cybermonday.cl

# *Ciber*
# Diccionario

01 ***Activo de información:*** Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

02 ***Adware:*** Es cualquier programa que automáticamente va mostrando publicidad al usuario durante su instalación o durante su uso y con ello genera beneficios a sus creadores.

03 ***Amenaza:*** Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.
Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

04 ***Ataques de negación de servicio (DoS):*** Tienen como objetivo degradar la calidad de un servicio, por ejemplo una página web, y dejarlo en un estado no funcional. Para lograrlo, se saturan los recursos del sistema que aloja el servicio que se quiere interrumpir, enviándoles una avalancha de peticiones que no son capaces de atender. Los ataques DDoS muchas veces son llevados a cabo por bots, sistemas infectados cuyo propietario muchas veces desconoce que sus dispositivos forman parte de esta red maliciosa.

05 ***Ataques a infraestructuras críticas mediante el ciberespacio:*** Es la alteración en el funcionamiento de infraestructuras críticas (físicas o de la información) realizada por medios electrónicos. Por ejemplo: disrupción masiva de sistemas financieros, intervención de servicios básicos, daños físicos a infraestructuras físicas, y otros relacionados.

06 ***Antivirus:*** Es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso (virus, troyanos, gusanos, etc.), así como proteger los equipos de otros programas peligrosos conocidos genéricamente como malware.

07 ***Autenticación:*** Procedimiento para comprobar que alguien es quién dice ser cuando accede a un computador o a un servicio online. Este proceso constituye una funcionalidad característica para una comunicación segura.

08 ***Autentificación de 2 factores (2FA):*** Desde fines de los años noventa estamos familiarizados con el uso de usuario/contraseña para controlar el acceso sin autorización a nuestros dispositivos. El usuario le dice al sistema o aplicación quienes somos; la contraseña nos autentica, es decir, es un método para comprobar que realmente somos quienes decimos ser. También podemos hacerlo con un token USB o una tarjeta de coordenadas o con una huella, el iris, la voz o el rostro.

09 ***Aviso Legal:*** Un aviso legal es un documento, en una página web, donde se recogen las cuestiones legales que son exigidas por la normativa de aplicación. El aviso legal puede incluir: 1. Términos y condiciones de uso 2. Política de privacidad y protección de datos si recogen datos de carácter personal (formularios, registro de usuarios,...etc.) 3. Información relativa al uso de cookies.

10 ***Backup:*** Copia de seguridad que se realiza sobre archivos o aplicaciones contenidas en un computador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados.

11 ***Botnet:*** Es un conjunto de computadores (denominados bots) controlados remotamente por un atacante que pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de spam o ataques de DDoS. Las botnets se caracterizan por tener un servidor central (C&C, de sus siglas en inglés Command & Control) al que se conectan los bots para enviar información y recibir comandos.

12 ***Cibercrimen:*** Son los actos delictuales donde el ciberespacio es el objeto del delito o su principal herramienta para cometer ilícitos contra individuos, organizaciones, empresas o gobiernos.

13 ***Ciberespacio:*** Es un ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones sociales que se verifican en su interior.

14 ***Ciberhigiene:*** Conducta personal referida a la actitud de cautela y cuidado que debe tener un usuario al conectarse a la red, y que va desde el cuidado de las claves personales, el visitar sitios dudosos, conexiones en redes abiertas, establecer nexos con desconocidos a través de las redes sociales, o compartir información a través de medios extraíbles entre otros.
En internet no todo es lo que parece, por lo que la educación temprana de los riesgos que conlleva el conectarse deben ser parte de nuestros hábitos.

15 ***Ciberseguridad:*** Es tanto una condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones que se verifican en el ciberespacio, como el conjunto de políticas y técnicas destinadas a lograr dicha condición.

16 ***Cookie:*** Es un pequeño archivo que almacena información enviada por un sitio web y que se guarda en el equipo del usuario, de manera que el sitio web puede consultar la actividad previa de éste y así recaba información sobre sus hábitos de navegación. Esto puede significar un ataque contra la privacidad de los cibernautas y por lo mismo hay que tener cuidado con ellas.

17 ***Confidencialidad:*** Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad de la información constituye la piedra angular de la seguridad de la información. Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información.

18 ***Control parental:*** Conjunto de herramientas o medidas que se pueden tomar para evitar que los menores de edad hagan un uso indebido del computador, accedan a contenidos inapropiados o se expongan a riesgos a través de Internet.


