ANALISIS DE VULNERABILIDADES EN EL AMBITO DE CIBERSEGURIDAD

TECICO EN CONTROL DE LA SEGURIDAD DIGITAL
Instructor. JORGE ENRIQUE SANCHEZ PINO

Introducción a la seguridad informática



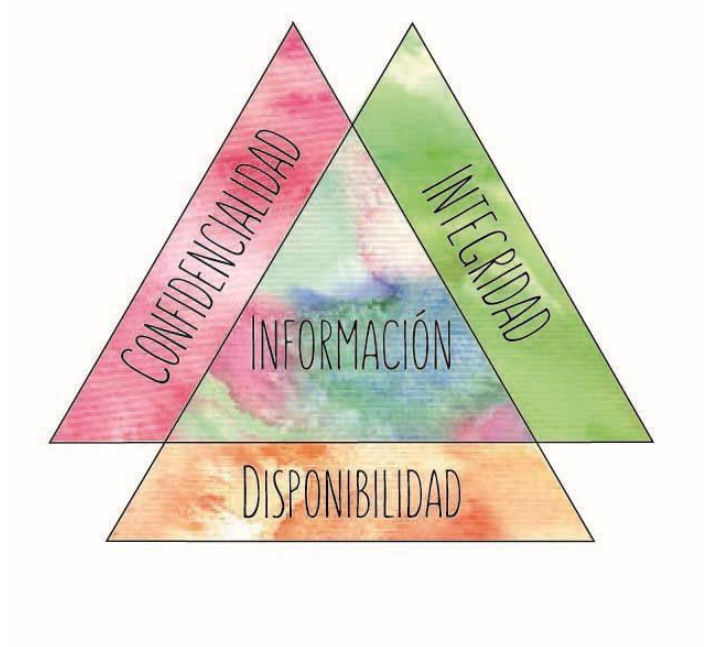
La seguridad de la información

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.



Componentes principales de la triada CIA

(conocida como la **Tríada** CIA, del inglés: "Confidentiality, Integrity, Availability") son los principios básicos de la **seguridad** de la información.
Se refiere a la **confidencialidad, integridad y disponibilidad** de la información de datos, independientemente de la forma, los datos pueden ser: electrónicos, impresos, mensajes de texto, audios u otras formas.
El triangulo de la Seguridad Informática.



Disponibilidad:

propiedad accesible y utilizable a demanda de la Entidad.



Integridad:

propiedad con exactitud y completitud de la información.

Confidencialidad:

propiedad de la información que la hace no disponible para ser divulgada a otros individuos, entidades o procesos no autorizados.

+ Privacidad:

es el derecho que tienen todos los titulares de la información que involucre datos personales o información clasificada que esté en poder de la Entidad en el marco de sus funciones.

Además, la seguridad de la información involucra la implementación de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.



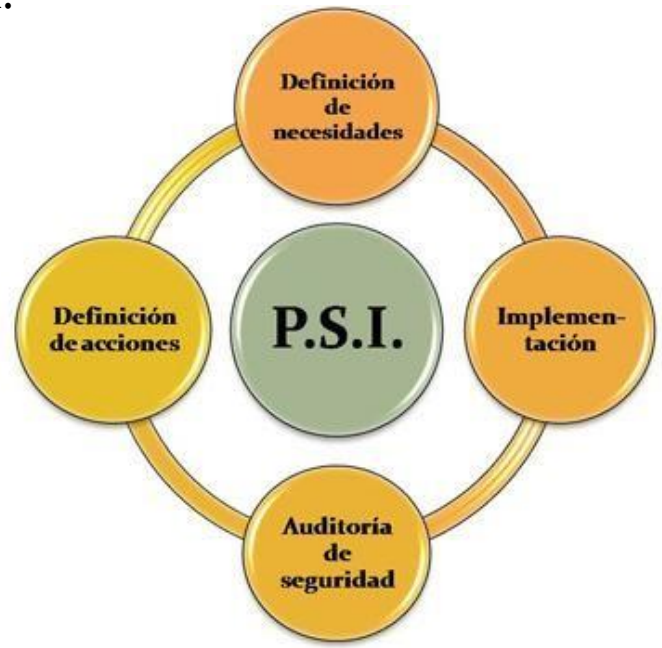
Principios e introducción

Los Gobiernos, entidades militares, instituciones financieras, los hospitales y las empresas privadas acumulan una gran cantidad de información confidencial sobre sus empleados, clientes, productos, investigación y su situación financiera. La mayor parte de esta información es recolectada, tratada, almacenada y puesta a la disposición de sus usuarios, en computadoras y trasmitida a través de las redes entre los ordenadores.



