GLOSARIO
DE TÉRMINOS DE
CIBERSEGURIDAD

UNIVERSIDAD CATÓLICA DE TEMUCO

DIRECCIÓN DE INFORMÁTICA
VICERRECTORÍA DE ADMINISTRACIÓN
Y ASUNTOS ECONÓMICOS

ÍNDICE

A

Adware 1
Antivirus 1
Arquitectura de seguridad 1
Ataque de Cadena de Suministro (Supply Chain Attack) 1
Autenticación 1
Autenticación multifactor (MFA) 1

B

Backup 1
Biometría 1
Botnet 2
Bots (Zombies) 2
Brecha de Seguridad 2

C

Certificado digital 2
Ciberataque 2
Ciberespionaje 2
Ciberseguridad 2
Cifrado 2
Clave privada 2
Clave pública 3
Código malicioso 3
Computación en la nube 3
Confidencialidad 3
Consentimiento Informado Digital 3
Contraseña Robusta 3
Cookie 3
Cortafuegos (Firewall) 3
Cortafuegos de próxima generación (NGFW) 3
Criptoanálisis 4
Criptografía 4
Cultura de seguridad 4

D

Data breach (Violación de datos) 4
DDoS (Ataque de Denegación de Servicio Distribuido) 4
Deep Web 4
Deepfake 4
Descifrado 4
Digitalización 4
Dirección IP 5
Dirección IP dinámica 5
DMZ (Zona Desmilitarizada) 5
DNS (Sistema de Nombres de Dominio) 5
Dominio 5
DoS (Denegación de Servicio) 5
Doxing 5

E

E-mail Spoofing 5
EDR (Endpoint Detection and Response) 5
Exploit 6
Exploit Zero-Day 6

F

Factor de autenticación 6
Falsificación 6
Firma digital 6
Firmware 6

G

Gestión de identidades y accesos (IAM) 6
Gestión de Riesgos 6
Gestión de Vulnerabilidades 7
Gobernanza de Datos 7

H

Hacker ético 7
Honeypot 7
Huella Digital 7

I

Identidad digital 7
Identificación biométrica 7
IDS (Sistema de Detección de Intrusos) 7
Ingeniería social 8
Integridad 8
Inteligencia Artificial Generativa (GenAI) 8
IoT (Internet de las Cosas) 8
IP (Internet Protocol) 8

J

Jailbreaking 8

K

Keylogger 8

M

Machine Learning (Aprendizaje automático) 8
Malware 9
Monitorización de redes 9

N

Navegador seguro 9
Nube híbrida 9

UNIVERSIDAD CATÓLICA DE TEMUCO
DIRECCIÓN DE INFORMÁTICA
VICERRECTORÍA DE ADMINISTRACIÓN Y ASUNTOS ECONÓMICOS

ÍNDICE

O

OEM (Fabricante de Equipos Originales) 9

P

Parche de seguridad 9
Pharming 9
Phishing 9
PIN (Número de Identificación Personal) 10
Política de privacidad 10
Política de seguridad 10
Privacidad 10
Prompt 10
Prompt Injection 10
Protección de Datos Personales 10
Proxy 10
PUP (Programa Potencialmente No Deseado) 10

Q

Quishing (QR Phishing) 11

R

Ransomware 11
Respaldo incremental 11
Riesgo cibernético 11
Rootkit 11

S

Sandboxing 11
Seguridad basada en el riesgo 11
Seguridad de la información 11
Seguridad en capas 12
Seguridad física 12
Servidor 12
Sextorsión 12
Shadow AI 12
Shadow IT 12
SIEM (Security Information and Event Management) 12
Smishing 12
Sniffer 12
SOC (Security Operations Center) 13
Spam 13
Spoofing 13
Spyware 13
Suplantación de identidad 13

T

Troyano 13
Túnel VPN 13

U

URL Spoofing 13
Usuario privilegiado 13

V

Vishing 14
VPN (Red Privada Virtual) 14
Vulnerabilidad 14

W

Wardriving 14
Whaling 14

X

XDR (Extended Detection and Response) 14
XSS (Cross-Site Scripting) 14

Z

Zero Trust (Confianza Cero) 15
Zero-Day 15

UNIVERSIDAD CATÓLICA DE TEMUCO
DIRECCIÓN DE INFORMÁTICA
VICERRECTORÍA DE ADMINISTRACIÓN Y ASUNTOS ECONÓMICOS

A

ADWARE

Software que automáticamente muestra o descarga publicidad en la computadora del usuario, a menudo incluido en aplicaciones gratuitas y utilizado para generar ingresos.

