

INTRODUCCIÓN AL MUNDO DE LA CIBERSEGURIDAD

JESSICA FABIANA RECALDE

ANALISTA SR. EN SEGURIDAD DE LA INFORMACIÓN

BDO EN ARGENTINA

API | Aseguramiento de Procesos Informáticos

RAS | Risk Advisory Services | IT Assurance, Audit and Compliance

CIBERSEGURIDAD CONCEPTO

NIST: *la capacidad de proteger o defender el uso del ciberespacio de los ataques cibernéticos.*



PUNTO DE VISTA AMPLIO

CISCO: *la describe como el esfuerzo constante por proteger los sistemas de red y todos los datos contra el uso no autorizado o los daños*



PUNTO DE VISTA RESTRINGIDO

TRIADA CID

ES UN MODELO DISEÑADO COMO GUÍA
PARA EL DESARROLLO DE LAS POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN.

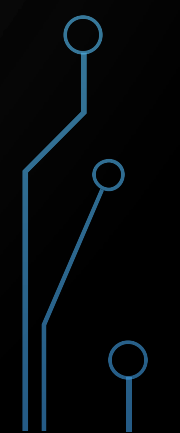
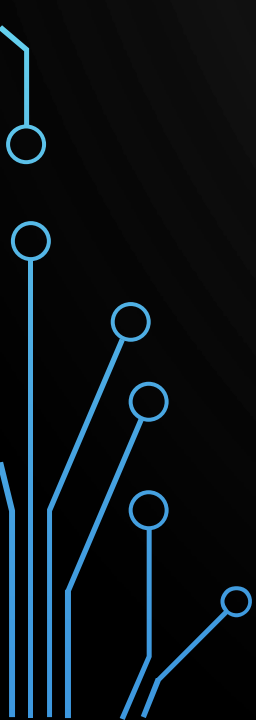





ATAQUES

CONCEPTO

Según IBM son *intentos no deseados de robar, exponer, alterar, deshabilitar o destruir información mediante el acceso no autorizado a los sistemas informáticos.*





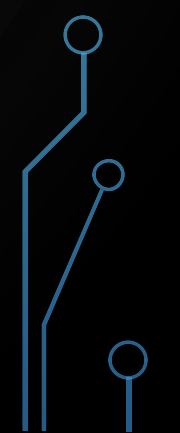

HERRAMIENTAS UTILIZADAS POR LOS CIBER ATACANTES



MALWARE

CONCEPTO

Es la contracción de la expresión en inglés “malicious software” o software malicioso, se trata de un término que se utiliza para describir el software diseñado para interrumpir las operaciones de un sistema u obtener acceso estos, sin el conocimiento o el permiso del usuario.



¿QUÉ ES LA INGENIERÍA SOCIAL?