En caso de que la información confidencial de una empresa, sus clientes, sus decisiones, su estado financiero o nueva línea de productos caigan en manos de un competidor; se vuelva pública de forma no autorizada, podría ser causa de la pérdida de credibilidad de los clientes, pérdida de negocios, demandas legales o incluso la quiebra de la misma.

Por lo que proteger la información confidencial es un requisito del negocio, y en muchos casos también un imperativo ético y una obligación legal.



Confidencialidad

La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito a ser transmitida desde el comprador al comerciante y el comerciante de a una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos. Si una parte no autorizada obtiene el número de la tarjeta en modo alguno, se ha producido una violación de la confidencialidad.

La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla, cuando se publica información privada, cuando un laptop con información sensible sobre una empresa es robado, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad.





Integridad

Para la Seguridad de la Información, la integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la huella digital.





Disponibilidad

La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizado para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La Alta disponibilidad sistemas objetivo debe seguir estando disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.



Garantizar la disponibilidad implica también la prevención de ataque Denegación de servicio.

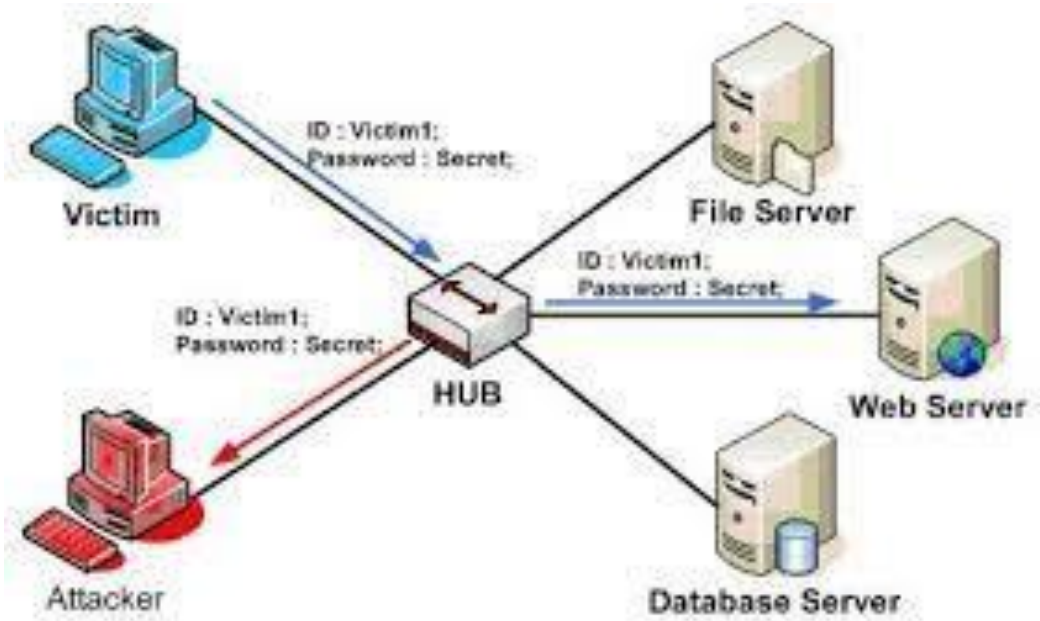
La disponibilidad además de ser importante en el proceso de seguridad de la información, es además variada en el sentido de que existen varios mecanismos para cumplir con los niveles de servicio que se requiera, tales mecanismos se implementan en infraestructura tecnológica, servidores de correo electrónico, de bases de datos, de web etc, mediante el uso de clusters o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, etc. La gama de posibilidades dependerá de lo que queremos proteger y el nivel de servicio que se quiera proporcionar.



