



SEGURIDAD Y AUDITORIA DE SISTEMAS

MG. HANS QUISPE ARCOS
HANS.QUISPE@UNICA.EDU.PE

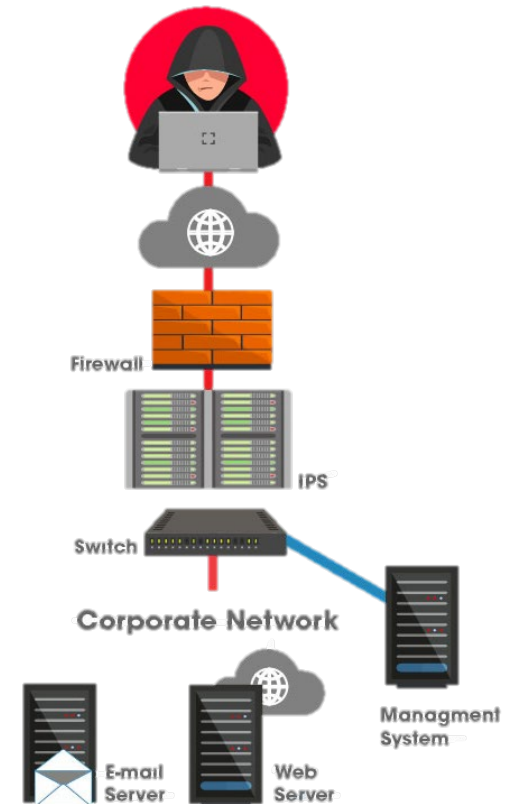


<https://youtu.be/6-asM2Bh2yE>

Sistemas de seguridad (IDS / IPS)



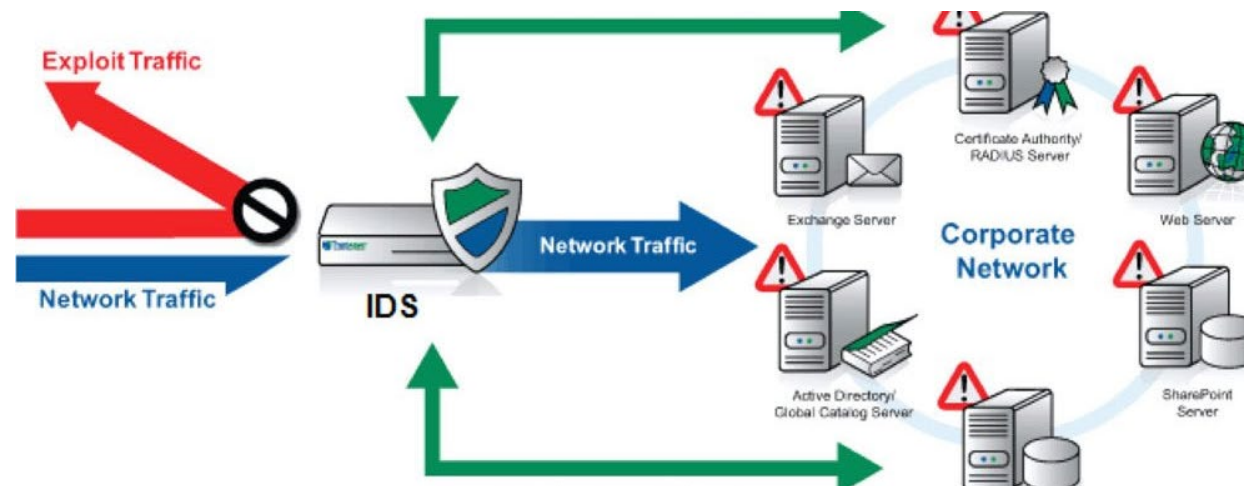
UNIVERSIDAD SAN LUIS GONZAGA - ICA



Introducción - IDS

Un IDS o sistema de detección de intrusos es un programa usado para detectar accesos no autorizados a un computador o a una red.

El IDS suele tener sensores virtuales con los que el núcleo del IDS puede obtener datos externos. El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.





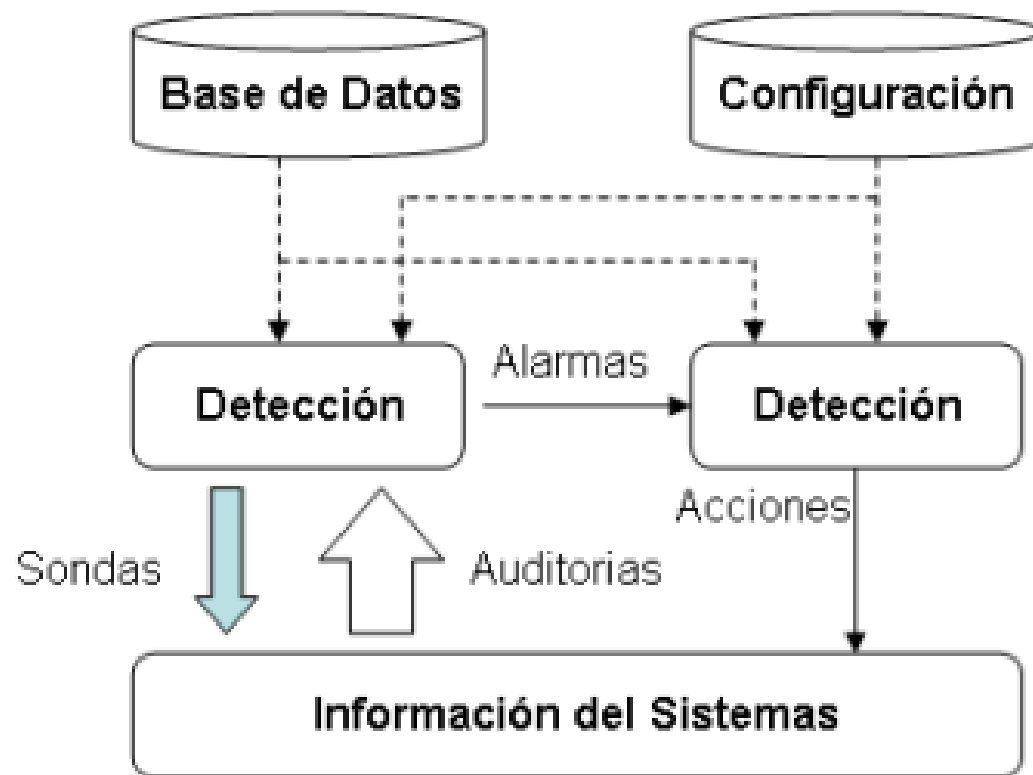
Funcionamiento

El funcionamiento de estas herramientas se basa en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados etc.

Normalmente esta herramienta se integra con un firewall ya que no puede detener los ataques por sí solo.



Funcionamiento





Tipos de IDS

- (HostIDS) El principio de funcionamiento de un HIDS depende del éxito de los intrusos, que generalmente dejen rastros de sus actividades en el equipo atacado, cuando intentan adueñarse del mismo, con propósito de llevar a cabo otras actividades.
- (NetworkIDS): un IDS basado en red, detectando ataques a todo el segmento de la red. Su interfaz debe funcionar en modo promiscuo capturando así todo el tráfico de la red.



Tipos de IDS

- Sistema pasivo: El sensor detecta una posible intrusión, almacena la información y manda una señal de alerta que se almacena en una base de datos.
- Sistema reactivo: El IDS responde a la actividad sospechosa reprogramada el cortafuegos para que bloquee el tráfico que proviene de la red del atacante.

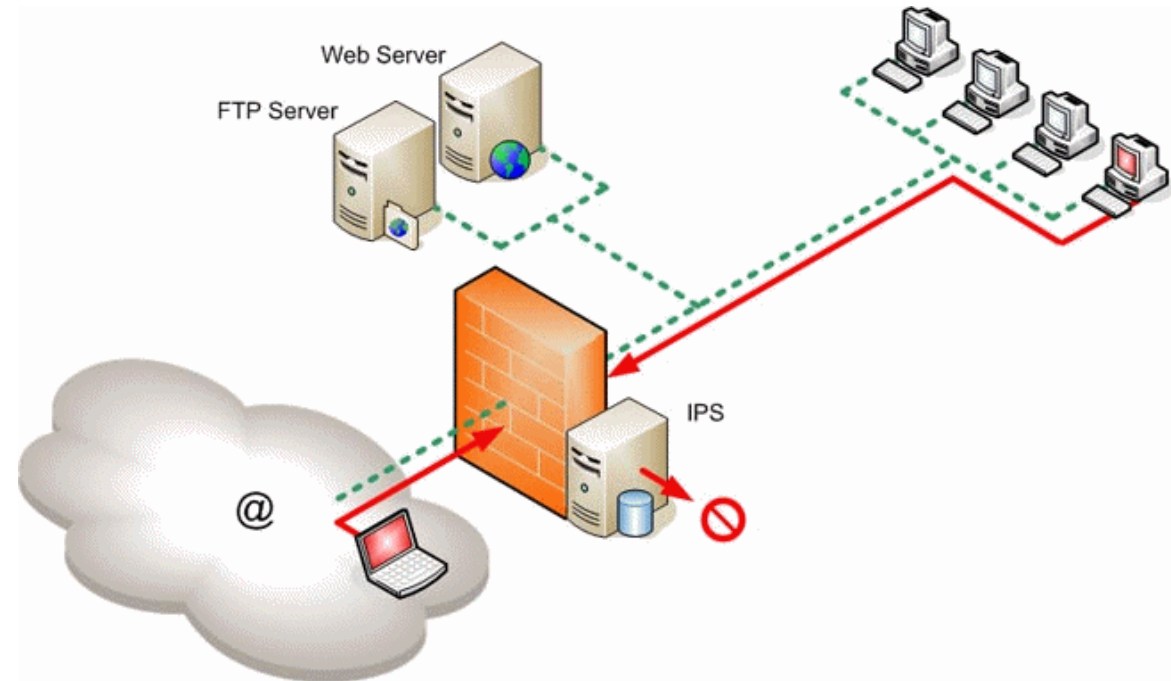


Mecanismo de detección de un ataque

- Heurística.
- Patrón
- Inteligencia Artificial

Introducción - IPS

A diferencia de los IDS esta nueva tecnología no se limita solo a escuchar el tráfico de la red y a mandar alertas en una consola, después de que ocurre una intrusión, el IPS funciona a nivel de la capa 7 tiene la capacidad de descifrar protocolos como HTTP, FTP y SMTP, algunos IPS permiten establecer reglas como se lo hace en los Firewalls.



