

Fundamentos de Seguridad de la Información

ING. OMAR VAZQUEZ GONZALEZ

ESPECIALISTA EN SEGURIDAD INFORMÁTICA Y T.I. CÉDULA. PROF. 12011987

Sobre mi...

- Ingeniero en Telemática
- Licenciado en Ciencias Computacionales
- Especialista en Seguridad Informática y T.I.
- Maestro en Ingeniería en Seguridad y T.I.
- Candidato a MBA
- +20 años como instructor
 - ✓ Becario de Telecomunicaciones
 - ✓ Desarrollador de Base de Datos
 - ✓ Desarrollador de Software Sr. (Back-end y Mobile)
 - ✓ Líder Técnico
 - ✓ Arquitecto de Soluciones
 - ✓ Arquitecto de Seguridad de Aplicaciones
 - ✓ Director de Seguridad de la Información





EL INSTITUTO POLITÉCNICO NACIONAL



Otorga el Diploma de

ESPECIALIDAD EN SEGURIDAD
INFORMÁTICA
Y TECNOLOGÍAS DE LA INFORMACIÓN

a Omar Vazquez Gonzalez



SEP
SECRETARÍA DE
INVESTIGACIÓN Y POSTGRADO

Por haber cumplido los requisitos académicos correspondientes.

En la Ciudad de México, a los 29 días del mes de enero del 2019.

El Director General

Dr. Mario Alberto Rodríguez Casas

"LA TÉCNICA AL SERVICIO DE LA PATRIA"



Estados Unidos Mexicanos
Secretaría de Educación Pública
Dirección General de Profesiones
Cédula Profesional Electrónica



Número de Cédula Profesional
12011987



Clave Única de Registro de Población
VXGO840208HMNZNM01



Entidad Federativa de Registro
CIUDAD DE MÉXICO

Libro	Foja	Número	Tipo
1201	111	8	C1

Se expide a: Datos del profesionista

OMAR
Nombre(s)

VAZQUEZ
Primer apellido

GONZALEZ
Segundo apellido

Quien cumplió con los requisitos establecidos en la Ley Reglamentaria del Artículo 5o.
Constitucional, relativo al ejercicio de las profesiones en la Ciudad de México y su Reglamento,
la cédula con efectos de patente para ejercer profesionalmente en el nivel de:

ESPECIALIDAD EN SEGURIDAD INFORMÁTICA Y
TECNOLOGÍAS DE LA INFORMACIÓN
Nombre del programa

505708
Clave

Datos de la institución educativa

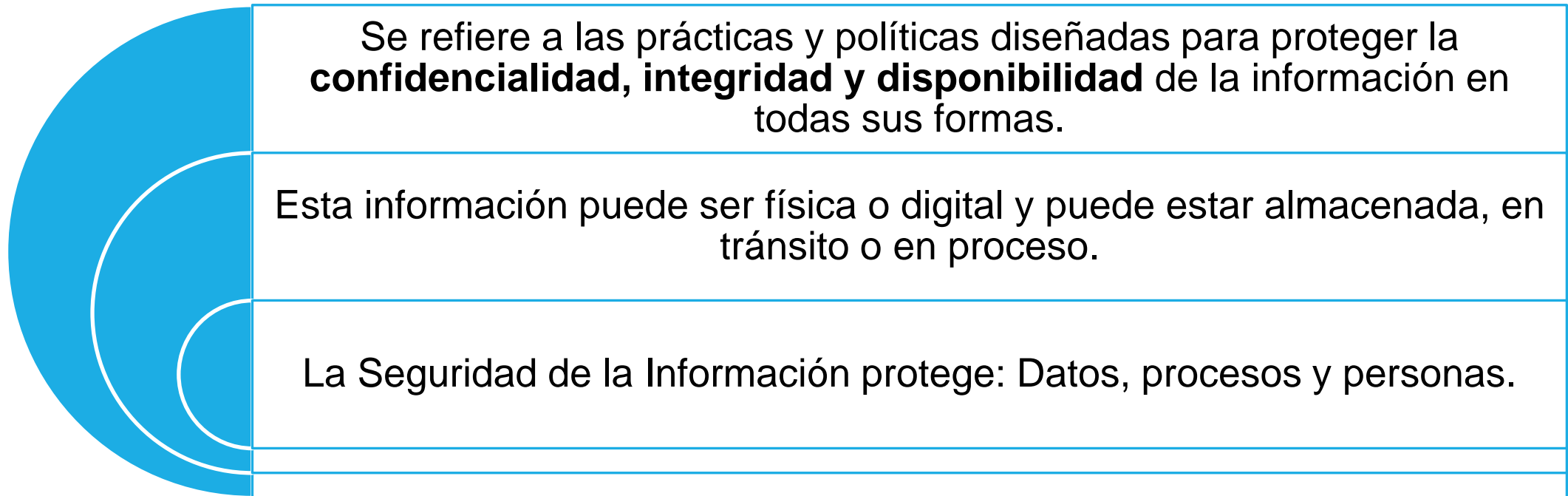
INSTITUTO POLITÉCNICO NACIONAL
Nombre o denominación

090002
Clave

- **Nombre completo**
- **Formación universitaria**
- **Rol actual**
- **Experiencia en TI**
- **Experiencia en Seguridad**
- **Expectativas del curso**



Seguridad de la Información



Triada de la Seguridad de la Información



Confidencialidad: Asegura que la información esté disponible solo para aquellos que tienen permiso para acceder a ella. Se logra mediante técnicas de cifrado, control de acceso y políticas de privacidad.



Integridad: Garantiza que la información sea precisa, completa y no esté alterada de manera no autorizada. Los métodos para mantener la integridad incluyen la autenticación, firmas digitales y sistemas de control de versiones.