ANTIVIRUS

Software diseñado para detectar, prevenir y eliminar malware, protegiendo los sistemas informáticos de virus, gusanos, troyanos y otras amenazas.

ARQUITECTURA DE SEGURIDAD

Diseño y estructura de medidas de seguridad implementadas en una organización para proteger la infraestructura tecnológica y los datos sensibles.

ATAQUE DE CADENA DE SUMINISTRO (SUPPLY CHAIN ATTACK)

Ataque que compromete proveedores, servicios, software o terceros relacionados con una organización para utilizar esa relación como medio de acceso a sus sistemas o información.

AUTENTICACIÓN

Proceso de verificar la identidad de un usuario, dispositivo o entidad mediante credenciales como contraseñas, biometría, o tokens de seguridad, asegurando que solo aquellos con permiso puedan acceder a ciertos recursos.

AUTENTICACIÓN MULTIFACTOR (MFA)

Mecanismo de seguridad que requiere verificar la identidad de un usuario mediante dos o más factores de autenticación independientes, como contraseña, código enviado al dispositivo móvil o biometría, reduciendo significativamente el riesgo de acceso no autorizado.

B

BACKUP

Copia de seguridad de datos que se crea para evitar la pérdida de información importante en caso de fallos del sistema, ataques cibernéticos o errores humanos, permitiendo la restauración de los datos a su estado original.

BIOMETRÍA

Métodos de autenticación basados en características físicas únicas del individuo, como huellas dactilares, reconocimiento facial o escaneo de retina, utilizados para proporcionar acceso seguro a sistemas y dispositivos.

BOTNET

Red de dispositivos comprometidos por un malware que, al ser infectados, se convierten en bots o equipos zombie controlados de forma centralizada por un atacante para ejecutar acciones coordinadas, como ataques de denegación de servicio (DDoS), envío masivo de correos maliciosos o distribución de malware.

BOTS (ZOMBIES)

Dispositivo o equipo informático que ha sido comprometido por un atacante y puede ser controlado de forma remota para ejecutar acciones automáticas sin el conocimiento de su propietario.

BRECHA DE SEGURIDAD

Incidente que provoca la pérdida, alteración, divulgación, destrucción o acceso no autorizado a información, sistemas o recursos tecnológicos.

C

CERTIFICADO DIGITAL

Documento electrónico emitido por una autoridad de certificación que vincula una clave pública con la identidad de una persona o entidad, utilizado para autenticar la comunicación en línea.

CIBERATAQUE

Intento malicioso de dañar, destruir o acceder sin autorización a redes, sistemas o datos de una organización o individuo, utilizando diversas técnicas como malware, phishing, o hacking.

CIBERESPIONAJE

Actividad de obtener información confidencial o secreta a través de métodos cibernéticos, generalmente llevada a cabo por gobiernos, empresas o individuos para obtener ventajas políticas o económicas.

CIBERSEGURIDAD

Conjunto de prácticas, procesos y tecnologías diseñados para proteger los sistemas informáticos, redes y datos contra ataques, daños y accesos no autorizados.

CIFRADO

Proceso mediante el cual la información se transforma utilizando algoritmos criptográficos para impedir su lectura por personas no autorizadas, de modo que solo quienes dispongan de la clave correcta puedan acceder al contenido original.

CLAVE PRIVADA

Parte de un par de claves criptográficas mantenida en secreto y utilizada para descifrar datos cifrados con la clave pública correspondiente, garantizando la seguridad de la comunicación.

CLAVE PÚBLICA

Parte de un par de claves criptográficas que se distribuye públicamente y se utiliza para cifrar información que solo puede ser descifrada por la clave privada correspondiente.

CÓDIGO MALICIOSO

Software diseñado intencionadamente para dañar, interrumpir, o robar información de sistemas informáticos, incluyendo virus, gusanos, troyanos y otros tipos de malware.