Ventajas



- Protección preventiva antes de que ocurra el ataque.
- Defensa completa (Vulnerabilidades del Sistema Operativo, Puertos, Trafico de IP, códigos maliciosos e intrusos).
- Maximiza la seguridad y aumenta la eficiencia en la prevención de intrusiones o ataques a la red de una empresa.
- Fácil instalación, configuración y administración.
- Es escalable y permite la actualización de dispositivos a medida que crece la empresa.

Características de un IPS



- Capacidad de reacción automática ante incidentes.
- Aplicación de nuevos filtros conforme detecta ataques en progreso.
- Mínima vigilancia.
- Disminución de falsas alarmas de ataques a la red.
- Bloqueo automático frente a ataques efectuados en tiempo real.
- Protección de sistemas no parchados.
- Optimización en el rendimiento del tráfico de la red-

¿QUÉ HEMOS APRENDIDO?



Gracias





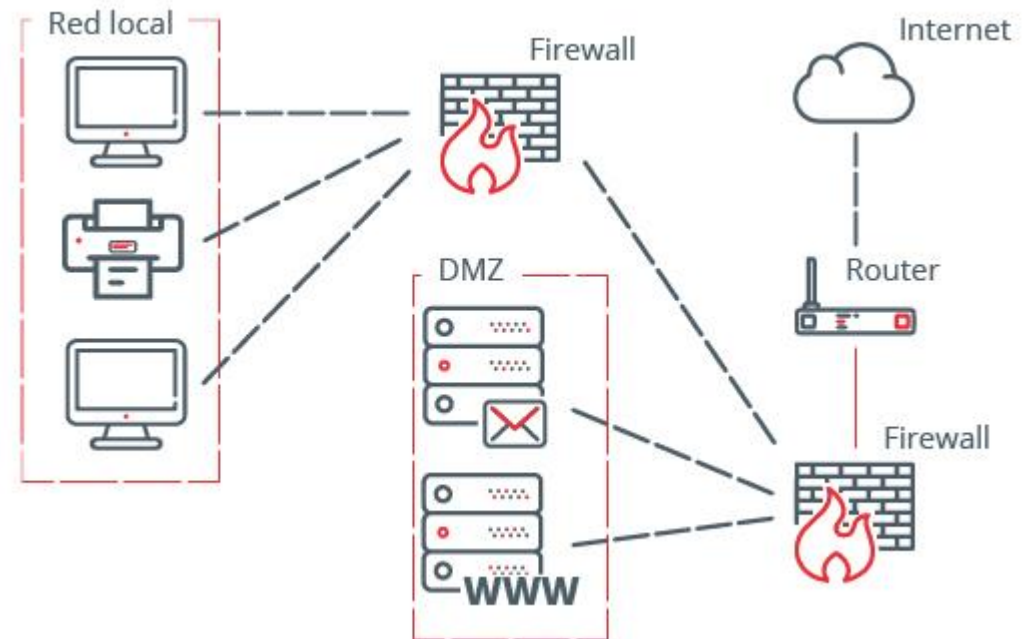
SEGURIDAD Y AUDITORIA DE SISTEMAS

MG. HANS QUISPE ARCOS
HANS.QUISPE@UNICA.EDU.PE

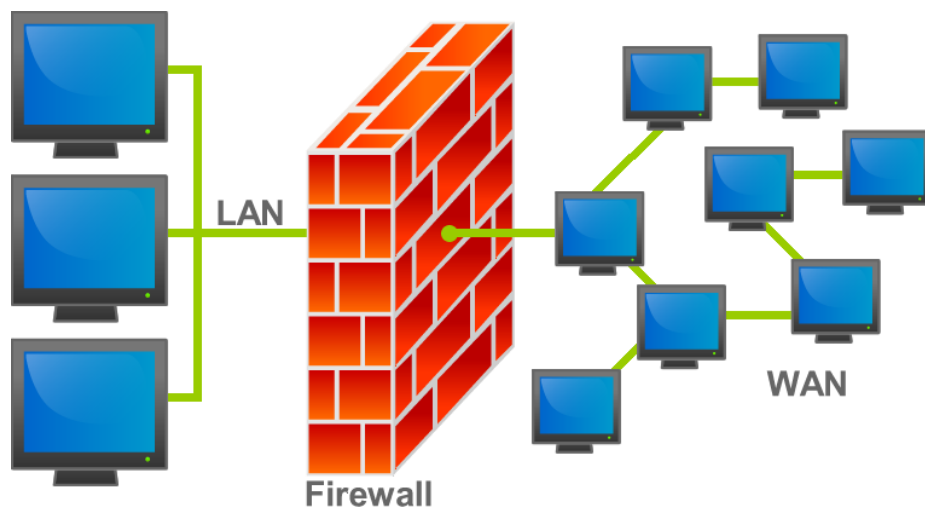


<https://www.youtube.com/watch?v=YR8xaXvGcWc>

Firewall y DMZ



Firewall



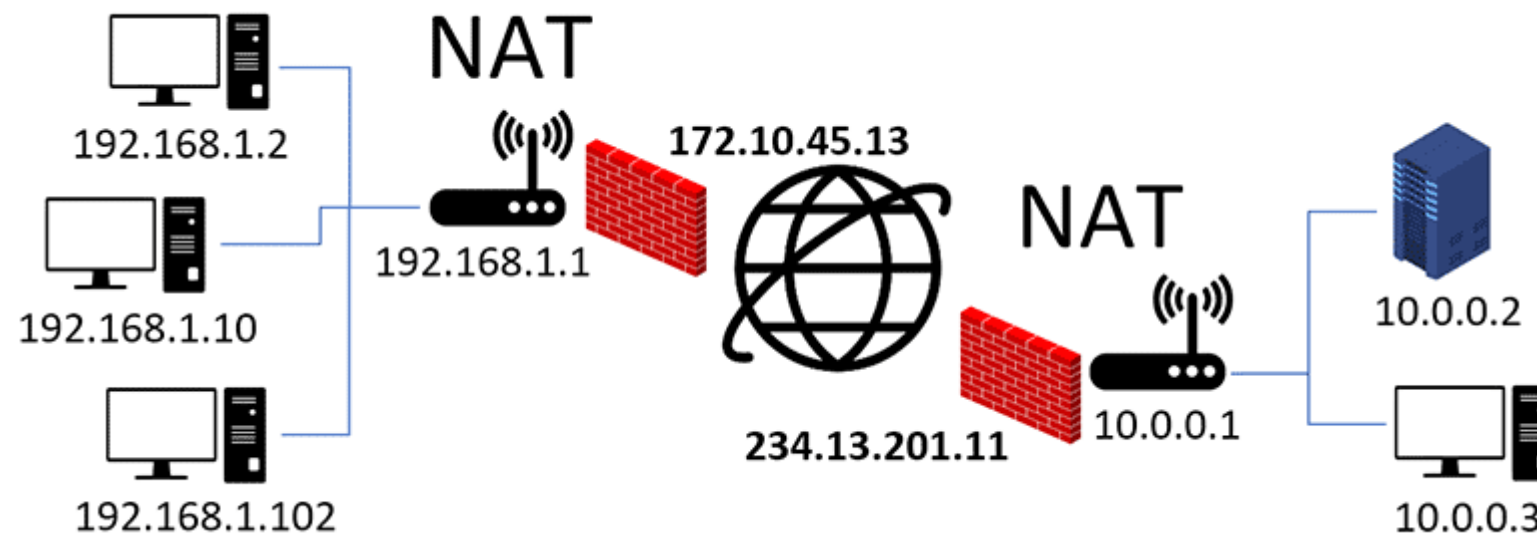
Un firewall analiza el tráfico que de nuestra red para diferenciar el tráfico permitido y el prohibido, bloqueando este último. Además permite una completa gestión del acceso a Internet por parte de todos los usuarios y equipos de la red local así como controlar y gestionar el acceso a los recursos corporativos desde cualquier sitio o dispositivo a través de Internet o la red interna.

Firewall

Tipos de Firewall

NAT

Network Address Translator, o en español traductor de direcciones de red. Su función es precisamente esa, traducir las direcciones para que sean posibles las conexiones. El NAT es una parte fundamental entre nuestros dispositivos e Internet.