Disponibilidad: Asegura que la información esté disponible y accesible cuando sea necesario para usuarios autorizados. Esto implica la implementación de medidas para prevenir interrupciones no planificadas, como redundancia de servidores y copias de seguridad regulares.



Activo de Información

Se define como cualquier recurso o entidad, ya sea tangible o intangible, que posee valor para una organización. Estos activos están directamente relacionados con la información y pueden incluir, pero no se limitan a, datos sensibles, sistemas informáticos, software, redes de comunicación, documentación, propiedad intelectual y recursos humanos.

Esto incluye no solo los datos en sí, sino también los sistemas que los procesan, transmiten y almacenan, así como los procesos y personas asociadas.

Ejemplos



Ejercicio

En una hoja de Excel realice un inventario de activos de Información

A) De su compañía (Puede ser sólo de su área o departamento)


B) De su persona

C) De su familia

***Su inventario es confidencial**

Retroalimentación: 4:15PM

Ataque



Un **ataque** se refiere a un intento deliberado y malicioso de comprometer la **confidencialidad, integridad o disponibilidad** de la información o los sistemas informáticos de una organización.

Ejemplos de ataques

Ataque de Fuerza Bruta: Intentos repetidos y automáticos de adivinar contraseñas o claves de acceso.

Phishing: Correos electrónicos o mensajes engañosos que pretenden ser de fuentes confiables para robar información sensible.

Ataque DDoS (Denegación de Servicio Distribuido): Sobrecargar un sistema o red con tráfico, dejándolo inaccesible para los usuarios legítimos.

Ransomware: Cifrado de archivos o sistemas, exigiendo un rescate para desbloquearlos.

Malware: Software malicioso que incluye virus, troyanos, gusanos y spyware, diseñado para dañar o robar información.

Inyección SQL: Introducción de código SQL malicioso en campos de entrada para manipular bases de datos.

Cross-Site Scripting (XSS): Inserción de scripts maliciosos en sitios web para robar información del usuario.

Man-in-the-Middle (MitM): Intercepción y posible alteración de la comunicación entre dos partes sin que lo sepan.

Ataque Zero-Day: Explotación de vulnerabilidades de software desconocidas para las que aún no hay parches disponibles.

Ataque de Ingeniería Social: Manipulación psicológica para obtener información confidencial de las personas.

Ataque de Intermediario (Proxy Attack): Utilización de un servidor proxy para ocultar la identidad del atacante.

Ataque de Falsificación de IP (IP Spoofing): Cambio de la dirección IP para hacer que un paquete parezca provenir de una fuente confiable.

Ataque de Falsificación de Correo Electrónico (Email Spoofing): Envío de correos electrónicos falsificados para parecer que provienen de una fuente confiable.

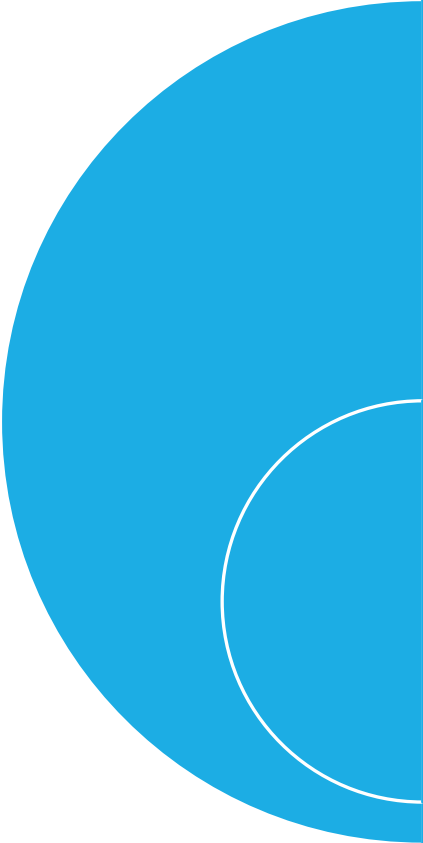
Ataque de Hombre en el Teléfono (Vishing): Engaño telefónico para obtener información sensible del usuario.

Ataque de Hombre en el Navegador (Clickjacking): Engaño visual para hacer que los usuarios hagan clic en algo diferente de lo que piensan que están haciendo.

Amenaza

Es todo aquello que tiene el **potencial** de dañar los activos de información al explotar una **vulnerabilidad**. En otras palabras, una amenaza es cualquier cosa que pueda aprovecharse para causar daño o interrupción en los activos de una organización, incluyendo sistemas de información, datos, procesos y personas.

Vulnerabilidad



Se define como una debilidad en un sistema, proceso, diseño o implementación que puede ser explotada para violar la seguridad del sistema.

Las vulnerabilidades pueden ser el resultado de errores en el software, configuraciones incorrectas, falta de actualizaciones de seguridad, o incluso debilidades en los procesos operativos.

Ejemplos de vulnerabilidades

Vulnerabilidades de Software: Errores de codificación en aplicaciones que pueden ser explotados por malware o atacantes para ejecutar código malicioso.

Configuraciones Incorrectas: Configuraciones inseguras en servidores, bases de datos o redes que permiten el acceso no autorizado.

Falta de Parches de Seguridad: Sistemas que no han sido actualizados con los últimos parches de seguridad, lo que deja al sistema vulnerable a exploits conocidos.

Contraseñas Débiles: Uso de contraseñas fáciles de adivinar o que no cumplen con las políticas de seguridad, lo que facilita los ataques de fuerza bruta.

Falta de Autenticación: Sistemas que no requieren autenticación adecuada o que permiten la autenticación débil.

Vulnerabilidades en Protocolos de Red: Debilidades en protocolos de red como SSL/TLS que pueden ser explotadas para interceptar datos.

Inyección de Código: Fallos que permiten la inserción de código malicioso en aplicaciones, como la inyección SQL.