COMPUTACIÓN EN LA NUBE

Tecnología que permite almacenar, procesar y gestionar datos y aplicaciones a través de servidores remotos accesibles vía Internet, eliminando la necesidad de infraestructura física local.

CONFIDENCIALIDAD

Principio de seguridad que garantiza que la información sensible solo sea accesible para personas autorizadas, protegiendo los datos de accesos no autorizados o divulgaciones inapropiadas.

CONSENTIMIENTO INFORMADO DIGITAL

Autorización libre, específica, informada e inequívoca otorgada por una persona para el tratamiento de sus datos personales a través de medios electrónicos o digitales.

CONTRASEÑA ROBUSTA

Contraseña que combina letras mayúsculas y minúsculas, números y símbolos, diseñada para ser difícil de adivinar o descifrar por atacantes, aumentando la seguridad de las cuentas.

COOKIE

Pequeño archivo de datos que un sitio web almacena en el navegador del usuario para recordar preferencias, mantener sesiones activas, personalizar la experiencia de navegación y, en algunos casos, recopilar información sobre su actividad con fines analíticos o publicitarios.

CORTAFUEGOS (FIREWALL)

Dispositivo o software que filtra el tráfico de red entrante y saliente, bloqueando conexiones sospechosas o no autorizadas para proteger redes privadas de amenazas externas.

CORTAFUEGOS DE PRÓXIMA GENERACIÓN (NGFW)

Dispositivo de seguridad que combina funciones de cortafuegos tradicionales con características avanzadas, como inspección de aplicaciones, prevención de intrusiones y control de contenido.

CRIPTOANÁLISIS

Estudio y análisis de sistemas criptográficos con el objetivo de romper o debilitar los métodos de cifrado, permitiendo descifrar mensajes sin la clave correspondiente.

CRIPTOGRAFÍA

Ciencia que estudia las técnicas para proteger la información mediante el uso de códigos y cifrados, asegurando la confidencialidad, integridad y autenticación de los datos transmitidos.

CULTURA DE SEGURIDAD

Conjunto de valores, creencias y prácticas compartidas dentro de una organización que promueven y apoyan la seguridad de la información, involucrando a todos los empleados en la protección de datos.

D

DATA BREACH (VIOLACIÓN DE DATOS)

Incidente en el que se accede, divulga o utiliza información confidencial sin autorización, a menudo debido a ataques cibernéticos o errores humanos.

DDOS (ATAQUE DE DENEGACIÓN DE SERVICIO DISTRIBUIDO)

Tipo de ciberataque en el que múltiples sistemas comprometidos inundan un servidor o red con tráfico, haciendo que los servicios se vuelvan inaccesibles para los usuarios legítimos.

DEEP WEB

Parte de Internet que no está indexada por motores de búsqueda convencionales, incluyendo bases de datos privadas, redes académicas y contenido protegido por contraseñas.

DEEPFAKE

Contenido digital generado o modificado mediante inteligencia artificial para simular de manera realista la apariencia, voz o comportamiento de una persona, pudiendo utilizarse para engañar o desinformar.

DESCIFRADO

Proceso de revertir el cifrado de información para devolverla a su formato original, haciéndola legible únicamente para personas con la clave o autorización correspondiente.

DIGITALIZACIÓN

Proceso de convertir información física o analógica en formato digital, facilitando su almacenamiento, acceso y gestión a través de sistemas informáticos.

DIRECCIÓN IP

Identificador numérico único asignado a cada dispositivo conectado a una red que permite su localización e identificación para el intercambio de información.

DIRECCIÓN IP DINÁMICA

Dirección IP que cambia cada vez que un dispositivo se conecta a una red, asignada temporalmente por el servidor DHCP para optimizar el uso de direcciones IP disponibles.

DMZ (ZONA DESMILITARIZADA)

Subred especial que actúa como una zona de amortiguación entre una red interna segura y una red externa no confiable, como Internet, para proteger los sistemas críticos de ataques.

DNS (SISTEMA DE NOMBRES DE DOMINIO)

Sistema que traduce nombres de dominio legibles por humanos (como www.uct.cl) en direcciones IP numéricas utilizadas por computadoras para localizar y acceder a sitios web.

DOMINIO

Nombre legible por humanos que identifica un recurso en Internet y que se traduce mediante el DNS a una dirección IP para facilitar el acceso a sitios web y servicios en línea.