Ventajas de las redes NAT

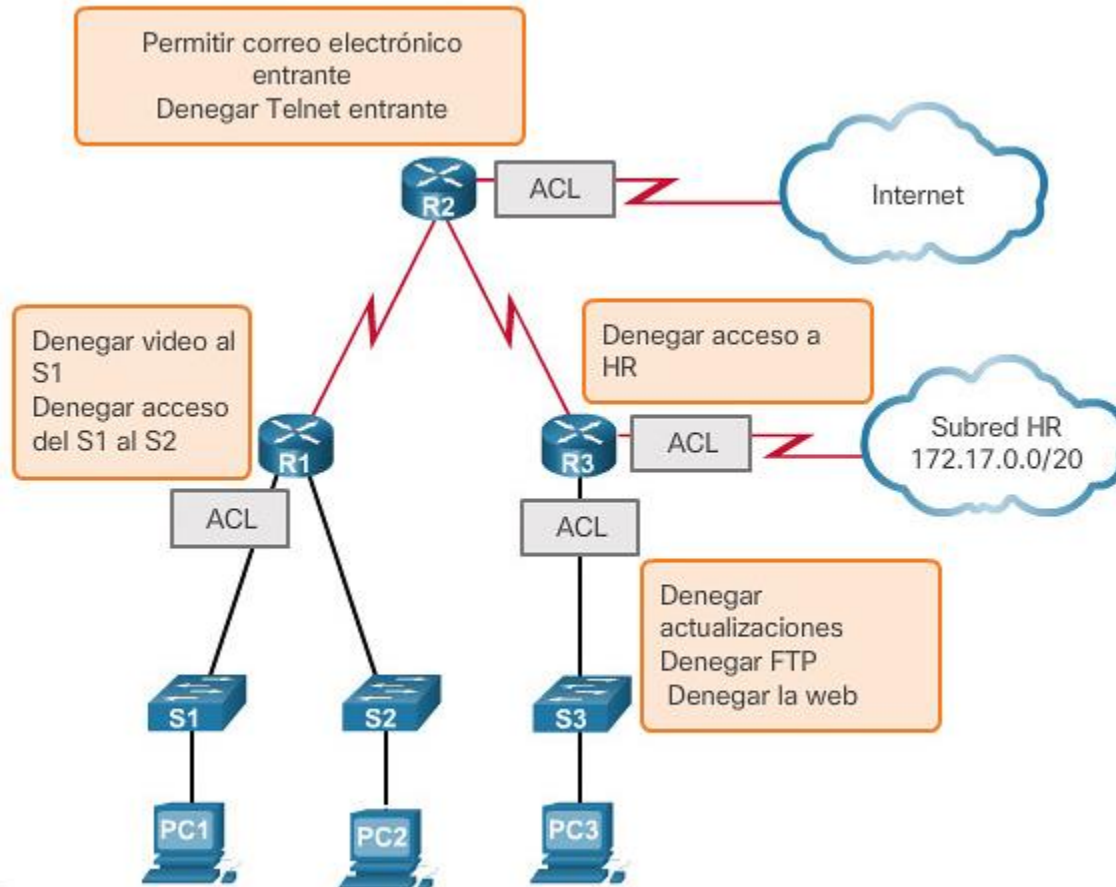
- ☐ Conserva los esquemas y rangos de direccionamiento registrados legalmente.
- ☐ Conserva las direcciones a través de la multiplexación de aplicaciones a nivel de puertos.
- ☐ Aumenta la flexibilidad de las conexiones a las redes públicas.
- ☐ Permite ocultar las direcciones IPv4 privadas de los usuarios y otros dispositivos



Desventajas de las redes NAT

- Debido al proceso de traducción de direcciones que realiza, incrementa en *delay* o lentitud.
- Se pierde el direccionamiento de extremo a extremo.
- Así mismo, se pierde también la trazabilidad de IPv4 de extremo a extremo debido a dicha traducción de direcciones.
- Debido a lo anterior, se dificulta la utilización de protocolos de tunneling como el IPsec, o conexión de túneles VPN, entre otros

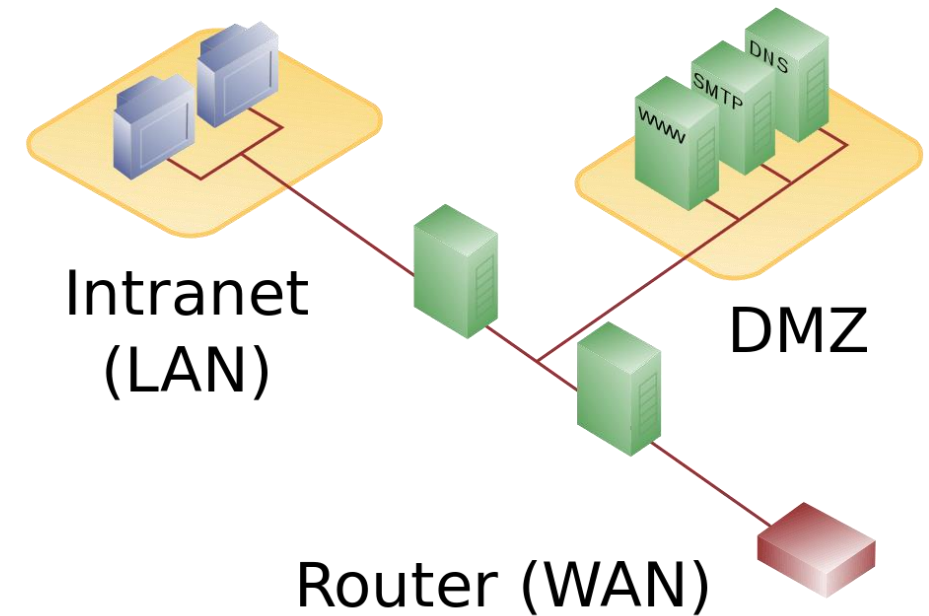
ACL



En seguridad informática , una lista de control de acceso (ACL) es una lista de permisos asociados con un recurso del sistema (objeto). Una ACL especifica a qué usuarios o procesos del sistema se les otorga acceso a los objetos, así como qué operaciones se permiten en objetos determinados

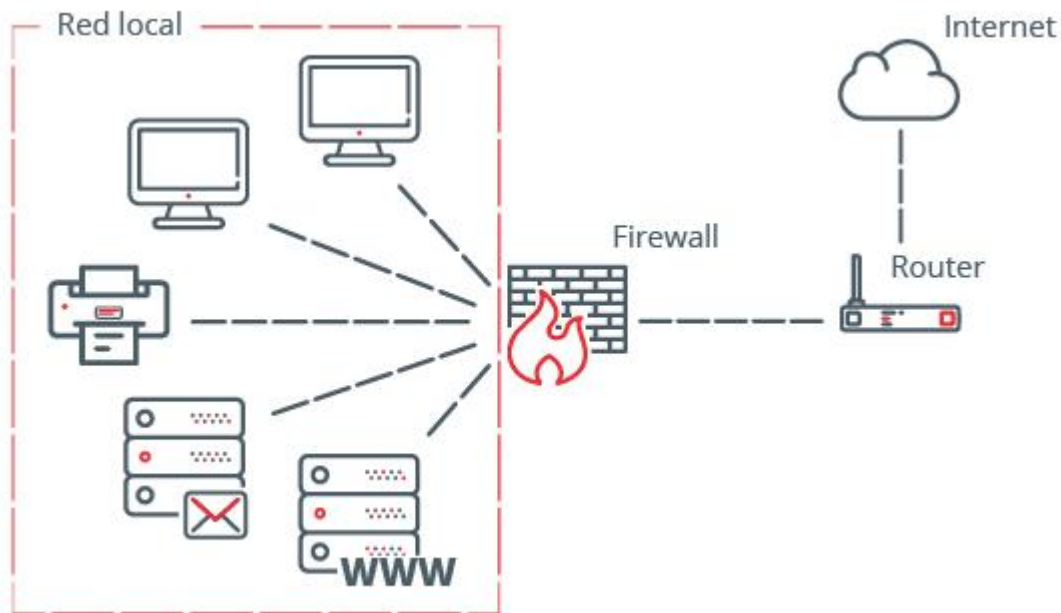
DMZ

La DMZ o zona desmilitarizada es una porción de una red empresarial situada tras un cortafuegos pero fuera de la red interna o segmentada de ella. La DMZ normalmente alberga servicios públicos, como servidores web, de correo y de dominios.