19 ***Cómo evitar fraudes (phishing, pharming y spear-phishing):*** Realizar operaciones en sitios seguros, verificando que la URL comiencen con https://. Tener presente que los bancos no solicitan actualizaciones de datos por correo electrónico o teléfono, como tampoco el ingreso de claves, salvo los datos necesarios al momento de realizar alguna operación. Verificar la barra de direcciones en el navegador, cuando se esté operando en sitios de Bancarios.

20 ***CSIRT:*** Equipo de respuesta ante incidentes de seguridad informática del Gobierno de Chile. Su tarea es proteger el uso libre y confiable de los sistemas y plataformas digitales de la población, a través del monitoreo constante de sitios de internet de organismos públicos, de un equipo técnico y certificado, de la detección de vulnerabilidades, gestión de incidentes y mejora continua de los estándares de ciberseguridad del país.

21 ***Dato informático:*** Toda representación de hechos, información o conceptos expresados de cualquier forma que se presente a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

22 ***Delito informático:*** Comportamientos ilícitos que se llevan a cabo mediante herramientas electrónicas para atentar contra la seguridad de los sistemas informáticos o los datos procesados por ellos.

23 ***Dirección IP:*** Las direcciones IP (del acrónimo inglés IP para Internet Protocol) son un número único e irrepetible con el cual se identifica a todo sistema conectado a una red.

24 ***Disponibilidad:*** Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran. Junto con la integridad y la confidencialidad son las tres dimensiones de la seguridad de la información.

25 ***HTTPS:*** Es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, cifrado mediante un algoritmo de cifrado simétrico cuya clave ha sido previamente intercambiada entre el navegador y el servidor. Es utilizado por cualquier tipo de servicio que requiera el envío de datos personales o contraseñas, entidades bancarias, tiendas en línea o pago seguro.

26 ***Incidente de seguridad:*** Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

27 ***Incidentes internos:*** Fugas involuntarias de información, interrupción accidental de sistemas informáticos, u otros incidentes involuntarios que pueden afectar la confidencialidad, integridad, disponibilidad y trazabilidad de la información.

28 ***Ingeniería social:*** Las técnicas de ingeniería social son tácticas utilizadas para obtener información datos de naturaleza sensible, en muchas ocasiones claves o códigos, de una persona. Estas técnicas de persuasión suelen valerse de la buena voluntad y falta de precaución de la víctima.

29 ***Integridad:*** La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales. La integridad, la disponibilidad y la confidencialidad constituyen las dimensiones claves en la seguridad de la información, ya que de un lado, se pretende evitar los accesos no autorizados a los datos, y de otro, se garantiza la no alteración de los mismos.

30 ***Malware:*** Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Abarca virus, gusanos, troyanos, backdoors y spyware, siendo todos programas de carácter dañino o lesivo.

31 ***Parche de seguridad:*** Un parche de seguridad es un conjunto de cambios que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos. Generalmente los parches de seguridad son desarrollados por el fabricante del software tras la detección de una vulnerabilidad en el software y pueden instalarse de forma automática o manual por parte del usuario.

32 ***Phishing:*** Es la denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial de forma fraudulenta, suplantando la personalidad de una persona o empresa de confianza para que el receptor de una comunicación electrónica aparentemente oficial (vía e-mail, fax, SMS o telefónicamente) crea en su veracidad y facilite, de este modo, los datos privados que resultan de interés para el timador.

33 ***Ransomware:*** El ciberdelincuente toma control del equipo infectado y secuestra la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera, extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos.

34 ***Respuesta a incidentes:*** Ante la sospecha o verificación de un incidente de seguridad, es necesario contar con un plan de acción en caso de que la información se vea comprometida. Se recomienda revisar los sistemas encargados de identificar accesos no autorizados como cortafuegos o logs, comprobar si se están llevando a cabo tareas de mantenimiento, identificar a grandes rasgos la gravedad del ataque y documentar toda la información recogida.

35 ***Robo de información de tarjetas de crédito/débito:*** Es común el método de la clonación cuando de por medio hay un dispositivo por donde pasa la tarjeta. Otra forma es configurando los sitios web que ofrecen venta de servicios o productos. Durante el checkout, la información se transfiere al ladrón en lugar que a la ubicación segura. Una buena forma de evitar esta situación es siempre hacer uso de los sitios web HTTPS en la dirección del buscador y sólo comprar en sitios que codifican su información.

36 ***Router:*** Es un dispositivo que distribuye tráfico de red entre dos o más diferentes redes. Un router está conectado al menos a dos redes, generalmente LAN o WAN y el tráfico que recibe procedente de una red lo redirige hacia la(s) otra(s) red(es). En términos domésticos un router es el dispositivo que proporciona el proveedor de servicios de telefonía (o ISP) y que permite conectar nuestra LAN doméstica con la red del IS.