Falta de Control de Acceso: Permisos mal configurados que permiten a usuarios no autorizados acceder a ciertas partes del sistema.

Vulnerabilidades del Sistema Operativo: Fallos en el sistema operativo que pueden ser explotados para obtener privilegios no autorizados.

Vulnerabilidades de Firmware y Hardware: Debilidades en el firmware y hardware de dispositivos que pueden ser explotadas para controlar el dispositivo.

Falta de Encriptación: Datos transmitidos sin encriptación adecuada, lo que facilita la interceptación.

Falta de Validación de Entrada: No validar adecuadamente los datos de entrada en aplicaciones web, lo que puede llevar a la inyección de código y otros ataques.

Falta de Auditoría y Monitoreo: La falta de registros de auditoría o monitoreo adecuados para detectar actividades inusuales.

Vulnerabilidades de Plugins y Extensiones: Fallos en los plug-ins y extensiones de navegadores que pueden ser explotados por sitios web maliciosos.

Vulnerabilidades de Aplicaciones Web: Errores en aplicaciones web que pueden ser explotados para el robo de datos o la manipulación del sitio.

Evento de Seguridad

Se refiere a cualquier suceso observable o detectable que indica una posible violación de la política de seguridad, fallo en los controles de seguridad, o una amenaza significativa a la confidencialidad, integridad o disponibilidad de los activos de información.

Estos eventos pueden incluir intentos de acceso no autorizado, malware detectado, interrupciones de red, o cualquier otro incidente que pueda comprometer la seguridad de los sistemas de información.

Ejemplos de eventos de seguridad

Intentos de Acceso No Autorizado: Incluye intentos de iniciar sesión no autorizados en sistemas, aplicaciones o redes.

Escaneo de Puertos: Actividades que implican el escaneo de puertos de red en busca de sistemas vulnerables.

Ataques de Fuerza Bruta: Intentos repetidos y automáticos de adivinar contraseñas o claves de acceso.

Phishing: Correos electrónicos, mensajes o sitios web falsos diseñados para engañar a los usuarios y robar información confidencial.

Malware: Detección de software malicioso, como virus, troyanos o ransomware, en sistemas o redes.

Actividades Anómalas de Usuarios: Comportamientos inusuales de usuarios, como el acceso a archivos o áreas no autorizadas.

Errores de Configuración: Configuraciones incorrectas en sistemas o firewalls que podrían permitir el acceso no autorizado.

Ataques de Denegación de Servicio (DDoS): Intentos de sobrecargar un sistema, red o sitio web con tráfico para dejarlo inaccesible.

Interrupciones de Energía: Cortes de energía que pueden afectar la disponibilidad de sistemas y equipos.

Errores de Software: Fallos o bugs en aplicaciones que podrían ser explotados para un acceso no autorizado.

Rastreo de Actividad de Red: Monitorización sospechosa de la actividad de red para obtener información sensible.

Dispositivos Perdidos o Robados: Pérdida o robo de dispositivos móviles o portátiles que pueden contener datos sensibles.

Incidente de Seguridad

Se define como un evento o una serie de eventos que comprometen la confidencialidad, integridad o disponibilidad de los activos de información de una organización.

Estos eventos pueden incluir intentos de acceso no autorizado, ataques de malware exitosos, pérdida de datos, interrupciones del servicio, entre otros. La gestión de incidentes de seguridad implica la identificación, registro, evaluación y respuesta a estos eventos de manera efectiva para minimizar el impacto, restaurar la operatividad normal y prevenir futuros incidentes similares.

Ejemplos de Incidentes

Violación de Datos:

Acceso no autorizado o robo de datos sensibles, como información personal, contraseñas o detalles de tarjetas de crédito.

Ataques de Ransomware:

Cifrado de datos por parte de un atacante que exige un rescate para restaurar el acceso a los archivos.

Ataques DDoS (Denegación de Servicio Distribuido): Sobrecarga intencional de un sistema o red con tráfico para dejarlo inoperable.

Intrusión en la Red:

Acceso no autorizado a sistemas y datos a través de vulnerabilidades en la red.

Phishing Exitoso: Engañar a los usuarios para que divulguen información confidencial, como contraseñas o información bancaria.

Infección por Malware:

Infección exitosa de sistemas con software malicioso que puede robar datos o dañar archivos.

Fuga de Información:

Divulgación no autorizada de información confidencial a través de medios electrónicos o impresos.

Suplantación de Identidad: Uso fraudulento de la identidad de otra persona para acceder a sistemas o realizar transacciones.

Fuga de Contraseñas:

Divulgación no autorizada de contraseñas, ya sea por robo, filtración o descifrado.

Ataque al Sitio Web: Manipulación o degradación del funcionamiento de un sitio web, a menudo para robar datos o difamar la organización.

Acceso no Autorizado a Sistemas Críticos:

Intrusión en sistemas cruciales para la operación de una organización, como sistemas de control industrial.

Amenaza Interna: Acciones maliciosas realizadas por empleados o contratistas, como robo de datos o sabotaje.

Fallo de Seguridad Física:

Acceso no autorizado a instalaciones físicas que almacenan información sensible, como centros de datos.

Ataques a Dispositivos IoT:

Compromiso de dispositivos del Internet de las cosas para su uso en ataques cibernéticos.

Ataque de Ingeniería Social:

Manipulación psicológica de personas para divulgar información confidencial o realizar acciones no deseadas.

Evento vs Incidente

La diferencia clave entre un **evento** y un **incidente de seguridad** radica en el impacto y la magnitud del suceso.

Un evento de seguridad se refiere a **cualquier suceso** observable o detectable que indica una **posible** amenaza a la seguridad de la información, como intentos de acceso no autorizado o actividades anómalas en la red.