DOS (DENEGACIÓN DE SERVICIO)

Tipo de ciberataque que busca hacer que un recurso o servicio en línea se vuelva inaccesible para los usuarios legítimos, generalmente sobrecargando el sistema con tráfico.

DOXING

Práctica de buscar y publicar información personal y privada de alguien sin su consentimiento, a menudo con intenciones de acosar o intimidar a la persona afectada.

E

E-MAIL SPOOFING

Técnica utilizada por los atacantes para falsificar la dirección del remitente en un correo electrónico, haciéndolo parecer como si proviene de una fuente confiable para engañar al destinatario.

EDR (ENDPOINT DETECTION AND RESPONSE)

Solución de seguridad diseñada para monitorear, detectar y responder a amenazas que afecten computadores, notebooks, servidores y otros dispositivos finales.

EXPLOIT

Programa o secuencia de comandos que aprovecha una vulnerabilidad en un sistema informático para ejecutar acciones no autorizadas, como obtener acceso o control sobre el sistema.

EXPLOIT ZERO-DAY

Método o herramienta utilizada para aprovechar una vulnerabilidad Zero-Day y comprometer un sistema antes de que la falla sea identificada o corregida por el fabricante.

F

FACTOR DE AUTENTICACIÓN

Método utilizado para verificar la identidad de un usuario, que puede ser algo que el usuario sabe (contraseña), algo que posee (token) o algo que es (biometría).

FALSIFICACIÓN

Creación, alteración o reproducción no autorizada de datos, documentos, credenciales o sitios web con el propósito de hacerlos parecer auténticos y utilizarlos para engañar a usuarios, obtener beneficios indebidos o realizar actividades fraudulentas.

FIRMA DIGITAL

Herramienta criptográfica que garantiza la autenticidad e integridad de un documento o mensaje digital, validando la identidad del firmante y asegurando que el contenido no ha sido alterado.

FIRMWARE

Software permanente incorporado en hardware, como routers o dispositivos de almacenamiento, que controla sus funciones básicas y puede actualizarse para corregir errores o mejorar la seguridad.

G

GESTIÓN DE IDENTIDADES Y ACCESOS (IAM)

Proceso y tecnologías utilizadas para gestionar y controlar los derechos de acceso de usuarios a sistemas, aplicaciones y datos, asegurando que solo las personas autorizadas puedan acceder a los recursos.

GESTIÓN DE RIESGOS

Proceso destinado a identificar, analizar, evaluar y tratar eventos o situaciones que puedan afectar el cumplimiento de los objetivos de una organización.

GESTIÓN DE VULNERABILIDADES

Proceso continuo de identificación, evaluación, priorización y corrección de debilidades de seguridad que podrían ser aprovechadas por atacantes.

GOBERNANZA DE DATOS

Conjunto de políticas, procesos, responsabilidades y controles destinados a garantizar que los datos sean gestionados de forma segura, confiable, íntegra y conforme a la normativa vigente.

H

HACKER ÉTICO

Profesional de la seguridad que utiliza sus habilidades de hacking con permiso de una organización para identificar y corregir vulnerabilidades en sus sistemas antes de que puedan ser explotadas maliciosamente.

HONEYPOT

Sistema de seguridad diseñado para atraer ciberataques, simulando vulnerabilidades, con el fin de detectar, desviar y analizar las tácticas empleadas por los atacantes.

HUELLA DIGITAL

Rastro de información que una persona deja al utilizar Internet y servicios digitales, ya sea de forma consciente (publicaciones, comentarios o formularios) o inconsciente (sitios visitados, ubicaciones o hábitos de navegación).

I

IDENTIDAD DIGITAL

Conjunto de datos, actividades y huella digital que una persona genera en Internet, permitiendo identificarla y contribuyendo a construir su imagen, reputación y presencia en entornos digitales.

IDENTIFICACIÓN BIOMÉTRICA

Técnica de autenticar a una persona mediante el análisis de sus características físicas únicas, como huellas dactilares, reconocimiento facial o escaneo del iris.

IDS (SISTEMA DE DETECCIÓN DE INTRUSOS)

Software o hardware que monitorea las redes y sistemas en busca de actividades sospechosas o violaciones de políticas, alertando a los administradores de posibles amenazas.