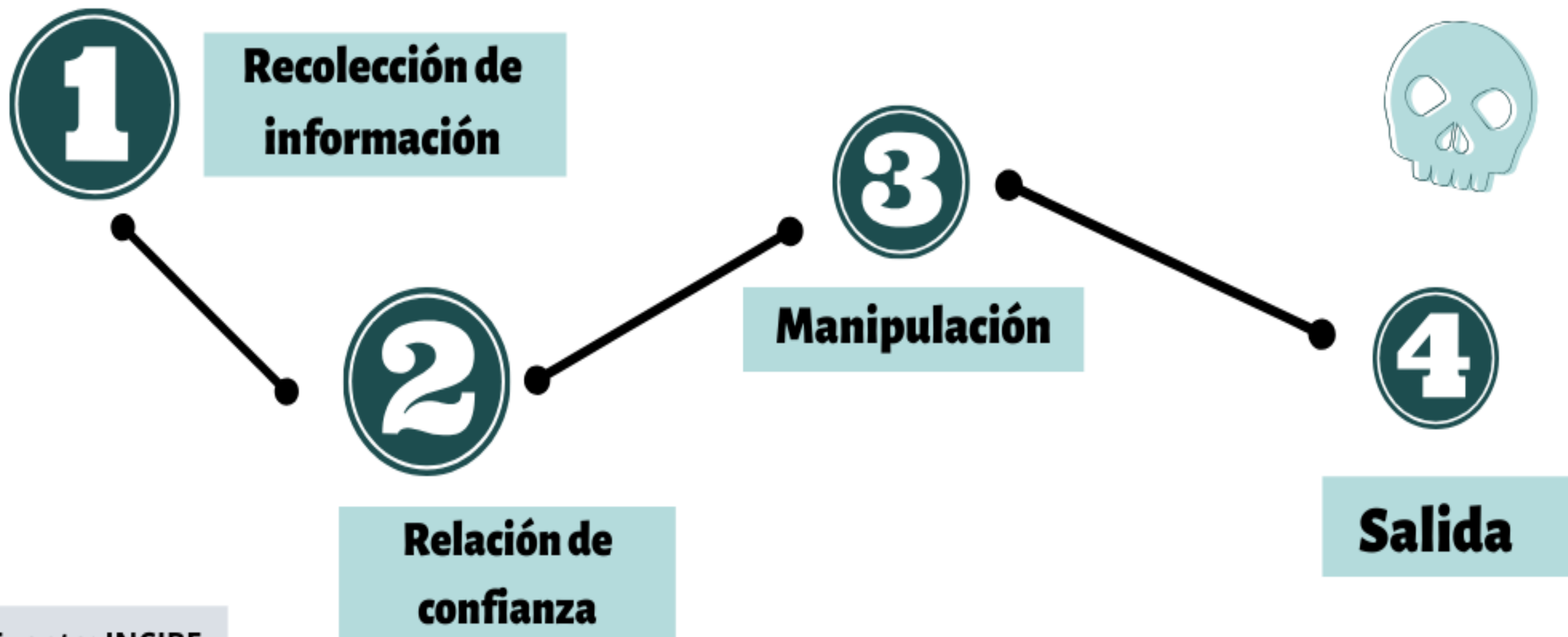


CONCEPTO



La ingeniería social es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados.

Ciclo de vida de un ciberataque de Ingeniería Social



¿COMO FUNCIONA LA INGENIERÍA SOCIAL?



RECOLECCIÓN DE INFORMACIÓN

El atacante identifica la víctima y recopila toda la información posible sobre ella.



RELACIÓN DE CONFIANZA

Establece el contacto con la víctima y se entabla relación.



EXTRACCIÓN DE LA INFORMACIÓN

Sirviéndose de técnicas de manipulación, accede y consigue la información deseada.



SALIDA SIN DEJAR PRUEBAS

El atacante intenta no dejar rastro para poder acceder más adelante si lo desea.

TÁCTICAS

Autoridad

Es más probable que las personas cumplan cuando reciben las instrucciones de “una autoridad”

Intimidación

Los delincuentes hostigan a una víctima para que tome medidas

Consenso/prueba social

Las personas tomarán medidas si sienten que a otras personas les gusta también

Escasez

Las personas tomarán medidas cuando consideren que existe una cantidad limitada

Urgencia

Las personas tomarán medidas cuando consideren que existe un tiempo limitado

Confianza/Familiaridad/Agrado

Los delincuentes crean una relación de confianza con una víctima la cual puede tomar más tiempo en establecerse.

TÉCNICAS MÁS COMUNES



PHISHING

Una técnica para intentar adquirir datos confidenciales, como números de cuentas bancarias, a través de una solicitud fraudulenta por correo electrónico o en un sitio web, en la que el perpetrador se hace pasar por una empresa legítima o una persona de confianza.



SPEAR PHISHING

Tipo de ataque de ingeniería social que se dirige a grandes empresas o a personas concretas. Los ataques de spear phishing están muy dirigidos a pequeños grupos o personas con poder, como ejecutivos de empresas y celebridades. Los ataques de ingeniería social que utilizan este método suelen estar bien estudiados y disfrazados de forma insidiosa, lo que dificulta su detección.



VISHING

También conocido como «phishing por voz», es un tipo sofisticado de ataque de phishing. En estos ataques, se suele falsificar un número de teléfono para que parezca legítimo: los atacantes pueden presentarse como personal informático, compañeros de trabajo o banqueros. Algunos atacantes también pueden utilizar cambiadores de voz para ocultar aún más su identidad.