Por otro lado, un incidente de seguridad es un evento o una serie de eventos que **han comprometido** la confidencialidad, integridad o disponibilidad de los activos de información, como un ataque de malware exitoso que ha causado pérdida de datos o una interrupción del servicio

Riesgo

Un **riesgo de seguridad de la información** se refiere a la **posibilidad** de que un evento o una amenaza explote una vulnerabilidad en los sistemas de información, lo que puede resultar en daño, pérdida, degradación o acceso no autorizado a la información. Este riesgo es una combinación de la probabilidad de que ocurra un evento no deseado y el impacto que tendría en los activos de información si ocurriera.

Riesgo

Mitiga (Reduce)

Acepta

Transfiere

Elimina

Riesgo = Impacto X probabilidad

Política de Seguridad de la Información

Política de Seguridad de la Información es un conjunto **formalizado** de principios, reglas y pautas establecidas por una organización para gestionar y proteger los activos de información. Esta política proporciona un marco estructurado para definir los objetivos de seguridad, roles y responsabilidades, prácticas permitidas y restricciones en relación con la gestión de la información.

Control de Seguridad de la Información

Un **control de seguridad de la información** es una medida **técnica, organizativa o legal** que se implementa para **mitigar o transferir** los riesgos de seguridad de la información. Estos controles son diseñados para salvaguardar la confidencialidad, integridad y disponibilidad de la información, y para asegurar que se cumplan los objetivos de seguridad establecidos por la organización.



Software Malicioso y ataques Informáticos

(Malware & Attacks)

Malware = Malicious Software

Derivado de las palabras "malicious software" en inglés, es un término técnico utilizado en el ámbito de la informática y la seguridad cibernética para referirse a cualquier tipo de software maligno diseñado específicamente para dañar, alterar, acceder sin autorización, o robar información de un sistema informático, red, o dispositivo digital. Este software malicioso puede incluir diversos tipos como virus, gusanos, troyanos, ransomware, adware, y spyware, entre otros.

Método de Propagación

El **método de propagación** se refiere a las técnicas y mecanismos utilizados por el malware para infiltrarse y extenderse en sistemas y redes. Estos métodos pueden variar ampliamente y evolucionar con el tiempo a medida que los desarrolladores de malware buscan formas más efectivas de distribuir sus creaciones.

Ejemplos

Correo Electrónico: El malware se disfraza como un archivo adjunto o un enlace en correos electrónicos aparentemente legítimos para engañar a los usuarios y hacer que descarguen e infecten sus sistemas.

Sitios Web Comprometidos: Los sitios web pueden ser comprometidos y utilizados para distribuir malware a los visitantes que descargan contenido infectado sin saberlo.

Descargas de Internet: El malware puede ser incluido en software aparentemente legítimo disponible para su descarga en sitios web no confiables o a través de intercambio de archivos peer-to-peer.

Dispositivos USB y Otros Dispositivos Extraíbles: El malware puede propagarse al conectarse a dispositivos USB o tarjetas de memoria que están infectados.

Redes Peer-to-Peer (P2P): Los programas de intercambio de archivos P2P pueden ser utilizados para propagar malware, ya que los usuarios comparten archivos sin verificar su seguridad.

Vulnerabilidades de Software: Los malware pueden aprovechar vulnerabilidades en el software para infiltrarse automáticamente en sistemas que no han sido actualizados con los últimos parches de seguridad.

Software “Pirata”

La propagación de malware a través de software pirata es un problema significativo en muchos países, incluyendo México. Aquí hay algunas razones por las cuales esto es particularmente relevante en el contexto mexicano:

- 1. Alto Uso de Software Pirata:** En México, hay una alta tasa de uso de software pirata debido a la disponibilidad generalizada y a menudo a un menor costo que el software legal. Esto crea una gran superficie para los atacantes que pueden ocultar malware en versiones pirateadas de software popular.
- 2. Falta de Conciencia:** Gran parte de la población y organizaciones en México pueden no estar completamente al tanto de los riesgos asociados con el software pirata. La falta de conciencia puede llevar a una menor precaución al descargar y utilizar software de fuentes no confiables.

Payload

El **payload** de un malware se refiere a la funcionalidad específica que realiza una vez que ha infectado un sistema. El payload puede variar enormemente según el tipo de malware y los objetivos del atacante.

Payload

- 1.Ransomware:** Cifrado de archivos del sistema y demanda de un rescate para desbloquearlos.
- 2.Keyloggers:** Registro de pulsaciones de teclas para robar contraseñas y otra información confidencial.
- 3.Botnets:** Incorporación del sistema en una red de computadoras zombies controlada por un atacante para realizar actividades maliciosas como ataques DDoS.
- 4.Spyware:** Monitoreo y recopilación silenciosa de información del usuario, como historial de navegación y datos personales.
- 5.Adware:** Despliegue de anuncios publicitarios no deseados en el sistema del usuario.
- 6.Rootkits:** Herramientas que ocultan la presencia del malware al sistema operativo y otros programas de seguridad.
- 7.Exploits:** Utilización de vulnerabilidades del sistema para realizar acciones específicas, como tomar el control del sistema o robar información.

Tipos de Malware

Virus:

- **Definición:** Un virus informático es un tipo de malware que se **adhiera a un archivo o programa existente** y se replica cuando el archivo o programa infectado se ejecuta. Utiliza técnicas de replicación para propagarse a otros archivos y programas, y puede dañar, alterar o eliminar datos en el sistema infectado

Caballos de Troya (Trojans)

Los troyanos son programas maliciosos que se disfrazan como aplicaciones legítimas para engañar a los usuarios y obtener acceso no autorizado a sus sistemas. A menudo se utilizan para robar información confidencial, proporcionar acceso remoto no autorizado al atacante o realizar actividades dañinas en el sistema huésped.