INGENIERÍA SOCIAL

Táctica utilizada por cibercriminales para manipular psicológicamente a personas y engañarlas para que revelen información confidencial o realicen acciones comprometedoras.

INTEGRIDAD

Propiedad que garantiza que los datos se mantienen completos, precisos y sin alteraciones desde su creación hasta su recepción, protegiéndolos contra modificaciones no autorizadas.

INTELIGENCIA ARTIFICIAL GENERATIVA (GENAI)

Tecnología basada en inteligencia artificial capaz de crear contenido nuevo, como textos, imágenes, videos, audios o código informático, a partir de instrucciones proporcionadas por una persona.

IOT (INTERNET DE LAS COSAS)

Red de dispositivos físicos conectados a Internet, como electrodomésticos, sensores y vehículos, que recopilan y comparten datos para mejorar la eficiencia y la automatización.

IP (INTERNET PROTOCOL)

Protocolo encargado de direccionar y enrutar paquetes de datos entre dispositivos conectados a una red, asegurando que la información llegue al destino correcto.

J

JAILBREAKING

Proceso de eliminar las restricciones impuestas por el fabricante en un dispositivo, como un iPhone, permitiendo al usuario instalar aplicaciones y modificar el sistema operativo de maneras no aprobadas oficialmente.

K

KEYLOGGER

Programa malicioso que registra y guarda todas las pulsaciones de teclas realizadas por un usuario, utilizado para robar contraseñas, información bancaria y otros datos sensibles.

M

MACHINE LEARNING (APRENDIZAJE AUTOMÁTICO)

Subcampo de la inteligencia artificial que permite a los sistemas aprender y mejorar automáticamente a partir de la experiencia, sin ser programados explícitamente para ello.

MALWARE

Software malicioso diseñado para causar daño, robar datos o realizar otras acciones no deseadas en un sistema informático sin el conocimiento o consentimiento del usuario.

MONITORIZACIÓN DE REDES

Actividad de supervisar el tráfico de red en tiempo real para detectar, analizar y responder a problemas de rendimiento, interrupciones o intentos de acceso no autorizados.

N

NAVEGADOR SEGURO

Software que proporciona funciones adicionales de seguridad, como bloqueo de rastreadores, cifrado de comunicaciones y protección contra phishing, para proteger la privacidad del usuario mientras navega por Internet.

NUBE HÍBRIDA

Modelo de computación en la nube que combina la infraestructura local (nube privada) con servicios de nube pública, permitiendo a las organizaciones utilizar ambos entornos de manera flexible.

O

OEM (FABRICANTE DE EQUIPOS ORIGINALES)

Empresa que produce componentes o dispositivos que son vendidos y utilizados por otra empresa para fabricar productos finales, como computadoras o automóviles.

P

PARCHE DE SEGURIDAD

Actualización de software que corrige vulnerabilidades conocidas, fallos de seguridad o errores de programación, protegiendo los sistemas contra amenazas y ayudando a mantener su estabilidad.

PHARMING

Técnica de ataque en la que los usuarios son redirigidos a un sitio web falso, a pesar de haber ingresado la dirección correcta, para robar sus datos de acceso o información financiera.

PHISHING

Técnica de fraude en la que los atacantes se hacen pasar por entidades legítimas a través de correos electrónicos, mensajes o sitios web falsos para engañar a las víctimas y obtener información confidencial.

PIN (NÚMERO DE IDENTIFICACIÓN PERSONAL)

Código de seguridad numérico utilizado para autenticar la identidad de un usuario en transacciones electrónicas, como retiros de cajeros automáticos o acceso a cuentas bancarias.

POLÍTICA DE PRIVACIDAD

Declaración emitida por una organización que describe cómo recopila, utiliza, almacena y protege los datos personales de los usuarios, cumpliendo con las regulaciones de privacidad.

POLÍTICA DE SEGURIDAD

Conjunto de normas, procedimientos y directrices establecidas por una organización para proteger la integridad, confidencialidad y disponibilidad de sus sistemas y datos.

PRIVACIDAD

Derecho del individuo a controlar cómo se recopila, utiliza, comparte y protege su información personal, garantizando que no sea accesible sin su consentimiento.