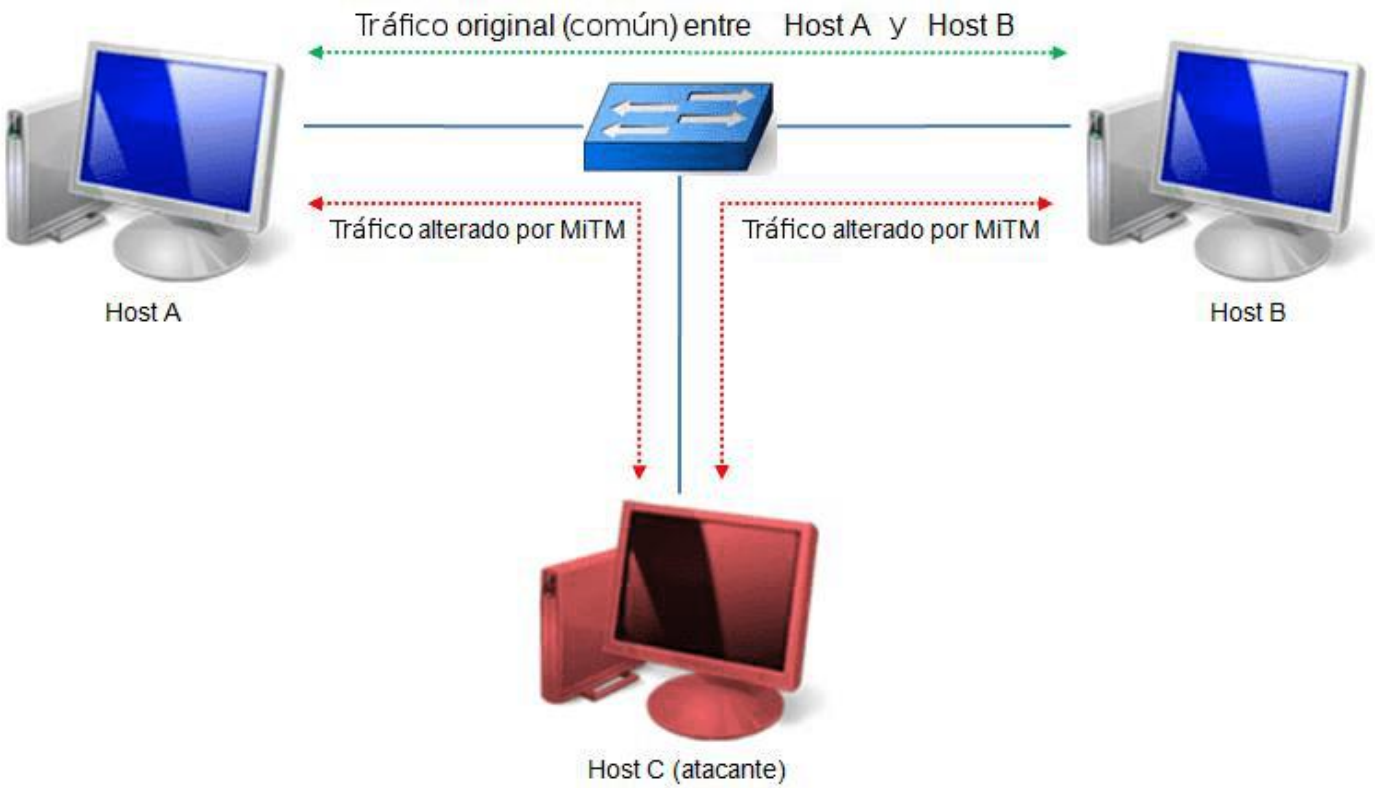
SPOOFING: Un ataque de suplantación de identidad es cuando una parte malintencionada se hace pasar por otro dispositivo o usuario en una red para lanzar ataques contra hosts de la red, robar datos, propagar malware o evitar los controles de acceso.



Algunos Ataques a los que tanto personas como compañías pueden estar expuestos o ser vulnerables a sufrir!!
SNIFFING: Corresponde al robo o la intercepción de datos al capturar el tráfico de la red utilizando un sniffer (una aplicación destinada a capturar paquetes de red).