Gusanos (Worms)

Los gusanos son malware autorreplicantes que se propagan automáticamente a través de redes y sistemas, aprovechando vulnerabilidades de seguridad. Difieren de los virus en que **no necesitan un archivo huésped para propagarse**, lo que les permite replicarse rápidamente y afectar múltiples sistemas en un corto período de tiempo.

Botnets

Una botnet es una red de **dispositivos comprometidos**, controlados de forma remota por un atacante. Estos dispositivos, o "bots", pueden ser utilizados para realizar ataques coordinados, como ataques DDoS, robo de datos, propagación de malware y otras actividades maliciosas, todo sin el conocimiento del propietario del dispositivo.

Ransomware

El ransomware es un tipo de malware que cifra archivos o bloquea el acceso a sistemas, exigiendo un rescate económico, generalmente en criptomonedas, para restaurar el acceso. Puede cifrar archivos importantes o incluso todo un sistema, dejando a las víctimas sin acceso a sus datos hasta que se realice el pago.

Rootkits

Un rootkit es un tipo avanzado de malware que se instala en un sistema y oculta su presencia y las actividades maliciosas del usuario y las herramientas de seguridad. Al modificar el sistema operativo y las funciones del kernel, los rootkits proporcionan un acceso persistente y no autorizado al sistema, lo que permite a los atacantes realizar acciones sin ser detectados.

Tipos de Virus

Macro Virus:

- **Definición:** Un macro virus es una forma de malware que se aprovecha de las macros en documentos y aplicaciones para ejecutar código malicioso. Estas macros, cuando se activan, pueden infectar otros documentos o programas, propagando el malware. Los macro virus suelen estar ocultos dentro de documentos aparentemente seguros y se activan cuando el usuario permite las macros durante la apertura del archivo.

Compression Virus

- **Definición:** Un virus de compresión es un tipo de malware que utiliza técnicas de compresión o cifrado para ocultar su código malicioso y dificultar su detección por parte de los programas antivirus. Estos virus comprimen sus archivos para camuflar su presencia, y cuando se ejecutan, se descomprimen en la memoria del sistema, activando así sus funciones maliciosas.

Stealth Virus

Un virus sigiloso es un tipo de malware que emplea técnicas avanzadas para ocultar su presencia y actividad en un sistema. Estos virus pueden enmascarar su código, alterar los resultados de las herramientas de seguridad y evitar la detección al modificar su comportamiento en función del entorno del sistema infectado. Su capacidad para evadir la detección lo convierte en un desafío para los programas antivirus tradicionales

Polymorphic Virus

Un virus polimórfico es un malware que tiene la capacidad de cambiar su código y estructura en cada infección, creando así variantes únicas. Esta capacidad de mutación dificulta su detección, ya que las firmas de los antivirus tradicionales no son efectivas contra él. El código del virus se reescribe cada vez que infecta un nuevo archivo o sistema, lo que le permite evadir fácilmente las técnicas de detección basadas en firmas

Boot Sector Virus

Un virus del sector de arranque es un tipo de malware que se aloja en el sector de arranque del disco duro o en otros dispositivos de almacenamiento, como discos flexibles o unidades USB. Este tipo de virus se activa cuando el sistema operativo se carga, permitiendo que el malware se ejecute antes de que el sistema operativo se inicie. Los virus del sector de arranque son capaces de propagarse a otros dispositivos de almacenamiento conectados a la computadora.

Multipartite Virus

Un virus multipartito es un malware multifacético que utiliza múltiples métodos de infección para propagarse y ejecutar acciones maliciosas en un sistema. Puede combinar técnicas de virus de macro, virus del sector de arranque y troyanos para infectar sistemas y archivos. Debido a su complejidad y capacidad para atacar a través de diferentes vectores, son especialmente desafiantes de eliminar y requieren una limpieza exhaustiva del sistema para su erradicación completa

Ingeniería Social

(Social Engineering)

