implementar y poner en práctica una directiva que requiera contraseñas seguras.
- Supervisar y analizar con regularidad el tráfico de red y el rendimiento del sistema.
- Comprobar con regularidad todos los registros y mecanismos de registro, incluidos los registros de eventos del sistema operativo, los registros específicos de aplicación y los registros de sistema de detección de intrusiones.
- Comprobar los procedimientos de restauración y copia de seguridad. Debe saber dónde se almacenan las copias de seguridad, quién tiene acceso a ellas y

los procedimientos para la restauración de datos y la recuperación del sistema. Asegúrese de que las copias de seguridad y los medios se comprueban con regularidad mediante la restauración selectiva de datos.

Si pudiéramos enlistar los pasos más frecuentes a seguir, luego de un incidente, serían los siguientes:

Pasos a seguir tras un incidente

1. Evaluación inicial
2. Respuesta inicial
3. Reunir pruebas forenses
4. Implementar una solución temporal
5. Enviar comunicaciones
6. Consultar a las autoridades locales pertinentes
7. Implementar soluciones permanentes
8. Determinar la repercusión financiera en el negocio

III.3. Preservación y presentación de evidencia digital

Podemos definir el **Análisis Forense Digital** como un conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial.

Por evidencia digital se entiende al conjunto de datos en formato binario, esto es, comprende los archivos, su contenido o referencias a éstos (metadatos) que se encuentren en los soportes físicos o lógicos del sistema atacado.

Dentro del Análisis Forense Digital (en adelante AFD), podemos destacar las siguientes fases:

1. Identificación del incidente.

2. Recopilación de evidencias.
3. Preservación de la evidencia.
4. Análisis de la evidencia.
5. Documentación y presentación de los resultados.

Si tras la realización de un primer análisis existen sospechas de que el incidente se ha provocado desde el interior de su red, tendrá que plantearse la posibilidad de llevar a cabo una investigación interna a la organización para depurar responsabilidades, bastará para este propósito recopilar información suficiente tanto en cantidad como calidad para poder tomar acciones disciplinarias posteriores, sin llegar a los tribunales.

Pero si el incidente, realizado por atacantes internos o externos, ha provocado daños importantes a su organización ya sean económicos, de imagen corporativa o su reputación ha quedado en entredicho, puede considerar abrir un proceso judicial contra sus atacantes. En este caso la investigación técnica deberá ser tratada como una investigación pericial técnica, incorporando procedimientos en materia de probatoria judicial, pues una evidencia digital no será considerada como prueba en un proceso judicial hasta que el juez así lo determine o si la legislación del país la reconoce como tal.

Para conocer más se sugiere:

- ver el video sobre el análisis forense digital: https://www.youtube.com/watch?v=yQYCmvplMDQ
- Leer el Artículo sobre las fases y herramientas de un Análisis Forense Digital https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

III.4. Documentación de incidentes, proceso de mejoras y actualización de medidas de seguridad

Como una de las fases finales, es necesario documentar los incidentes de seguridad, esto es de suma importancia, ya que, basados en la documentación de los incidentes ocurridos, en un futuro podrán tomarse las acciones pertinentes para mejorar la seguridad y actualizar las medidas que sean necesarias.

El resultado de este proceso de documentación debe compartirse al interior de la organización para que los demás miembros puedan conocerlo e implicarse en las tareas que en adelante conllevará, para ello debe ser redactado de forma clara y simple, ya que los receptores de este documento son de diversas áreas y niveles de formación.

Básicamente debería contener lo siguiente:

- Estado previo de la organización al momento del desastre
- Descripción de la situación de desastre
- Identificación de información, procesos y recursos que deben recuperarse
- Responsabilidades
- Plan de acción incluyendo tareas y calendario de actividades y entregas
- Lista de recursos que deberán implicarse

SÍNTESIS DE LA UNIDAD

- Una vez que se han identificado estas debilidades o fallas en la seguridad de los sistemas internos, es necesario poner en marcha una política y de remediación.
- Para minimizar la cantidad y repercusión de los incidentes de seguridad, debe seguir una serie de acciones.
- Para que las evidencias digitales sean aceptadas legalmente en un proceso judicial se puede hacer uso de los principios y técnicas del análisis forense digital.

Bibliografía

- Convenio de Budapest https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
- Investigación y aplicación de la Ley en los ciberincidentes https://www.sites.oas.org/cyber/Documents/2016%20-%20Investigación%20y%20aplicación%20de%20la%20ley%20a%20los%20incidentes%20cibernéticos-Cameron%20Brown.pdf
- https://nic.ar/index.php/es/enterate/novedades/que-es-convenio-budapest
- Área Digital Asociación por los Derechos Civiles, La Convención de Cibercrimen de Budapest y América Latina, Breve guía acerca de su impacto en los derechos y garantías de las personas. Volumen 1 https://adcdigital.org.ar/wp-content/uploads/2018/03/Convencion-Budapest-y-America-Latina.pdf
- Manual de respuesta a incidentes https://www.sites.oas.org/cyber/Documents/Manual%20para%20el%20Manejo%20de%20Incidentes.pdf
- ARPAGIAN, Nicolás "La Cybérsecurité". Que sais je? 2018 Francia
- State of Cybersecurity Report 2018. https://www.wipro.com/content/dam/nexus/en/service-lines/applications/latest-thinking/state-of-cybersecurity-report-2018.pdf
- Tendencias y oportunidades en Ciberseguridad. OAS – INCIBE https://www.sites.oas.org/cyber/Documents/2016%20-%20Tendencias%20y%20oportunidades%20en%20ciberseguridad-Alberto%20Bohorquez.pdf