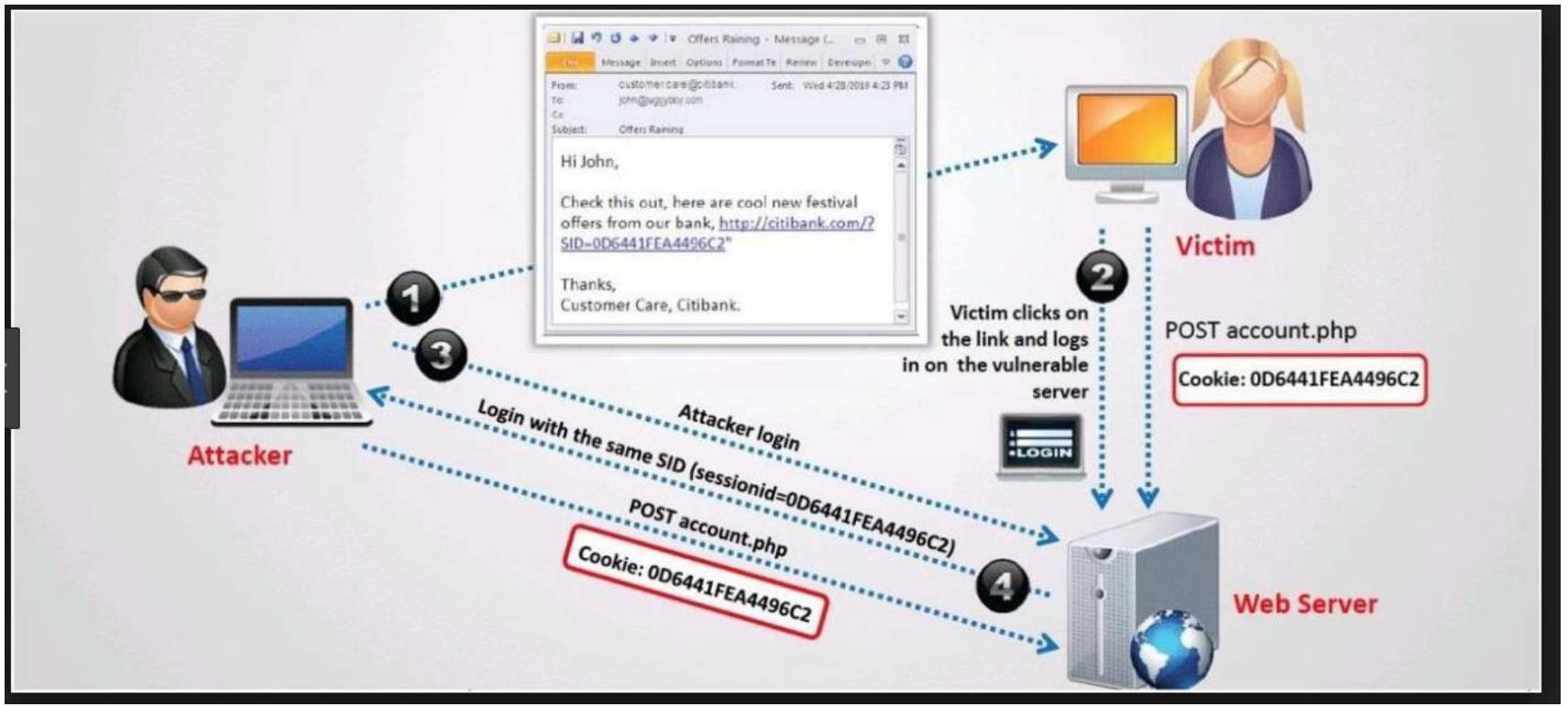
MAN-IN-THE-MIDDLE: Un ataque de hombre en el medio es un ataque en el que el atacante transmite en secreto y posiblemente altera las comunicaciones entre dos partes que creen que se están comunicando directamente entre sí.
DOS: Es un ataque destinado a apagar una máquina o red, haciéndola inaccesible para sus usuarios previstos.



Los ataques DoS logran esto inundando el objetivo con tráfico o enviándole información que desencadena un bloqueo. En ambos casos, el ataque DoS priva a los usuarios legítimos del servicio o recurso que esperaban.



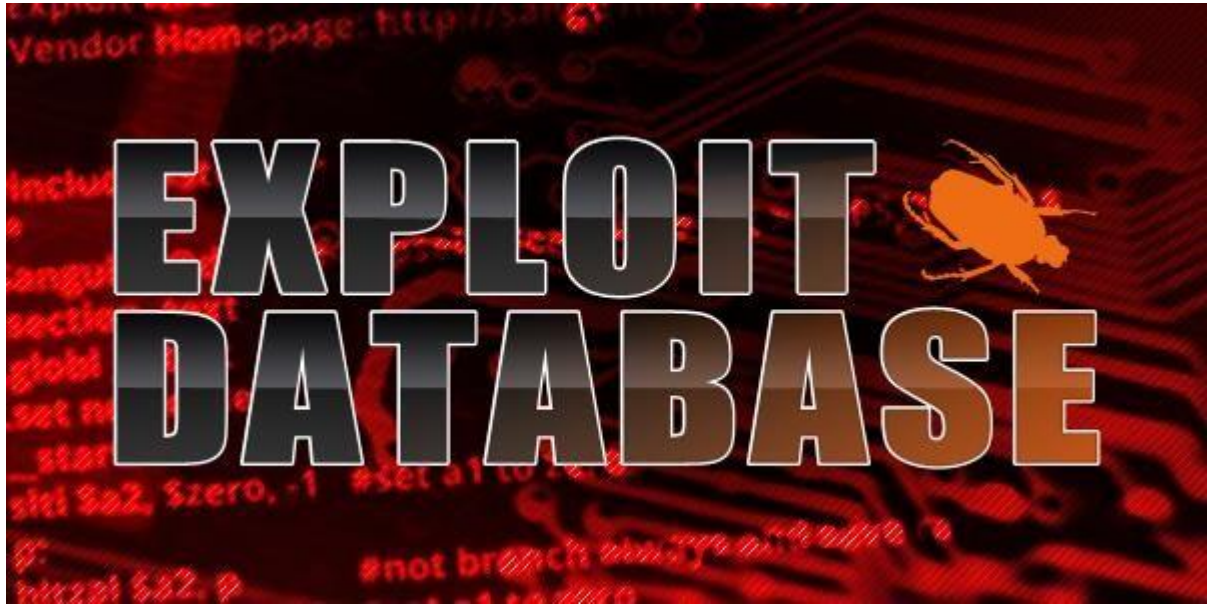
HIJACKING: Esto es básicamente una variante del ataque del hombre en el medio, pero implica tomar el control de un aspecto de la red de área de almacenamiento en lugar de simplemente capturar paquetes de datos.