PROMPT

Instrucción o conjunto de indicaciones que una persona entrega a una herramienta de inteligencia artificial para obtener una respuesta, contenido o resultado específico.

PROMPT INJECTION

Técnica utilizada para manipular una herramienta de inteligencia artificial mediante instrucciones ocultas o maliciosas, con el fin de alterar su comportamiento o acceder a información no autorizada.

PROTECCIÓN DE DATOS PERSONALES

Conjunto de medidas legales, técnicas y organizativas destinadas a resguardar la privacidad y el tratamiento adecuado de los datos de las personas.

PROXY

Servidor que actúa como intermediario entre un usuario y el Internet, ocultando la dirección IP del usuario y filtrando el tráfico para mejorar la seguridad y privacidad.

PUP (PROGRAMA POTENCIALMENTE NO DESEADO)

Software que puede no ser malicioso, pero se instala en un sistema sin el consentimiento del usuario o mediante tácticas engañosas, a menudo causando molestias o cambios en la configuración del sistema.

Q

QUISHING (QR PHISHING)

Modalidad de phishing que utiliza códigos QR fraudulentos para dirigir a las personas hacia sitios web falsos o maliciosos con el fin de robar información o instalar software malicioso.

R

RANSOMWARE

Tipo de malware que cifra los datos de la víctima y exige un rescate para restaurar el acceso, a menudo amenazando con eliminar o divulgar la información si no se paga.

RESPALDO INCREMENTAL

Tipo de copia de seguridad que solo guarda los datos que han cambiado desde el último respaldo, reduciendo el tiempo y espacio de almacenamiento necesarios para proteger la información.

RIESGO CIBERNÉTICO

Probabilidad de que una organización o individuo sufra una pérdida o daño como resultado de un ciberataque, fallo en la seguridad de la información o vulnerabilidades tecnológicas.

ROOTKIT

Conjunto de herramientas de software malicioso diseñado para ocultar la presencia de malware en un sistema, permitiendo a los atacantes mantener acceso y control sobre el sistema sin ser detectados.

S

SANDBOXING

Técnica de seguridad que ejecuta programas o archivos en un entorno aislado y controlado para evitar que afecten al sistema principal, protegiendo contra malware y exploits.

SEGURIDAD BASADA EN EL RIESGO

Enfoque de ciberseguridad que prioriza la protección de activos según su valor, vulnerabilidades y la probabilidad de ser atacados, optimizando recursos para mitigar los riesgos más significativos.

SEGURIDAD DE LA INFORMACIÓN

Conjunto de prácticas y tecnologías destinadas a proteger la información y los sistemas de información contra accesos no autorizados, alteraciones, y destrucción.

SEGURIDAD EN CAPAS

Estrategia de ciberseguridad que emplea múltiples niveles de defensa, combinando diferentes herramientas y técnicas para proteger un sistema contra una amplia gama de amenazas.

SEGURIDAD FÍSICA

Medidas tomadas para proteger los sistemas informáticos y datos contra daños físicos, como acceso no autorizado, robos, incendios, o desastres naturales, asegurando la continuidad operativa.

SERVIDOR

Computadora o software que proporciona servicios, recursos o datos a otras computadoras (clientes) en una red, gestionando y facilitando la comunicación y el intercambio de información.

SEXTORSIÓN

Forma de chantaje en la que el atacante amenaza con divulgar imágenes o videos sexuales privados de la víctima a menos que se cumplan ciertas demandas, como el pago de dinero.

SHADOW AI

Uso de herramientas de inteligencia artificial sin autorización o control institucional, especialmente cuando se utilizan para procesar información de la organización o datos personales.

SHADOW IT

Uso de sistemas, aplicaciones, dispositivos o servicios tecnológicos sin conocimiento, autorización o supervisión del área de informática de la organización.

SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)

Herramienta que recopila y analiza registros de actividad provenientes de distintos sistemas para detectar eventos sospechosos y apoyar la gestión de incidentes de seguridad.

SMISHING

Tipo de fraude que utiliza mensajes de texto (SMS) para engañar a las personas y obtener información confidencial, credenciales o inducirlas a acceder a enlaces maliciosos.

SNIFFER

Herramienta de software que intercepta y analiza el tráfico de red, capturando datos como contraseñas, correos electrónicos o cualquier otra información transmitida entre dispositivos en una red.