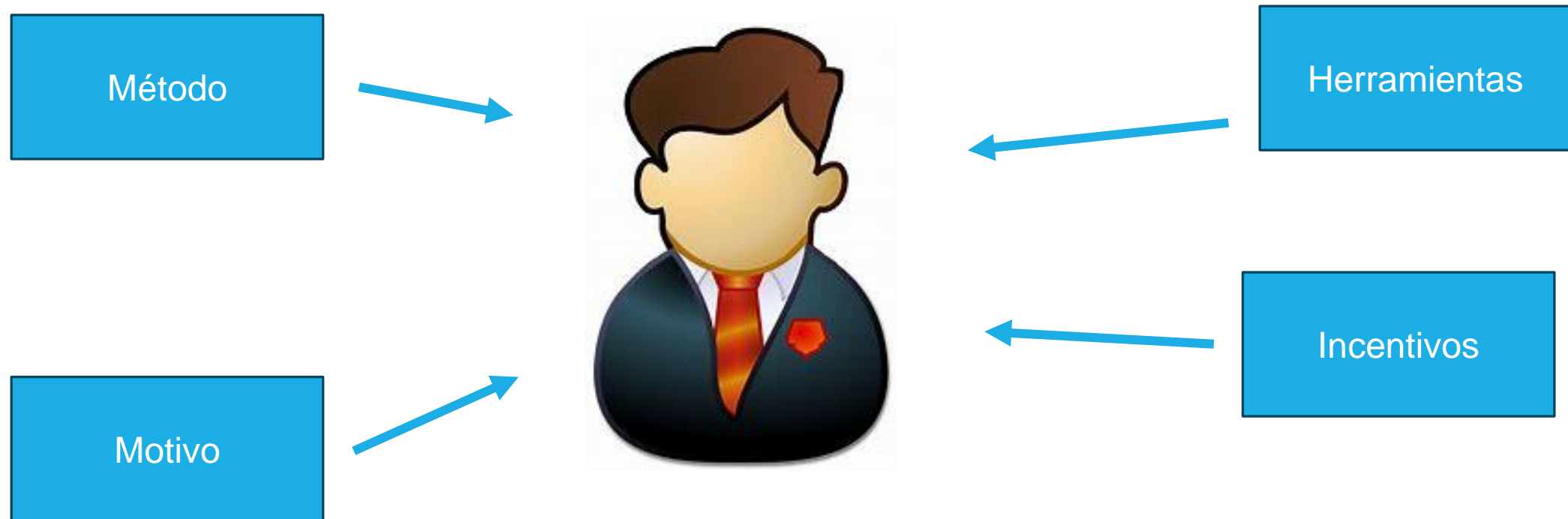


¿Qué es la ingeniería Social?

Es una técnica empleada por atacantes para manipular a las personas y convencerlas de revelar información confidencial (contraseñas, detalles financieros, etc.).

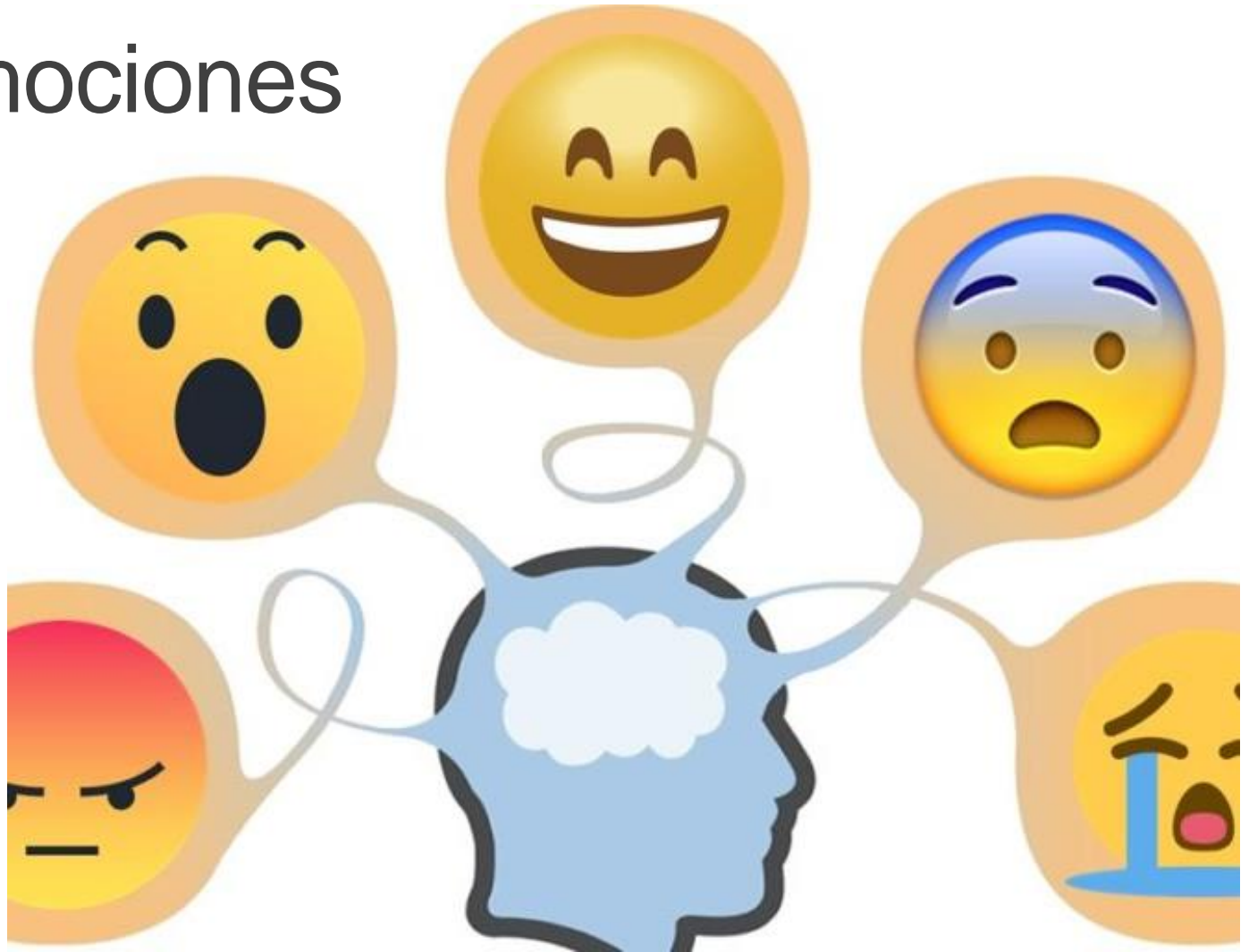
En lugar de atacar sistemas informáticos directamente, los ingenieros sociales se enfocan en explotar las debilidades (vulnerabilidades) humanas, como la curiosidad, la **confianza** o la falta de conciencia, para obtener acceso a información valiosa.

Ataque de ingeniería social



Usan nuestras emociones

- Pueden ofrecer regalos gratis o recompensas
- Ofrecen información valiosa
- Apelan a las emociones humanas:
 - Confianza
 - Miedo
 - Urgencia
 - Ambición
 - Compasión
 - Amor
 - Odio



Técnicas de persuasión



Autoridad: Las personas tienden a obedecer figuras de autoridad y expertos en un tema específico.



Intimidación: El uso del miedo pueden forzar a las personas a actuar de cierta manera para evitar consecuencias negativas.



Consenso: Las personas tienden a seguir la mayoría, especialmente en situaciones inciertas, asumiendo que la mayoría tiene razón.