PHISHING: Es un tipo de ataque de ingeniería social que a menudo se usa para robar datos de usuarios, incluidas las credenciales de inicio de sesión y los números de tarjetas de crédito. Ocurre cuando un atacante, disfrazado de entidad de confianza, engaña a una víctima para que abra un correo electrónico, un mensaje instantáneo o un mensaje de texto.



EXPLOIT: Un exploit es cualquier ataque que aprovecha las vulnerabilidades en aplicaciones, redes o hardware. Por lo general, toman la forma de software o código que tiene como objetivo obtener el control de las computadoras o robar datos de la red.



Servicios de Seguridad

El objetivo de un servicio de seguridad es mejorar la seguridad de los sistemas de procesamiento de datos y la transferencia de información en las organizaciones. Los servicios de seguridad están diseñados para contrarrestar los ataques a la seguridad y hacen uso de uno o más mecanismos de seguridad para proporcionar el servicio.



No Repudio

Proporciona protección contra la interrupción, por parte de alguna de las entidades implicadas en la comunicación, de haber participado en toda o parte de la comunicación. El servicio de Seguridad de No repudio o irrenunciabilidad está estandarizado en la ISO-7498-2.

No Repudio de origen: El emisor no puede negar que envío porque el destinatario tiene pruebas del envío, el receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor, de negar tal envío, tenga éxito ante el juicio de terceros. En este caso la prueba la crea el propio emisor y la recibe el destinatario.

Prueba que el mensaje fue enviado por la parte específica.



No Repudio de destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. Este servicio proporciona al emisor la prueba de que el destinatario legítimo de un envío, realmente lo recibió, evitando que el receptor lo niegue posteriormente. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.

Prueba que el mensaje fue recibido por la parte específica.

Si la autenticidad prueba quién es el autor de un documento y cual es su destinatario, el “no repudio” prueba que el autor envió la comunicación (no repudio en origen) y que el destinatario la recibió (no repudio en destino).

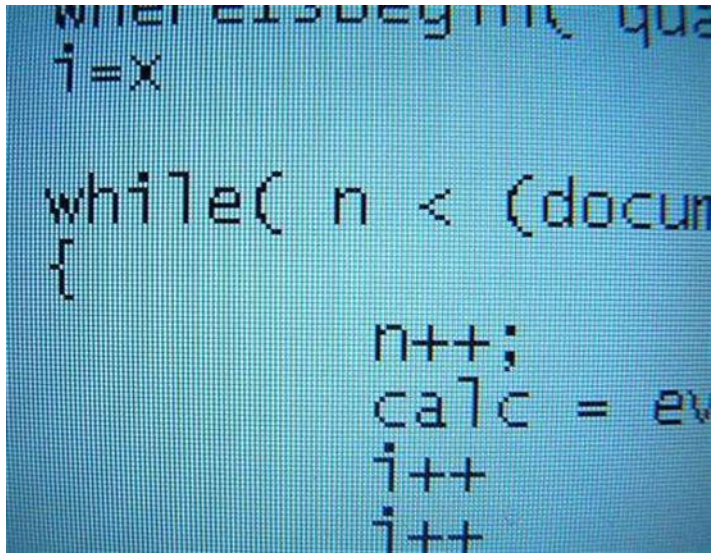
Principales atacantes

EL HACKER El Hacker es una persona con amplios conocimientos en tecnología, bien puede ser informática, electrónica o comunicaciones, mantiene permanentemente actualizado y conoce a fondo todo lo relacionado con programación y sistemas complejos; es un investigador nato que se inclina ante todo por conocer lo relacionado con cadenas de datos cifrados y las posibilidades de acceder a cualquier tipo de "información segura".