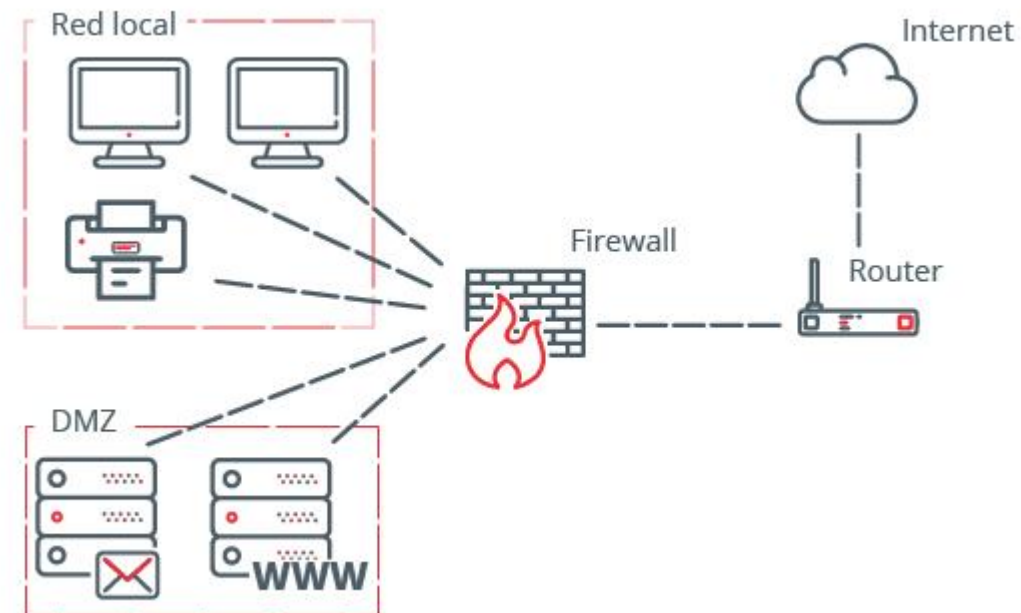


Arquitectura DMZ

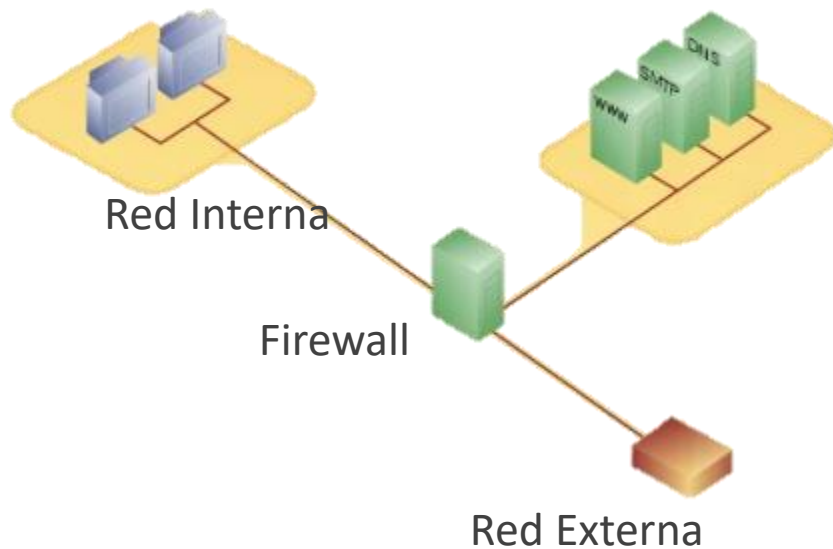
Red Interna



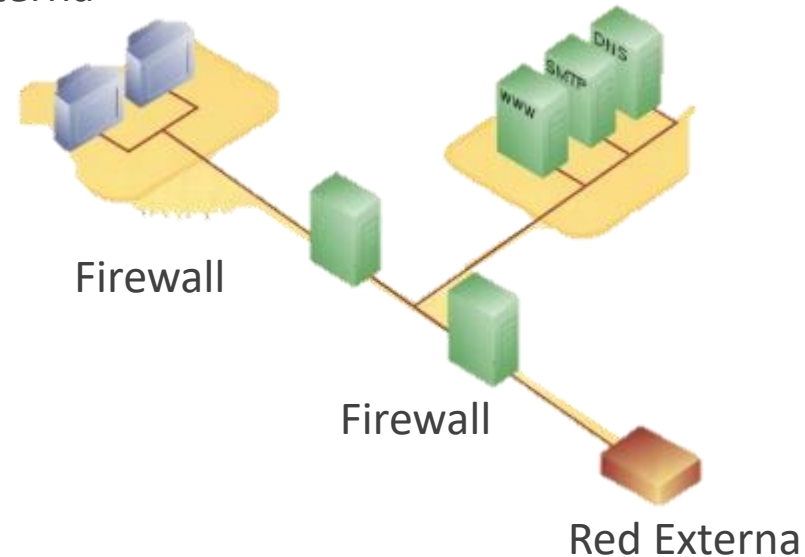
Red Interna con DMZ



Arquitectura DMZ



Red Interna



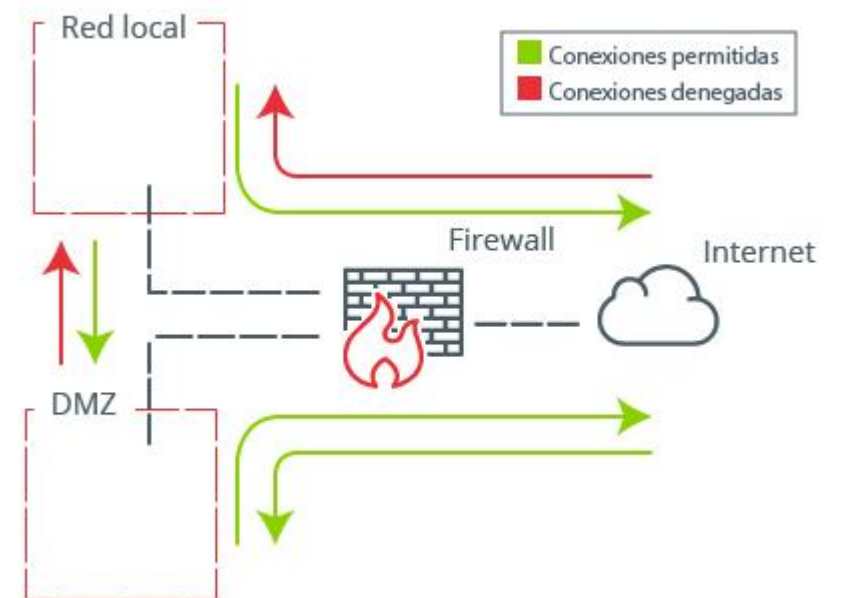
Beneficios de DMZ

- ☐ Aislamiento de segmentación.
- ☐ Servicio de Proxy.
- ☐ Carga de trabajo.
- ☐ Reconocimiento de red.



Reglas básicas de un firewall con DMZ

Origen	Destino	Política
Internet	DMZ	Permitido
Internet	LAN	Denegado
DMZ	Internet	Permitido
DMZ	LAN	Denegado
LAN	DMZ	Permitido
LAN	Internet	Permitido



¿QUÉ HEMOS APRENDIDO?



Gracias





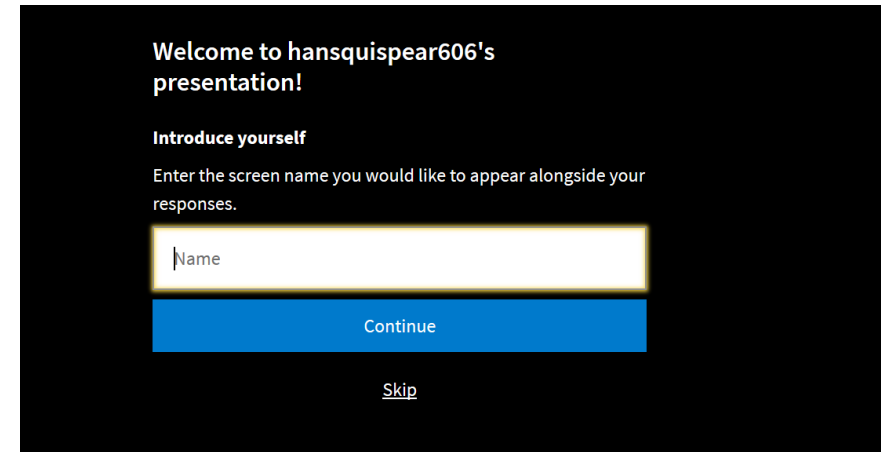
SEGURIDAD Y AUDITORIA DE SISTEMAS

MG. HANS QUISPE ARCOS
HANS.QUISPE@ÚNICA.EDU.PE

2023 © Mg. Hans Quispe Arcos

NORMAS DE CONVIVENCIA

- Silenciar celulares.
- Para la participación durante la sesión, lo puedes realizar de la siguiente manera:
 - Realizando tus preguntas por el chat de la sesión.
 - Levantando la mano, para abrir el micrófono y dialogar.
 - De ser factible activa tu cámara durante la participación.
- Para las actividades interactivas, es necesario que:
 - Ingreses a la url: <https://pollev.com/hansquispear606>
 - Escribir tus Apellidos y Nombres completos.

A screenshot of a presentation welcome screen with a black background. The text is white. It says "Welcome to hansquispear606's presentation!". Below that, it says "Introduce yourself" and "Enter the screen name you would like to appear alongside your responses.". There is a white text input field with the placeholder text "Name". Below the input field is a blue button with the text "Continue". At the bottom, there is a link that says "Skip".

Welcome to hansquispear606's presentation!

Introduce yourself

Enter the screen name you would like to appear alongside your responses.

Name

Continue

[Skip](#)

¿Cuál es la rama de la ingeniería de sistemas por la que se están inclinando?

¿Cuál es la expectativa del curso?

Powered by  **Poll Everywhere**

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app

INTRODUCCIÓN DE SEGURIDAD

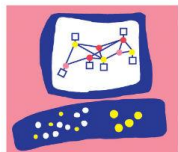


¿Qué tan importante cree usted, que es la seguridad hoy en día en la organizaciones y porque?

¿Conoces herramientas para explotar vulnerabilidades?

Powered by  **Poll Everywhere**

Start the presentation to see live content. For screen share software, share the entire screen. Get help at pollev.com/app



Check Point[®]
SOFTWARE TECHNOLOGIES LTD.



INTRODUCCIÓN DE SEGURIDAD

No se puede empezar a hablar de seguridad sin conocer un poco acerca de los hackers

Los hackers son personas sumamente hábiles para vulnerar los sistemas de seguridad y pueden estar en cualquier lado.

Ahora abordaremos los temas de perdidas económicas, los mitos y paranoias que se han generado por desconocimiento del tema de seguridad.

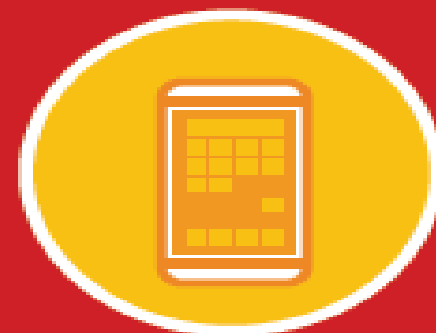


Situación Actual de la Seguridad

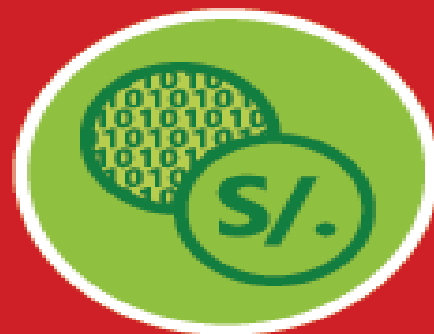
- La situación actual de la seguridad ha variado notablemente desde los gusanos y los virus.
- Las pérdidas por falta de una acción integral de seguridad son enormes.