SMISHING

Tipo de ataque de phishing que llega en forma de mensaje de texto o SMS.

CARACTERÍSTICAS:

- ✓ Habitualmente, estos ataques piden a la víctima que realice alguna acción inmediata a través de enlaces maliciosos en los que hay que hacer clic o números de teléfono a los que hay que llamar.
- ✓ A menudo, solicitan a las víctimas que revelen información personal que los atacantes pueden usar en beneficio propio.
- ✓ Los ataques de smishing suelen transmitir una sensación de urgencia para que las víctimas actúen rápidamente y caigan en la trampa.

PIGGYBACKING

El «Piggybacking» es una práctica mediante la cual un delincuente sigue a una persona autorizada a todas partes para obtener ingreso a una ubicación segura o a un área restringida.

Los delincuentes utilizan varios métodos para efectuar la actividad de «piggyback»:

- ✓ Dan la apariencia de estar acompañados por una persona autorizada
- ✓ Se unen a una multitud grande y fingen ser miembro
- ✓ Apuntan a una víctima que es descuidada con respecto a las reglas de las instalaciones





PHARMING

Un ataque en el que un atacante corrompe un servicio de infraestructura, como DNS (Sistema de nombres de dominio), lo que hace que el suscriptor sea redirigido a un verificador/RP falsificado, lo que podría hacer que el suscriptor revele información confidencial, descargue software dañino o contribuya a un fraude. acto.

PHISHING

¿COMO DETECTAR SI UN SITIO WEB ES SEGURO?



← Seguridad
learning.edx.org

La conexión es segura
Tu información (p. ej., contraseñas o números de tarjetas de crédito) es privada cuando se envía a este sitio. [Más información](#)

El certificado es válido



CS50's Computer Science for Lawyers

Retoma por donde quedaste

Continuar con el curso

Expandir todo

https://support.google.com/chrome/answer/95617?visit_id=637891299086522964-1267203051&p=ui_security_indicator&rd=1

EJEMPLO DE SITIO WEB SEGURO



Certificado

General **Detalles** Ruta de certificación

Información del certificado

Este certif. está destinado a los siguientes propósitos:

- Prueba su identidad ante un equipo remoto
- Asegura la identidad de un equipo remoto
- 2.23.140.1.2.2

* Para ver detalles, consulte la declaración de la entidad de ce

Emitido para: sni.cloudflaressl.com

Emitido por: Cloudflare Inc ECC CA-3

Válido desde 30/6/2021 **hasta** 30/6/2022

Declaración del emisor

Aceptar

Lawyers

DETALLES DE UN CERTIFICADO DE SEGURIDAD



Certificado

General Detalles **Ruta de certificación**

Ruta de certificación

- DigiCert Baltimore Root
 - Cloudflare Inc ECC CA-3
 - sni.cloudflaressl.com

Ver certificado

Estado del certificado:
Certificado válido.

Aceptar

Lawyers

DETALLES DE UN
CERTIFICADO
VÁLIDO

PHISHING

Robo de información personal a través de **correo electrónico**



PHARMING

Robo de información personal a través de una **página web falsa con apariencia real**