Su formación y las habilidades que poseen les da una experticia mayor que les permite acceder a sistemas de información seguros, sin ser descubiertos, y también les da la posibilidad de difundir sus conocimientos para que las demás personas se enteren de cómo es que realmente funciona la tecnología y conozcan las debilidades de sus propios sistemas de información.



EL CRACKER Se denomina así a aquella persona con comportamiento compulsivo, que alardea de su capacidad para reventar sistemas electrónicos e informáticos. Un Cracker es un hábil conocedor de programación de Software y Hardware; diseña y fabrica programas de guerra y hardware para reventar software y comunicaciones como el teléfono, el correo electrónico o el control de otros computadores remotos.



EL LAMMER A este grupo pertenecen aquellas personas deseosas de alcanzar el nivel de un hacker pero su poca formación y sus conocimientos les impiden realizar este sueño. Su trabajo se reduce a ejecutar programas creados por otros, a bajar, en forma indiscriminada, cualquier tipo de programa publicado en la red.



EL COPYHACKER Son una nueva generación de falsificadores dedicados al crackeo de Hardware, específicamente en el sector de tarjetas inteligentes. Su estrategia radica en establecer amistad con los verdaderos Hackers, para copiarles los métodos de ruptura y después venderlos los bucaneros.
Los Copyhackers se interesan por poseer conocimientos de tecnología, son aficionados a las revistas técnicas y a leer todo lo que hay en la red. Su principal motivación es el dinero.



BUCANEROS

Son los comerciantes de la red más no existen en ella; aunque no poseen ningún tipo de formación en el área de los sistemas, si poseen un amplio conocimiento en área de los negocios.



PHREAKER

Se caracterizan por poseer vastos conocimientos en el área de telefonía terrestre y móvil, incluso más que los propios técnicos de las compañías telefónicas; recientemente con el auge de los celulares, han tenido que ingresar también al mundo de la informática y del procesamiento de datos.



NEWBIE

Es el típico "novatos" de red, sin proponérselo tropieza con una página de Hacking y descubre que en ella existen áreas de descarga de buenos programas de Hackeo, baja todo lo que puede y empieza a trabajar con ellos.