Conectividad



Smartphones



**Dinero
electrónico**

El cliente ha
evolucionado ...

BANK

30+ AÑOS
ATRÁS...

+95%



Interacciones
Bancarias eran cerca
de la agencias mas
cercana a la casa

15+ AÑOS
ATRÁS...

+60%

Interacciones Bancaria
eran en canales
digitales
(ATM's y Banca Web)

Servicios Financieros
Cuando sea, Donde sea!!!



+50% ▲

Interacciones Bancarias
via canales digitales

Milennials esperan mas
que un servicio
una experiencia

+30% ▲

Interacciones Bancarias
via celulares y similares



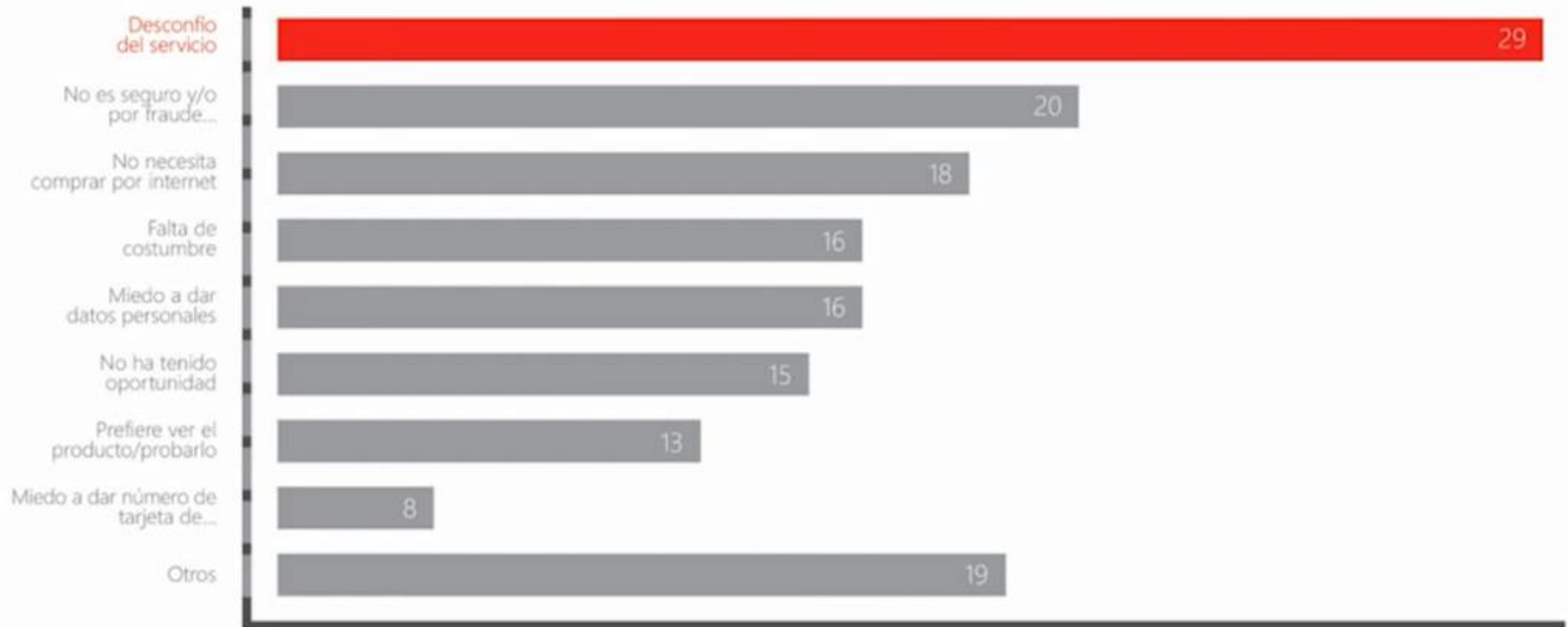
Clientes de alto valor todavía
están representados por los
no-milenials
(Excelencia del
Servicio)

+45%

Clientes que consultan la
web para informarse de
productos financieros
(Pre-Venta)

... a una experiencia
continuamente conectada

Razones por las que los entrevistados Peruanos nunca han comprado por Internet



Hackers: Paranoia o realidad

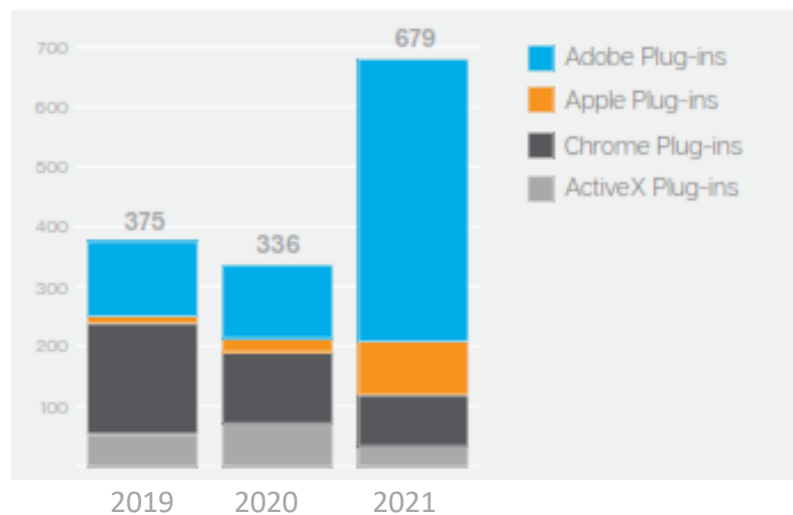
Para los hackers todo sistema es atractivo ya que este puede tener información Valiosa, sea utilizado como puente o para almacenar Información valiosa

- ☐ Se encuentran en todos lados.
- ☐ No son genios necesariamente.
- ☐ El Administrador de Seguridad debe desconfiar de todos incluso de si mismo.
- ☐ El sistema es tan seguro como el Administrador.
- ☐ Los equipos actúan según su programación.

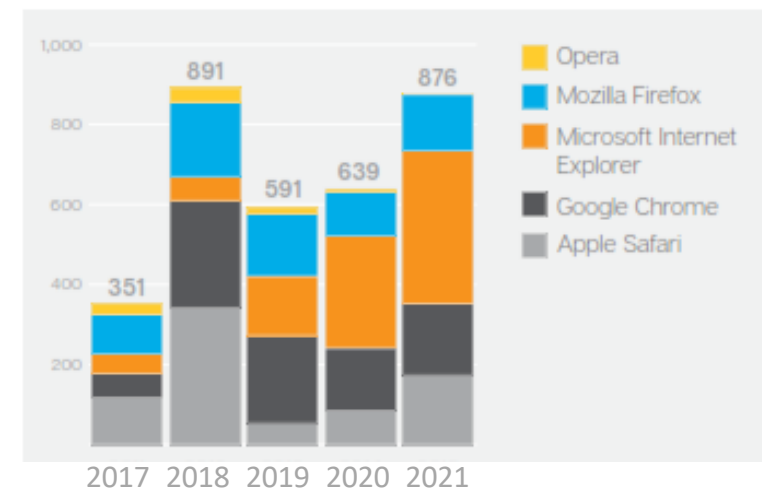
Amenazas en la web

Si el servidor web es vulnerable, también lo son los sitios web que alojan y las personas que los visitan. Los atacantes están aprovechando cualquier vulnerabilidad que puedan para comprometer los sitios web y sus servidores host.

La facilidad de uso y la amplia disponibilidad de ataques web, se duplicó en 2021



Browser Vulnerabilities



Mitos de Seguridad

- ☐ 100% de seguridad en el sistema.
- ☐ Mi red no es atractiva.
- ☐ Mi clave de acceso es obvia nadie la adivinara.
- ☐ Linux es mas seguro que Windows.
- ☐ Mi mail server tiene antivirus mi estación no lo necesita.

Valor de la Información

- ☐ El principal bien de las empresas es la información
- ☐ La clasificación de esta define el diseño del sistema de seguridad al poner en orden las prioridades de los bienes a proteger
- ☐ El camino que recorre la información también de ser protegido
- ☐ Determinar el nivel de inversión sobre cada parte del sistema esta en relación a las prioridades de la organización

Clasificación de la información

Según Krutz y Vines

- ☐ Publica
- ☐ Sensible
- ☐ Privada
- ☐ confidencial

Org. Gubernamentales

- ☐ No clasificada
- ☐ Sensitiva pero no clasificada
- ☐ Confidencial
- ☐ Secreta
- ☐ Top secret

Criterio de Clasificación

Existen infinidad de clasificaciones una mas compleja que otra para efectos prácticos, el valor de la información se puede clasificar así :

- ☐ Valor
- ☐ Antigüedad
- ☐ Vida útil
- ☐ Asociación personal

Amenazas vulnerabilidades y Riesgos

- El nivel de riesgo mide el grado de seguridad de una organización basado en las vulnerabilidades, el valor de la información y la probabilidad de ser atacados.

$$R = V \times A \times VI$$

- R = Riesgo
- V = Vulnerabilidad
- A = Amenaza
- VI = Valor de la información

$$ALE = VI \times EF \times ARO$$

- ALE = Perdida anual esperada
- VI = Valor de la información
- ARO = Razón de ocurrencia anual
- EF = Factor de exposición

La ecuación mencionada muestra que el riesgo tiene una relación directa con la amenaza y la vulnerabilidades

Disminuyendo el Riesgo

Las vulnerabilidades se anulan efectuando:

- ☐ Aplicación de parches
- ☐ Ejecución de checklists y workarounds
- ☐ Definición y aplicación de procedimientos, entrenamiento, etc.