Escasez: La percepción de que algo es escaso o limitado puede aumentar su valor percibido.



Familiaridad: Las personas tienden a confiar en lo que les resulta familiar, como personas o marcas conocidas.



Confianza: Las personas son más propensas a obedecer o compartir información con aquellos a quienes confían o perciben como confiables.



Urgencia: Puede presionar a las personas para que actúen rápidamente, sin tomar el tiempo necesario para evaluar la situación.



Shoulder Surfing



Dumpster Diving



Eavesdropping



Reverse social engineering

Tipos de ingeniería social

A blurred background image showing two people, a man and a woman, sitting at a desk and looking at a computer screen. The man is on the left, and the woman is on the right. They appear to be in a professional or educational setting.

Shoulder Surfing

Es un tipo de ataque en el que un atacante observa directamente la pantalla de la computadora, teléfono móvil u otro dispositivo de la víctima para obtener información confidencial. Esto puede implicar mirar por encima del hombro de alguien mientras están ingresando una contraseña, un número de tarjeta de crédito u otra información sensible.

Dumpster Diving

Implica buscar información valiosa en la basura o en contenedores de reciclaje. Los atacantes pueden buscar documentos impresos, discos duros antiguos, o cualquier otro tipo de material que pueda contener datos confidenciales. A menudo, las organizaciones desechan documentos sin destruir adecuadamente la información, lo que los convierte en un objetivo.



Eavesdropping

Escucha ilegal: Es la práctica de escuchar conversaciones privadas sin el consentimiento de los participantes. En el contexto de la ingeniería social, esto puede implicar escuchar conversaciones telefónicas, mensajes de voz o incluso interceptación de comunicaciones electrónicas para obtener información confidencial. Este tipo de ataque puede ocurrir en redes inalámbricas no seguras o mediante técnicas avanzadas de interceptación de datos.

Reverse Social Engineering:



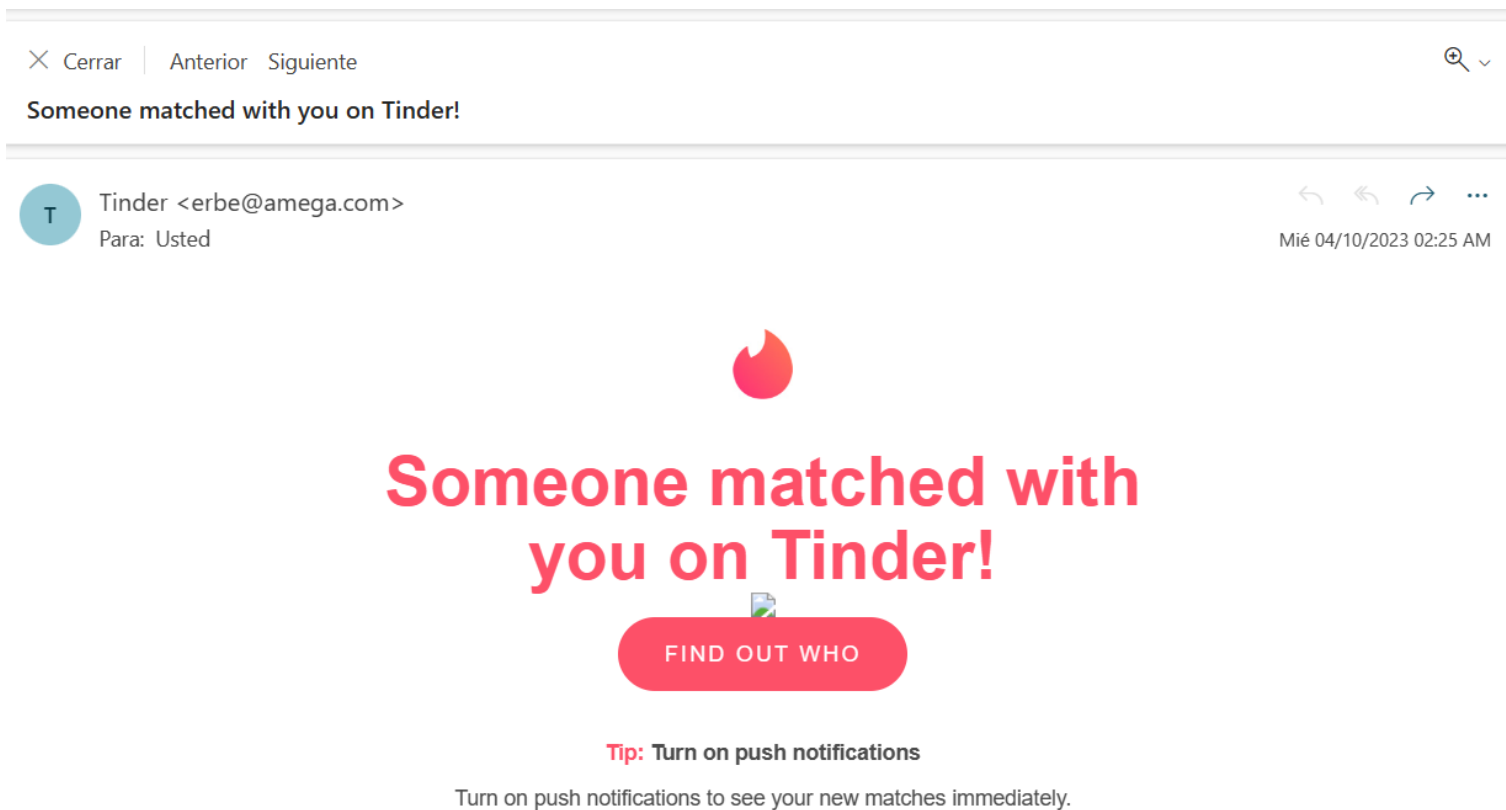
Implica convencer a las personas de que son parte de una organización confiable y que necesitan ayuda para solucionar un problema de seguridad. En lugar de que el atacante inicie el contacto, la víctima es persuadida para que se comuniquen con el atacante, creyendo que están buscando ayuda legítima. El atacante explota la confianza de la víctima para obtener información confidencial o acceso a sistemas restringidos.