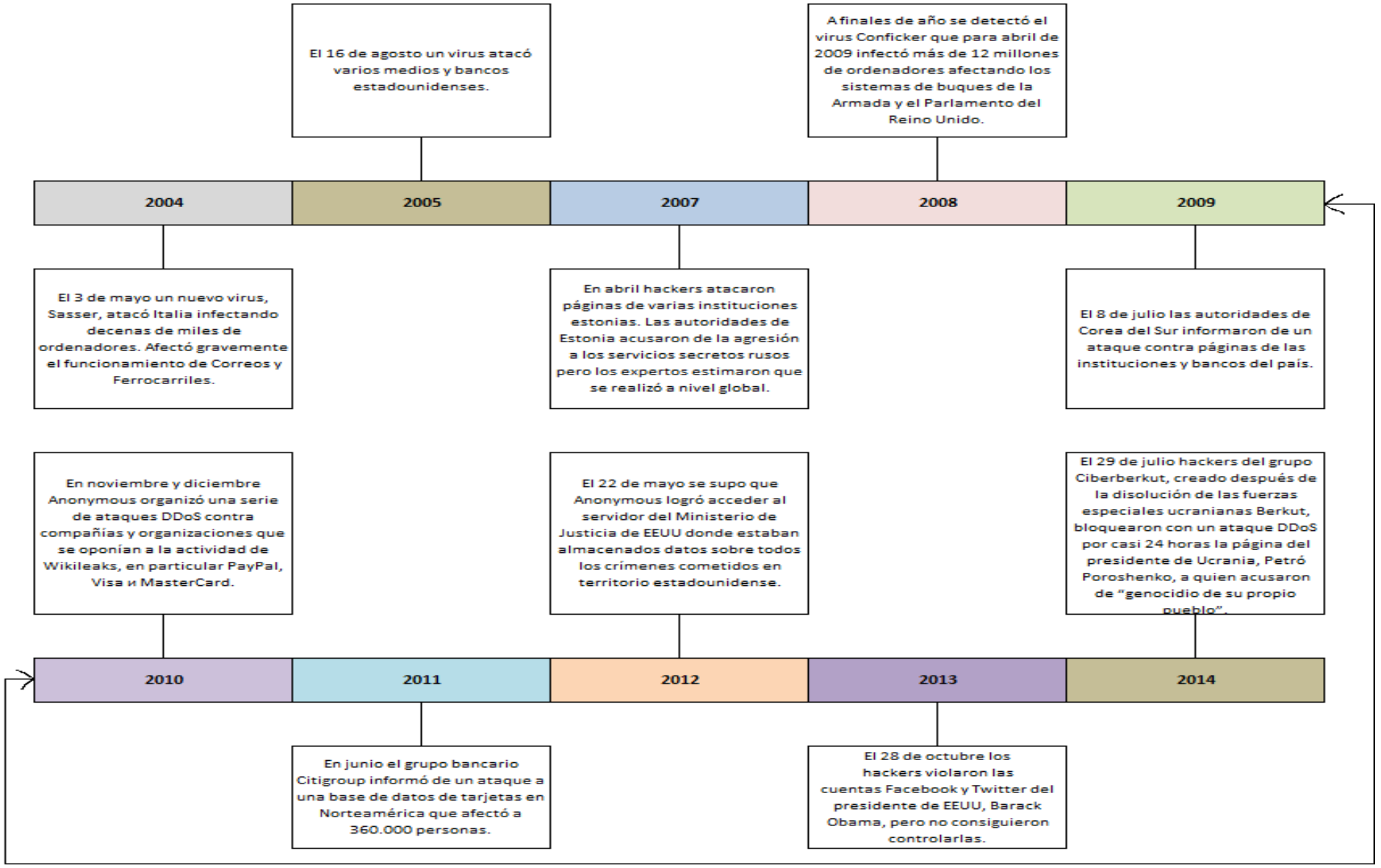


SCRIPT KIDDIE

Denominados también “Skid kiddie”, son simples usuarios de Internet, sin conocimientos sobre Hack o Crack aunque aficionados a estos temas no los comprenden realmente, simplemente son internautas que se limitan a recopilar información de la red y a buscar programas que luego ejecutan sin los más mínimos conocimientos, infectando en algunos casos de virus a sus propios equipos.También podrían denominarse los “Pulsa Botones o Clickquiadores“ de la red.



Ataques por año



Planificación de la seguridad

Hoy en día la rápida evolución del entorno técnico requiere que las organizaciones adopten un conjunto mínimo de controles de seguridad para proteger su información y sistemas de información. El propósito del plan de seguridad del sistema es proporcionar una visión general de los requisitos de seguridad del sistema y se describen los controles en el lugar o los previstos para cumplir esos requisitos. El plan de seguridad del sistema también delinea las responsabilidades y el comportamiento esperado de todos los individuos que acceden al sistema. Debe reflejar las aportaciones de distintos gestores con responsabilidades sobre el sistema, incluidos los propietarios de la información, el propietario de la red, y el alto funcionario de la agencia de información de seguridad (SAISO).

Los administradores de programas, los propietarios del sistema, y personal de seguridad en la organización debe entender el sistema de seguridad en el proceso de planificación. Los responsables de la ejecución y gestión de sistemas de información deben participar en el tratamiento de los controles de seguridad que deben aplicarse a sus sistemas.

El manejo de riegos dentro de la seguridad en la información

Dentro de la seguridad en la información se lleva a cabo la clasificación de las alternativas para manejar los posibles riegos que un activo ó bien puede tener dentro de los procesos en una empresa. Esta clasificación lleva el nombre de manejo de riegos. El manejo de riesgos, conlleva una estructura bien definida, con un control adecuado y su manejo, habiéndolos identificado, priorizados y analizados, a través de acciones factibles y efectivas. Para ello se cuenta con las siguientes técnicas de manejo del riesgo:



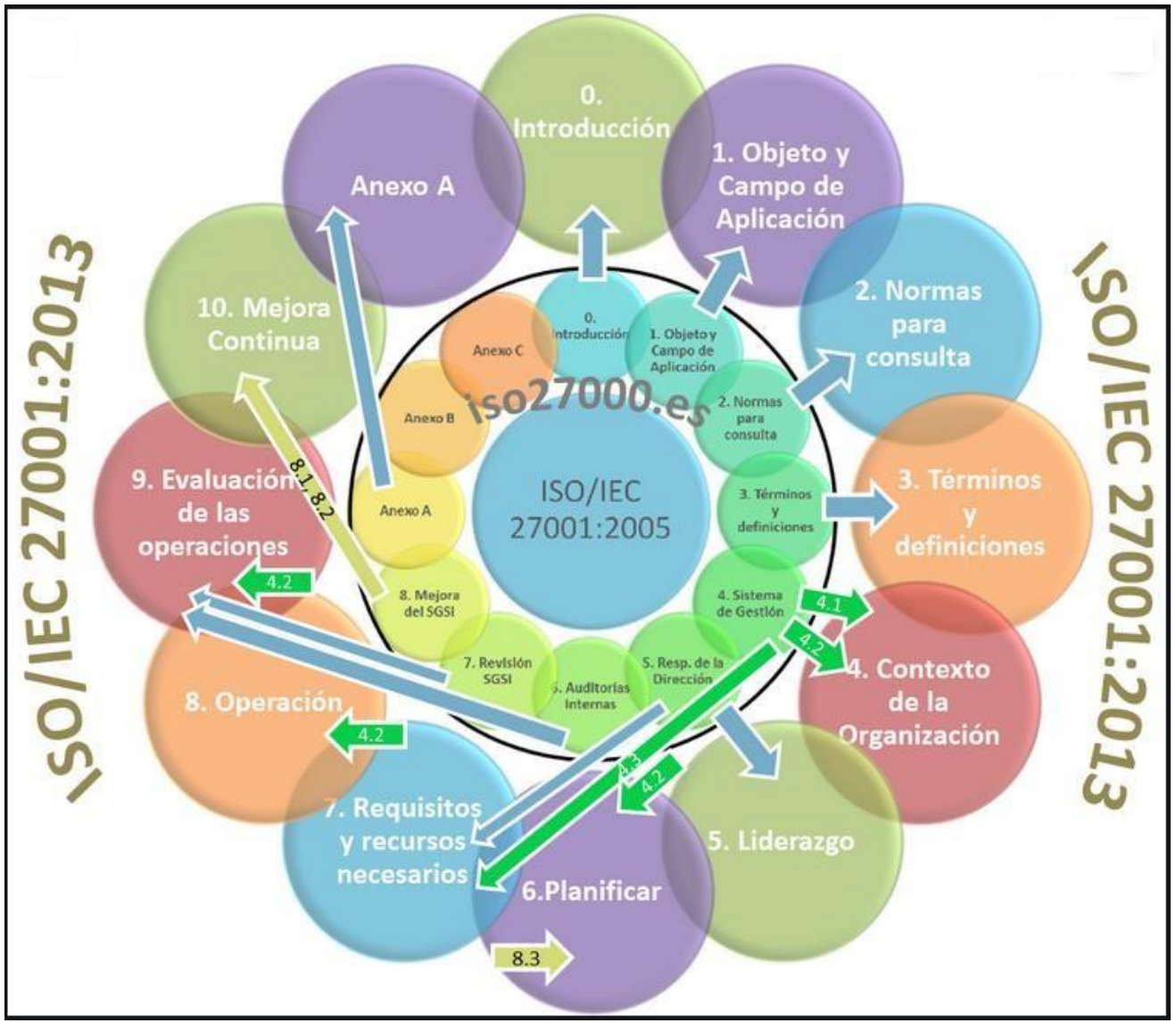
Evitar. Es logra cambios significativos por mejoramiento, rediseño o eliminación, en los procesos, siendo el resultado de adecuados controles y acciones realizadas.
Reducir. Cuando el riesgo no puede evitarse por tener varias dificultades de tipo operacional, la alternativa puede ser su reducción hasta el nivel más bajo posible. Esta opción es la más económica y sencilla y se consigue optimizando los procedimientos y con la implementación de controles.
Retener. Cuando se reduce los riegos, se podría retener los riesgos residuales. Dentro de los planes del manejo de riegos de la empresa debe plantear como manejar dichos riegos si ocurrieran.
Transferir. Es buscar un respaldo y compartir el riego con otros controles o entidades. Esta técnica se usa ya sea para eliminar un riesgos de un lugar y transferirlo a otro, ó para minimizar el mismo, compartiéndolo con otras entidades.

Estándares de seguridad de la información

- ISO/IEC 27000-series
- ISO/IEC 27001
- ISO/IEC 17799

Otros estándares relacionados

- COBIT
- ISACA
- ITIL



Certificaciones

- CISM - CISM Certificaciones [4] : Certified Information Security Manager
- CISSP - CISSP Certificaciones [5] : Security Professional Certification
- GIAC - GIAC Certificaciones [6] : Global Information Assurance Certification

Certificaciones independientes en seguridad de la información

- CISA- Certified Information Systems Auditor , ISACA
- CISM- Certified Information Security Manager, ISACA
- Lead Auditor ISO27001- Lead Auditor ISO 27001, BSI
- CISSP - Certified Information Systems Security Professional, ISC2
- SECURITY+, COMPTia - Computing Technology Industry Association
- CEH - Certified Ethical Hacker
- PCI DSS - PCI Data Security Standard

Herramientas

CRYPTOOL
WIRESHARK
KALI LINUX