Seguridad Informática

- *Esta disciplina se encargaría de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que articulados con prácticas de gobierno de tecnología de información establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo.*



Seguridad de la información

- *Es la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que nos exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información*



Seguridad de la información vs Seguridad Informatica



IT Security vs Information Security

Compromisos de la Organizaciones con la Seguridad

La seguridad involucra a cada miembro de la organización y debe consistir en:

- ▣ Definición de procedimientos (y cumplirlos).
- ▣ Entrenamiento.
- ▣ Charlas y seminarios.
- ▣ No solicitar privilegios que podrían poner en riesgo la organización.

Seguridad Física

- ☐ La protección lógica de los sistemas es insuficiente por lo que se considera la parte física que toma en cuenta las siguientes situaciones: pérdida de energía eléctrica, accesos irrestricto a los servidores, incendios, etc.

De esta manera la seguridad Física recomienda establecer:

- ☐ Un acondicionamiento físico.
- ☐ Procedimientos administrativos.
- ☐ Seguridad de los sistemas móviles.
- ☐ Seguridad del personal.

¿QUÉ HEMOS APRENDIDO?



Gracias





SEGURIDAD Y AUDITORIA DE SISTEMAS

MG. HANS QUISPE ARCOS
HANS.QUISPE@UNICA.EDU.PE

ETHICAL HACKING



Ethical Hacking



El ethical hacking, también conocido como prueba de penetración o piratería de sombrero blanco, involucra las mismas herramientas, trucos y técnicas que usan los piratas informáticos, pero con la gran diferencia de que la piratería ética es legal.

Ethical Hacking

- ❑ Es un profesional de seguridad informática independiente irrumpiendo en los sistemas informáticos.
- ❑ No daña los sistemas de destino, no roba información.
- ❑ Evalúa la seguridad de los sistemas de destino e informa a los propietarios sobre los errores encontrados.

¿Quiénes son los hackers?

- ☐ Una persona que disfruta aprendiendo detalles de un lenguaje o sistema de programación.
- ☐ Una persona que disfruta haciendo la programación en lugar de solo teorizar sobre ella.
- ☐ Una persona capaz de apreciar la piratería de otra persona
- ☐ Una persona que capta la programación rápidamente.
- ☐ Una persona que es un experto en un lenguaje o sistema de programación en particular.

Fases del Hacking ético

☐ Reconocimiento

Pasivo

☐ Escaneo

Activo

☐ Obteniendo Acceso

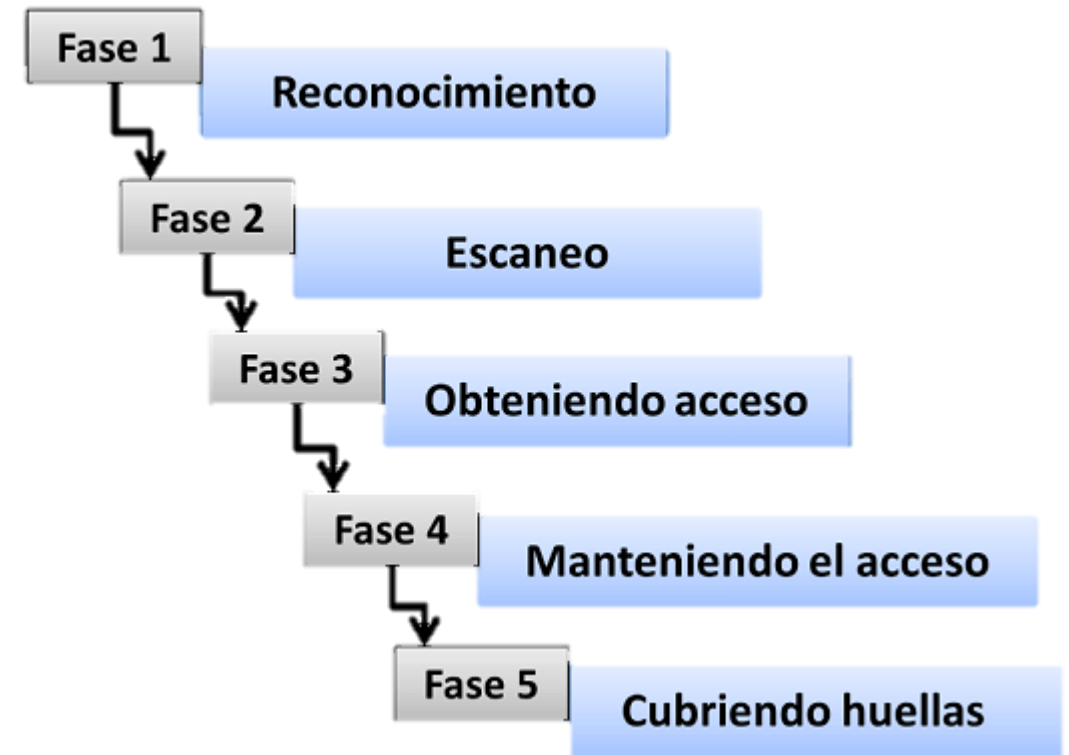
Sistema operativo / aplicación

Redes

Denegación de servicio

☐ Manteniendo el acceso

☐ Cubriendo huellas



Tipos de hacker



Tipos de hacker

Black Hat: También llamados crackers. Utilizan sus habilidades y conocimientos en hacking con fines ilegales, como robos informáticos, fraude, extorsión, destrucción de datos y una amplia gama de tipos de afectación. Los sombreros negros realizan estas acciones sin consentimiento ni permiso que son necesarios para cualquier prueba de seguridad.



Tipos de hacker



White Hat: Se trata de los profesionales en el hacking ético que realizan sus actividades bajo contratos legales y utilizar sus conocimientos o técnicas de ataques solo con fines de mejora de la seguridad. Los sombreros blancos son altamente reconocidos y aceptados dada la ética con la que ejecutan sus investigaciones de seguridad

Tipos de hacker

Gray Hat: Este grupo se mantiene en un limbo o zona difusa entre los 2 grupos anteriores. Los sombreros grises ejecutan sus ataques con o sin consentimiento, sin intención de dañar, sino de hacer notar la necesidad de que hay puntos débiles en una organización.



Tipos de hacker

Otras vertientes de clasificación

□ Ethical (Hackers):

Profesionales éticos en las pruebas de intrusión que trabajan de forma legal

□ Cibercriminales:

Criminales informáticos que ejecutan ataques para su propio beneficio ilícito.

Cabe resaltar que realizar un ataque no contratado legalmente, pero con toda la buena intención podría servir para que la empresa victima te contrate, aunque también podría ocasionar que vayas a la cárcel.



Otros perfiles de atacantes

Hacktivista: Personas que ejecutan ataques con la intención de reivindicar alguna posición política, religiosa o de otra índole. Suelen exponer datos, modificar sitios web y ejecutar otro tipo de ataques contra la entidad contra la que protestan.

Script Kiddie: Personas no calificadas y con conocimientos insuficientes en el funcionamiento de la tecnología como para poder realizar un ataque bien hecho y estructurado.



Otros perfiles de atacantes

State sponsored Hacker: Los gobiernos o estados cuentan con una gran cantidad de dinero y contratan a personas con altos conocimientos en hacking para acciones defensivas u ofensivas contra organizaciones conflictivas, otros estados o naciones o para cumplir algún otro objetivo geopolítico.



Ciberterroristas: Terroristas que utilizan técnicas de ataque informático para atacar infraestructuras críticas gubernamentales, empresas o a las personas a gran escala para lograr sus objetivos antisistema

Motivaciones

- ☐ Diversión
- ☐ Curiosidad
- ☐ Para probar sus habilidades
- ☐ Por pago
- ☐ Venganza
- ☐ Destrucción
- ☐ Encargo de gobiernos



¿QUÉ HEMOS APRENDIDO?



Gracias





SEGURIDAD Y AUDITORIA DE SISTEMAS

MG. HANS QUISPE ARCOS
HANS.QUISPE@UNICA.EDU.PE



<https://youtu.be/0qR94nV4mn4>

TRANSFORMACIÓN DIGITAL



ELEMENTOS DE SEGURIDAD

La seguridad se define como una estrategia a seguir para proteger un bien.

Esta estrategia debe basarse en elementos que puedan guiar nuestro diseño y adaptarlo a las necesidades de la organización.



Los Pilares de la Seguridad

La seguridad es el conjunto de métodos, procedimientos y esquemas que definen una estrategia para proteger la información basada en tres pilares.

- ❑ Confidencialidad
- ❑ Integridad
- ❑ Disponibilidad

Importante: Los pilares de la seguridad definen la estrategia a seguir en el diseño e implementación de un sistema de seguridad.

Relaciones de Confianza

Las relaciones de confianza establecen los permisos y accesos de los usuarios y servicios a recursos o a otros servicios, además de la verificación de autenticidad de las transacciones.