SOC (SECURITY OPERATIONS CENTER)

Centro de Operaciones de Seguridad encargado de monitorear, detectar, analizar y responder a incidentes de ciberseguridad que puedan afectar a una organización.

SPAM

Correos electrónicos o mensajes no solicitados enviados en masa, a menudo con fines publicitarios o maliciosos, que pueden saturar bandejas de entrada y potencialmente contener malware.

SPOOFING

Técnica mediante la cual un atacante suplanta una identidad digital para hacerse pasar por una entidad legítima y ganar la confianza de usuarios o sistemas con fines maliciosos.

SPYWARE

Software que se instala en un dispositivo sin el conocimiento del usuario y recopila información sobre su actividad, como hábitos de navegación o datos personales, enviándola a terceros.

SUPLANTACIÓN DE IDENTIDAD

Técnica en la que un atacante se hace pasar por otra persona, utilizando información falsa o robada, para engañar a otros y obtener acceso a recursos o información sensible.

T

TROYANO

Tipo de malware que se disfraza como software legítimo, engañando al usuario para que lo instale, y luego ejecuta actividades maliciosas en el sistema infectado, como robar datos o abrir puertas traseras.

TÚNEL VPN

Canal cifrado y seguro que se crea dentro de una red para proteger la transmisión de datos, permitiendo a los usuarios acceder a recursos de forma privada y segura, como si estuvieran en la red local.

U

URL SPOOFING

Técnica de engaño en la que un atacante crea una URL falsa que parece legítima para atraer a los usuarios a un sitio web malicioso, donde pueden robar sus credenciales o instalar malware.

USUARIO PRIVILEGIADO

Individuo que posee derechos de acceso superiores a los de un usuario común, como administradores de sistemas, con la capacidad de modificar configuraciones, gestionar usuarios y acceder a datos sensibles.

V

VISHING

Tipo de ataque de phishing que utiliza llamadas telefónicas o mensajes de voz para engañar a las víctimas y obtener información confidencial, como contraseñas o números de tarjeta de crédito.

VPN (RED PRIVADA VIRTUAL)

Tecnología que crea una conexión segura y cifrada sobre una red menos segura, como Internet, permitiendo a los usuarios acceder a recursos de forma privada y protegida.

VULNERABILIDAD

Debilidad en un sistema informático, red o aplicación que puede ser explotada por atacantes para obtener acceso no autorizado o causar daño.

W

WARDRIVING

Práctica de buscar redes Wi-Fi abiertas mientras se conduce, con el objetivo de acceder a ellas sin autorización, a menudo con intenciones maliciosas o para obtener acceso gratuito a Internet.

WHALING

Variante del phishing que se dirige a altos ejecutivos o personas de alto perfil dentro de una organización, utilizando correos electrónicos personalizados para engañarlos y obtener información confidencial.

X

XDR (EXTENDED DETECTION AND RESPONSE)

Plataforma de seguridad que integra información proveniente de múltiples fuentes, como equipos, correos electrónicos, redes y servicios en la nube, para detectar y responder de manera más eficiente a amenazas avanzadas.

XSS (CROSS-SITE SCRIPTING)

Tipo de vulnerabilidad en aplicaciones web que permite a los atacantes inyectar scripts maliciosos en páginas web vistas por otros usuarios, robando sus cookies, redirigiéndolos o ejecutando comandos arbitrarios.

Z

ZERO TRUST (CONFIANZA CERO)

Modelo de seguridad basado en el principio de que ningún usuario, dispositivo o sistema debe considerarse confiable por defecto, requiriendo validación continua antes de otorgar acceso a recursos institucionales.

ZERO-DAY

Vulnerabilidad en software o hardware desconocida por el fabricante y sin un parche disponible, que puede ser explotada por atacantes antes de que se descubra y solucione.

LA SEGURIDAD DE LA INFORMACIÓN EN LA UCT ES RESPONSABILIDAD DE TODOS Y DE TODAS

UNIVERSIDAD CATÓLICA DE TEMUCO

DIRECCIÓN DE INFORMÁTICA
VICERRECTORÍA DE ADMINISTRACIÓN Y ASUNTOS ECONÓMICOS