37 ***Servidor:*** Puede entenderse como servidor tanto el software que realiza ciertas tareas en nombre de los usuarios, como el computador físico en el cual funciona ese software, una máquina cuyo propósito es proveer y gestionar datos de algún tipo de forma que estén disponibles para otras máquinas que se conecten a él.

38 ***Spam:*** Es correo basura digital, esto es, comunicaciones no solicitadas que se envían de forma masiva por Internet o mediante otros sistemas de mensajería electrónica. El spamming es el acto de enviar estos mensajes, mientras la persona que participa en esta práctica se la denomina spam-mer. Normalmente, el spam es de naturaleza comercial y, aunque es preocupante, no es necesariamente malicioso o fraudulento (aunque puede serlo).

39 ***Spyware:*** Es un malware que recopila información de un computador y después la envía a una entidad remota sin el conocimiento o el consenti-miento del propietario del computador. El término spyware también se utiliza más ampliamente para referirse a otros productos como adware, falsos antivirus o troyanos.

40 ***Suplantación de identidad en línea:*** Es la actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude, acoso (cyberbulling). Un ejemplo es, en las redes sociales, crear un perfil de otra persona e interactuar con otros usuarios haciéndose pasar por ella.

41 ***Troyano:*** Se trata de un tipo de malware o software malicioso que se caracteriza por carecer de capacidad de autoreplicación. Generalmente, este tipo de malware requiere del uso de la ingeniería social para su propagación. Una de las características de los troyanos es que al ejecutarse no se evidencian señales de un mal funcionamiento.

42 ***URL:*** Las siglas URL (Uniform Resource Locator) hacen referencia a la dirección que identifica un contenido colgado en Internet. Las URL permiten tener acceso a los recursos colgados en una red gracias a la dirección única y al servicio de DNS que permite localizar la dirección IP del contenido al que se quiere acceder

43 ***Uso correcto de claves:*** Sólo deben ser de conocimiento del usuario, y jamás compartirlas con terceros desconocidos. Cambiarlas con frecuencia y utilizar de preferencia claves que contengan letras, números y símbolos. Jamás dejarlas escritas en algún lugar visible.

44 ***Virus:*** Programa diseñado para que al ejecutarse, se copie a sí mismo adjuntándose en aplicaciones existentes en el equipo. De esta manera, cuando se ejecuta una aplicación infectada, puede infectar otros archivos. A diferencia de otro tipo de malware, como los gusanos, se necesita acción humana para que un virus se propague entre máquinas y sistemas.

45 ***Vulnerabilidad:*** Fallos o deficiencias de un programa que puede permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota. Los agujeros de seguridad pueden ser aprovechados por atacantes mediante exploits (fragmento de software, de datos o secuencia de comandos o acciones) para acceder a los sistemas con fines maliciosos.

46 ***Wifi:*** Una red wifi es una red de dispositivos inalámbricos interconectados entre sí y generalmente también conectados a Internet a través de un punto de acceso inalámbrico. Se trata por tanto de una red LAN que no utiliza un cable físico para el envío de la información.

# Tips para este cybermonday.cl

01

***Cuidar las claves personales,*** no usarlas en cualquier lado, tratar de tener claves diferentes

**Registrarse**

¿Aún no tienes una cuenta? Créala ahora.

Usuario

123456

Recuérdame ¿Olvidaste la contraseña?

**Registrarse**

¿Aún no tienes una cuenta? Créala ahora.

Usuario

kZs6X}p3yT

Recuérdame ¿Olvidaste la contraseña?

02


***No ocupar acceso de internet de wifi en cualquier lugar o que uno no conoce,*** ya que la mayoría de los robos de datos se producen normalmente en los acceso de wifi desconocidos.

03

Ser conscientes de los sitios web que vamos a visitar y que no tienen acreditación de seguridad, y que no sabemos nada ¿Cómo podemos verificar esto? mediante un ***candado verde al costado izquierdo de la URL***

***https://www.cyber.cl/***

04

***No abrir los correos de direcciones que uno no conoce,*** siempre ver los orígenes de quien están mandando los mail

# Tips para este cybermonday.cl

05


***Revisar con extrema precaución la dirección de los sitios web,*** ya que, un mínimo cambio en la dirección de la url, puede ser un sitio falso que le robará la información personal de sus cuentas mediante ***el phishing***

https://www.elbanconacionaldechile.cl

https://www.banconacionaldechile.cl

06

***Ingresar de manera directa y con la dirección del sitio donde queremos comprar.***

Tiendas de ropa cerca

https://www.tiendaderopa.cl