□ Lo complementan:



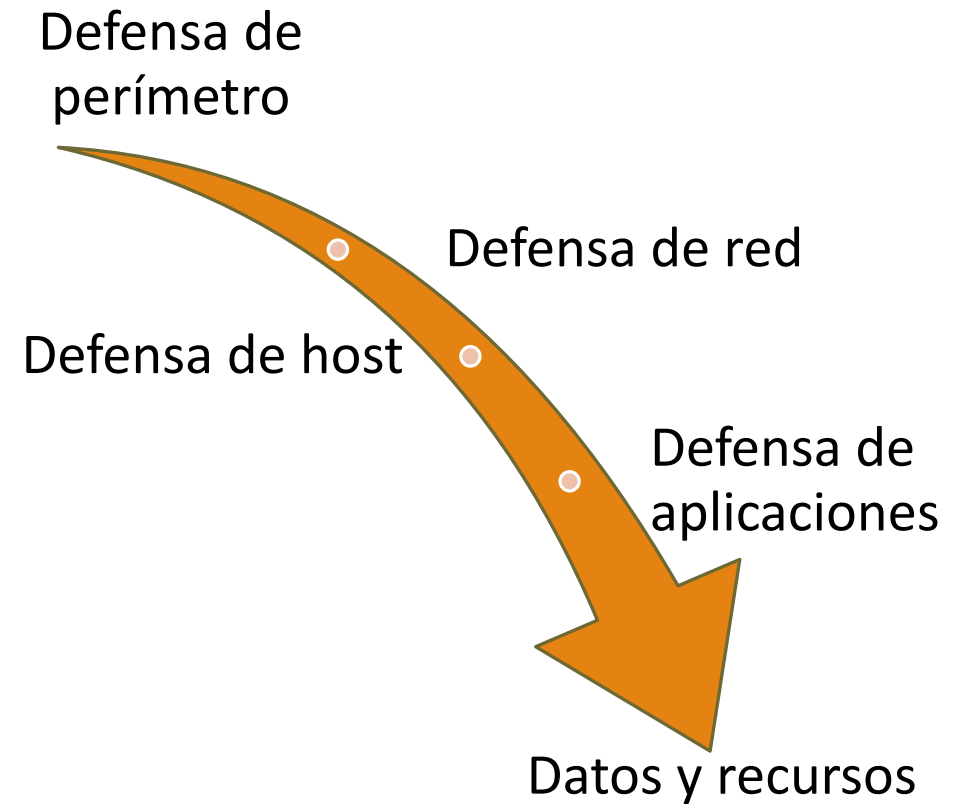
Autenticación



No repudiación

Estrategia de Seguridad Multicapa

- Las estrategias de seguridad mas eficiente es establecer un sistema por capas tal como se muestra en la figura empezando por los primeros niveles de accesos hasta los datos mismos.



Asume que capas previas fallan

Proceso de Seguridad

Ataques y Contra Medidas

Define la aplicación de los conceptos de seguridad, este ítem se enfoca completamente en la parte de análisis de riesgo.

Ataques y contra medidas

- Script kiddies
- Hackers medium
- Hackers

Proceso de Seguridad

Escenarios Típicos de Ataque

Tipos de ataque

- Los ataques son amenazas que se materializan y generan perdidas en los sistemas que eligen como objetivo.

Código hostil

- Referido a programas explícitamente creados para causar un daño severo en los sistemas objetivo dentro de los cuales tenemos

Proceso de Seguridad

Escenarios Típicos de Ataque

- ☐ Fuerza bruta
- ☐ Denial of service
- ☐ Spoofing
- ☐ Man in the middle
- ☐ Spamming
- ☐ Sniffers
- ☐ Keyloggers
- ☐ Ingeniería social
- ☐ Virus
- ☐ Gusanos
- ☐ Troyanos
- ☐ Spyware
- ☐ Malware
- ☐ Phishing
- ☐ Ransomware

Proceso de Seguridad

Escenarios Típicos de Ataque

- ❑ Errores de código
- ❑ La premura del desarrollo de programas y aplicaciones dentro de cada una de sus fases generan que muchos de los aspectos de seguridad no sean analizados a profundidad y por tanto no considerados en el diseño general

Por ejemplo algunos comandos del lenguaje C son susceptibles a ataques de Buffer overflow como son

Strcpy, wcsncpy, lstrcpy, and _mbstrcpy, strcat, wscat, lstrcat, _tcscat, and _mbscat estas funciones no chequean el tamaño del buffer destino y tampoco si hay punteros nulos o invalidos

Strncpy, wcsncpy, _tcscat, ltrcpyn, and _mbsnbcpy no esta garantizado que estas funciones terminen en valor nulo en el buffer destino

Ejemplo Buffer Overflow

```
#include <stdio.h>

#include <string.h>
```

Errado

```
int main(int argc, char *argv[])
{
    char buffer[10];
    if (argc < 2)
    {
        fprintf(stderr, "MODULO DE USO: %s string\n", argv[0]);
        return 1;
    }
    strcpy(buffer, argv[1]);
    return 0;
}
```

```
#include <stdio.h>

#include <string.h>
```

Corregido

```
int main(int argc, char *argv[])
{
    char buffer[10];
    if (argc < 2)
    {
        fprintf(stderr, "MODULO DE USO: %s string\n", argv[0]);
        return 1;
    }
    strcpy(buffer, argv[1]);
    buffer[sizeof(buffer) - 1] = '\0';
    return 0;
}
```

Proceso de Seguridad

Análisis de Riesgo

FASE	PROCESOS
Identificar el conocimiento (IC) de la empresa	IC De la empresa IC Del área operacional IC Del personal Establecer los requerimientos de seguridad
Identificar vulnerabilidades de la infraestructura	Mapeo de bienes de Inf. De alta prioridad e infraestructura de inf. Ejercitar la evaluación de vulnerabilidad de la infraestructura
Determinar las estrategias de administración de riesgos	Conducir un análisis de riesgo multidimensional Desarrollar estrategias de protección

Proceso de Seguridad

Análisis de Riesgo

Fase I: Identificar el conocimiento de la empresa

Recopila toda la información disponible acerca del sistema: valor de la inf. Amenazas, vulnerabilidades, procedimientos, diagramas de red de flujo etc, esta fase tiene 4 procesos por medio de los cuales el CISO debe obtener la información necesaria en todos los niveles jerárquicos.

Proceso de Seguridad

Análisis de Riesgo

Fase I: Identificar el conocimiento de la empresa

Los procesos son

- ▣ Identificar el conocimiento de la empresa.
- ▣ Identificar el conocimiento del área operacional.
- ▣ Identificar el conocimiento del personal.
- ▣ Establecer requerimiento de seguridad.

Proceso de Seguridad

Análisis de Riesgo

Fase II: Identificar vulnerabilidades de la infraestructura

Basado en la información de la primera fase, aquí se identifican los componentes de alta prioridad y sus vulnerabilidades.

- ❖ Mapeo de bienes de información de alta prioridad a infraestructura de información
Este combina la información de bienes y amenazas de la fase I con el conocimiento del personal acerca de la infraestructura de la inf. Para establecer ubicación de bienes , trayectos de accesos y flujos de datos para identificar los bienes de alta prioridad.
- ❖ Ejecutar la evaluación de vulnerabilidades de la infraestructura
Identifica la políticas y practicas ausentes así como las vulnerabilidades de infraestructura usando los requerimientos y conocimiento de los bienes amenazas riesgos de la fase I.

Proceso de Seguridad

Análisis de Riesgo

Fase III: Determinar estrategias de administración de riesgos

Basado en la información obtenida de las fases anteriores, son estimados el impacto y probabilidad de los riesgos y utilizados para ayudar a priorizar los riesgos en adición a esto es desarrollada e implementada una estrategia de protección en la empresa.

- ❖ Conducir un análisis de riesgo multidimensional

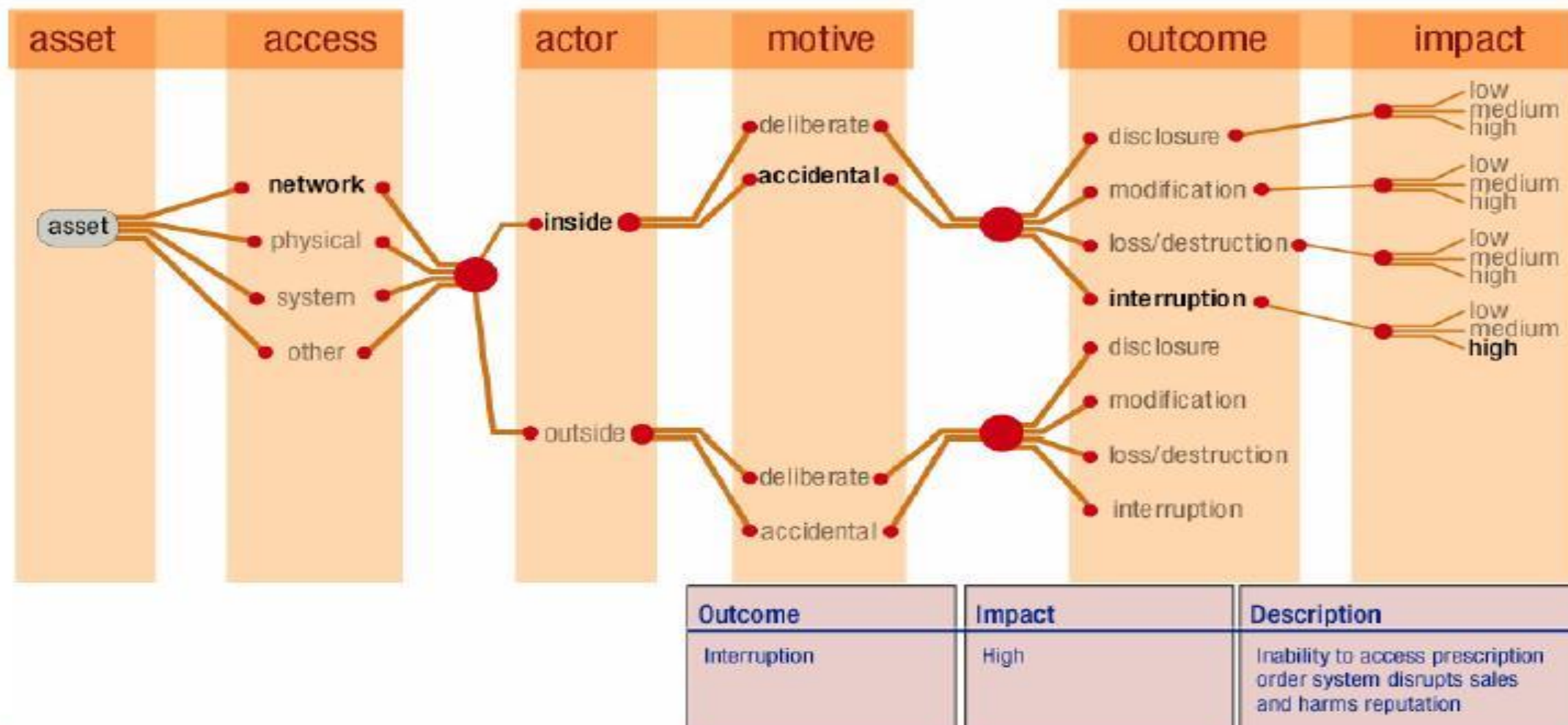
El objetivo es generar una lista priorizada de riesgos basada en el impacto de probabilidad