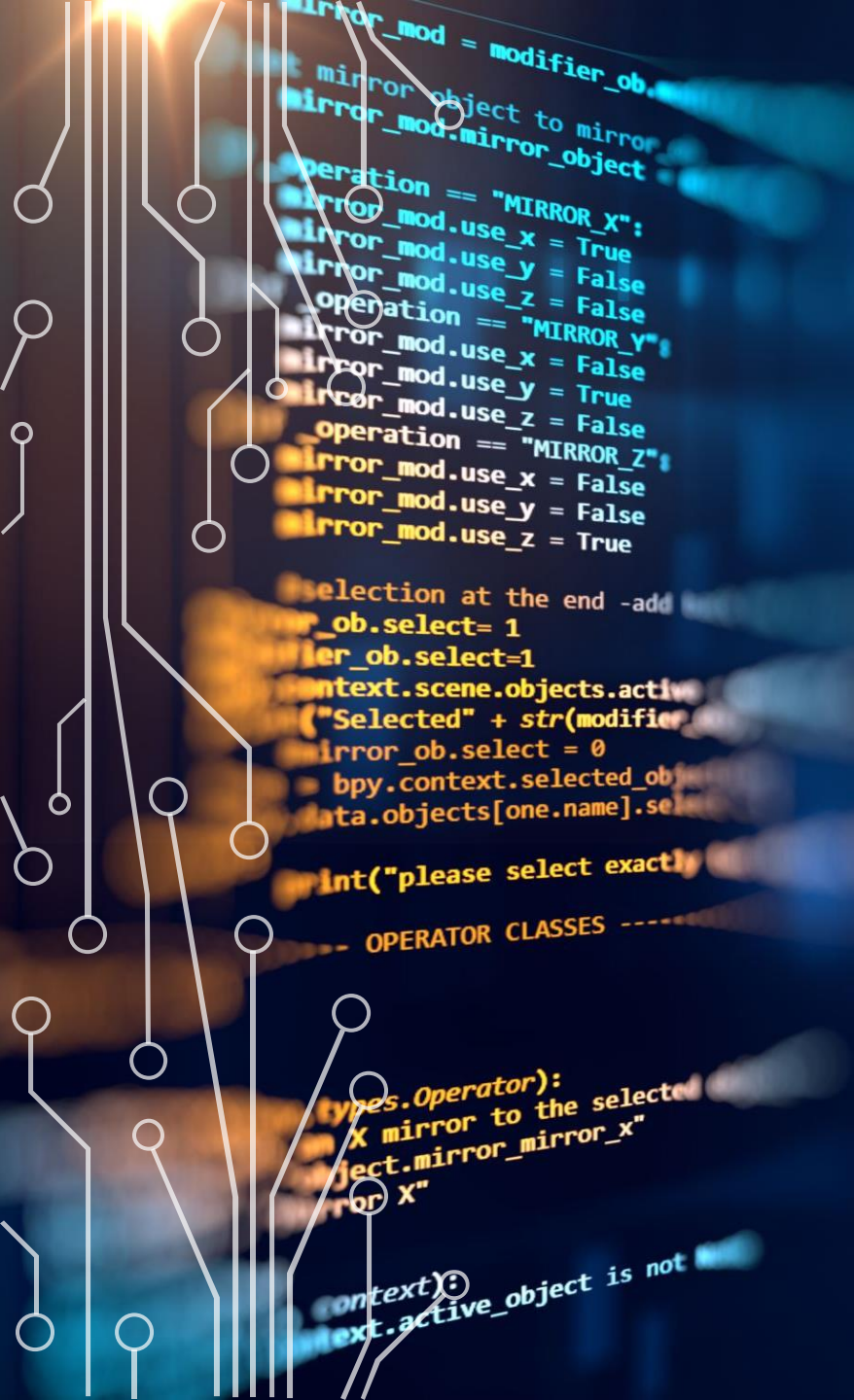
¿CÓMO PROTEGERSE?

Cambie la configuración de spam en el correo electrónico.

Investigue la fuente.

Si algo parece demasiado bueno para ser cierto, seguramente sea falso.

Utilice software de seguridad y confianza.



¿CUÁNDO UN ATAQUE DE INGENIERÍA CONSTITUYE UN DELITO?

La **estafa** mediante el uso de tarjeta magnética o de los datos de la tarjeta;

La **defraudación** mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos;

El **daño informático**, que consiste en alterar, destruir o inutilizar datos, documentos, programas o sistemas informáticos; vender, distribuir, hacer circular o introducir en un sistema informático, cualquier programa destinado a causar daños.

La **pena es mayor** en caso de dañar datos, documentos, programas o sistemas informáticos públicos; causar daño en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

A photograph of two business professionals shaking hands over a desk. The desk is cluttered with various office supplies including a calculator, a smartphone, a pen, and several documents with charts and graphs. The background is a bright, modern office space with large windows. The overall tone is professional and positive.

¡MUCHAS GRACIAS!

API | Aseguramiento de Procesos Informáticos

RAS | Risk Advisory Services | IT Assurance, Audit and Compliance