Phishing

En esta modalidad, los perpetradores se disfrazan como entidades fiables, enviando correos electrónicos fraudulentos que aparentan ser legítimos, emanados de organizaciones confiables como instituciones bancarias o plataformas de servicios en línea. Estos mensajes electrónicos a menudo contienen enlaces que dirigen a sitios web fraudulentos meticulosamente diseñados para imitar las auténticas interfaces.

Los destinatarios son inducidos a proporcionar información sensible, como credenciales de inicio de sesión. La urgencia y el realismo cuidadosamente contruidos en estos mensajes contribuyen a engañar a las víctimas.

Ejemplo de Phishing



Smishing

Es un término que proviene de la combinación de las palabras "SMS" (Short Message Service) y "phishing". Se refiere a un tipo de ataque de ingeniería social en el cual los atacantes utilizan mensajes de texto (SMS) para engañar a las personas y obtener información confidencial o persuadirlas para que realicen acciones específicas, como hacer clic en enlaces maliciosos.





Vishing

Implica el uso de llamadas telefónicas para engañar a las personas y obtener información confidencial o realizar actividades maliciosas. El término "vishing" proviene de la combinación de las palabras "voice" (voz) y "phishing". En un ataque de vishing, los atacantes se hacen pasar por entidades legítimas, como instituciones financieras, empresas o agencias gubernamentales, y llaman a las víctimas para solicitar información confidencial



QRishing

QR Code Phishing o **QR Phishing**, es una técnica de ingeniería social que involucra el uso de códigos QR para dirigir a los usuarios a sitios web maliciosos o fraudulentos. En este tipo de ataque, los delincuentes colocan códigos QR falsos en lugares públicos, carteles, anuncios o correos electrónicos. Estos códigos QR están vinculados a sitios web que parecen legítimos.

Spear phishing

Es una forma altamente especializada de ataque de phishing en la que los ciberdelincuentes dirigen sus esfuerzos a individuos específicos o a organizaciones selectas. Implica una investigación cuidadosa sobre la víctima. Los atacantes recopilan información detallada sobre el objetivo, como direcciones de correo electrónico, nombres, cargos y conexiones sociales, para personalizar los mensajes de phishing y hacerlos más convincentes.





Whaling

Spear phishing a alto nivel, es una forma específica de ataque de phishing que se dirige a individuos o entidades de alto perfil dentro de una organización, como ejecutivos, gerentes de nivel C (CEO, CFO, CTO, etc.) o personas influyentes en la industria. A diferencia de los ataques de phishing comunes que se envían a grandes grupos de personas, el whaling se enfoca en personas específicas, claves en la estrategia de la empresa.

Potenciales daños de whaling



Pérdida de datos sensibles y confidenciales.



Fraude financiero y transferencias no autorizadas.



Daño a la reputación de la empresa.



Pérdida de productividad debido a investigaciones internas.



Litigios y multas por incumplimiento de regulaciones.



Amenazas continuas y persistencia de futuros ataques.



Impacto negativo en relaciones comerciales y socios.

Campañas de Phishing

- Configure una cuenta de correo en un servidor SMTP que brinde la posibilidad de hacer Spoofing.
- Configure un servidor web para alojar la página de destino de la simulación de Phishing.
- Aplique las medidas de seguridad pertinentes en ambos servidores para proteger la seguridad de la información.
- Adquiera y configure dominios para envío de correos de simulación de Phishing y para navegación web del sitio de Phishing simulado.
- Adquiera y configure certificados SSL para los dominios en cuestión
- Elabore un plan de contingencia para los dominios de simulación que caigan en listas negras globales.
- Elabore y siga un procedimiento de actualización y hardening de la infraestructura definida.

Campañas de Phishing

- Como recomendación, asegúrese de seleccionar una herramienta que automatice todo el ciclo de vida de la simulación de Phishing:
 - Calendarización de la campaña.
 - Envío de correos.
 - Registro de interacciones de los usuarios.
 - Repote de resultados en tiempo real.
 - Recolección de registros de auditoría inalterables.
 - Identificación y ocultado de falsos positivos.

Defina la duración de la campaña. **Es recomendable no extender la simulación por más de 48 horas**

Simulación de Phishing

Nuestra plataforma le permite planificar campañas de correos electrónicos de Phishing simulado con un par de clics, de manera rápida y eficiente. A través de esta herramienta podrá conocer las acciones de riesgo que ponen en peligro la información confidencial de su organización.

Nuestros contenidos predefinidos se mantienen actualizados y cubren las técnicas y temáticas de Phishing más frecuentes y novedosas utilizadas por los ciberdelincuentes. A su vez, usted puede crear sus propios escenarios de Phishing personalizados al 100%.

Muestre a la dirección reportes y estadísticas con el estado actual y avance de los usuarios en relación a la asimilación de los hábitos seguros.



Criptografía y Seguridad de datos

*(Cryptography & Data
Security)*



Gestión de accesos e identidad.

Identity and Access Management (IAM)



Seguridad en el Desarrollo de Software

*(Security Development
Lifecycle **SDLC**)*



Seguridad en Cómputo en la Nube

(Cloud Security)



Evaluación de Seguridad de la Información

(Security Assessment)



Informática Forense y Gestión de Incidentes

*(Forensics & Incident
Handling)*



Continuidad del Negocio y Recuperación de Desastres

*(Business Continuity &
Disaster Recovery)*



¡Muchas Gracias!