- ❖ Desarrollar estrategias de protección

El objetivo es desarrollar la estrategia para reducir los riesgos y un plan de administración de riesgos para manejarlos en una forma continua.

PERFIL DE RIESGO

Asset-Based Risk Profile



¿QUÉ HEMOS APRENDIDO?



Gracias





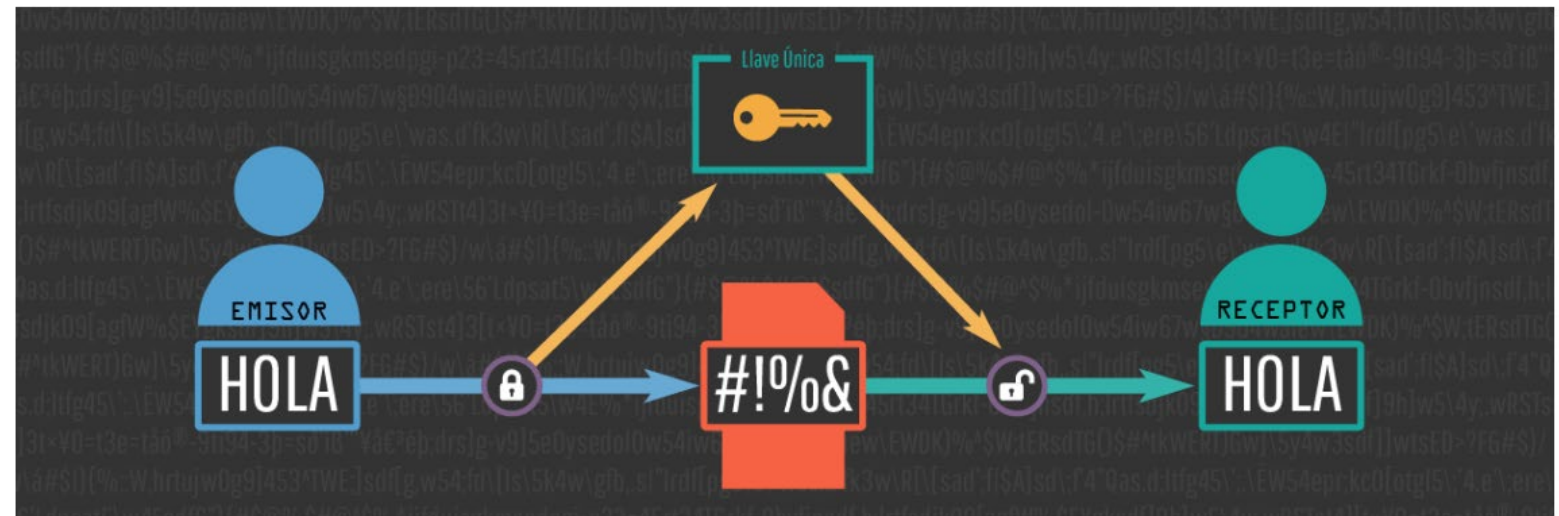
SEGURIDAD Y AUDITORIA DE SISTEMAS

MG. HANS QUISPE ARCOS
HANS.QUISPE@UNICA.EDU.PE



<https://youtu.be/Q8K311s7EiM>

Criptografía



Criptografía

Criptografía y seguridad informática son dos elementos que crean una llave perfecta que abre tus entornos digitales. si bien cada elemento surgió y evolucionó de manera autónoma para ganar por mérito propio su correspondiente sitio de honor; criptografía y seguridad informática se combinan para garantizar el acceso exclusivo únicamente a quienes autorices.

Aunque la criptografía acumula miles de años de historia; comenzó con el sencillo deseo de ocultar o restringir a unos pocos los mensajes importantes.

Criptografía



Principales amenazas en internet

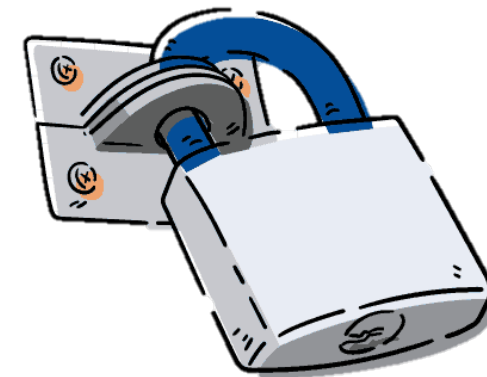
- Anexos a mensajes enviados por correo electrónico infectados con virus.
- El intercambio de códigos de virus.
- Firewalls o cortafuegos mal configurados.
- Ataques a la disponibilidad de los recursos de información existentes en la red (bancos de datos o software disponibles para descargar por los usuarios).
- La alteración de las páginas web.

Principales amenazas en internet

- El "repudio" y las estafas asociadas al comercio electrónico.
- Las vulnerabilidades de los sistemas operativos y la desactualización de los "parches" concernientes a su seguridad.
- La rotura de contraseñas.
- La suplantación de identidades.
- El acceso a páginas terroristas, etc.

Uso de la criptografía

En sí, la criptografía es un arte de técnica compleja empleado para la protección u ocultamiento de información. en la época moderna y específicamente durante el siglo pasado; se empleaba exclusivamente para proteger datos y documentos de origen con información militar o asuntos políticos.

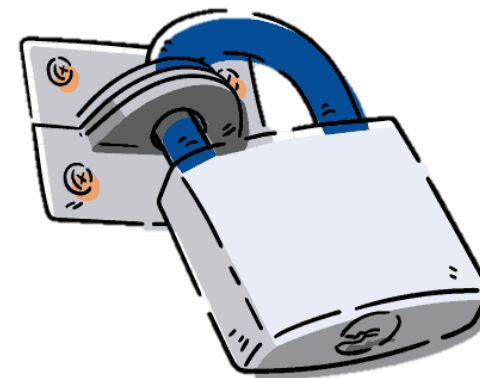


Sin embargo, con la llegada y masificación del internet, la criptografía y seguridad informática evolucionaron conjuntamente y de manera natural hacia la empresa privada. y de ahí, a los individuos.

Por esta razón, criptografía y seguridad informática en nuestra época se traducen en diversos tipos y presentaciones que conviene conocer bien.

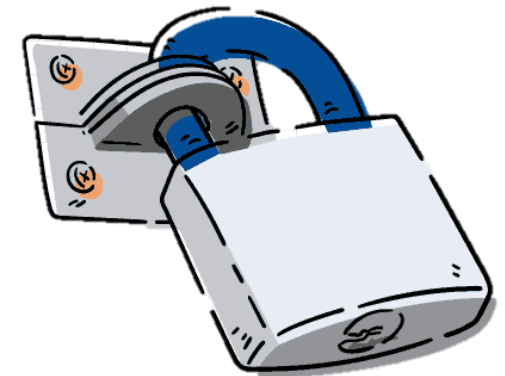
Sistemas criptográficos

En la actualidad, los sistemas criptográficos se dividen en dos campos de estudio principales: criptografía simétrica y asimétrica. mientras la encriptación simétrica se emplea a menudo como sinónimo de criptografía simétrica, la criptografía asimétrica abraza dos usos primarios: encriptación asimétrica y firmas digitales



Encriptación simétrica vs Asimétrica

Los algoritmos de encriptación o cifrado a menudo se dividen en dos categorías: encriptación simétrica y asimétrica. la diferencia fundamental entre estos dos métodos de encriptación radica en el hecho de que los algoritmos de cifrado simétricos emplean una única clave, mientras que los asimétricos utilizan dos claves distintas pero vinculadas. dicha distinción, a pesar de ser simple en apariencia, explica las diferencias funcionales entre los dos tipos de técnicas de encriptación y la forma en que son empleadas



Ejemplo

Por ejemplo, si Clara le envía a Juan un mensaje protegido por encriptación simétrica, deberá compartir también la clave empleada para el cifrado, para que éste pueda desencriptarlo y leerlo. esto significa que si un actor malicioso intercepta la clave será capaz de acceder a la información encriptada.

En cambio, si Clara decide emplear un esquema asimétrico, encriptará el mensaje con la

“clave pública” de Juan para que éste pueda desencriptarlo con su propia “clave privada”.

como se deduce, la encriptación asimétrica ofrece un nivel de seguridad más elevado porque, incluso en el caso de que alguien intercepte y encuentre la clave pública de Juan, no podrá desencriptar el mensaje.

¿QUÉ HEMOS APRENDIDO?



Gracias

