

Alex Tovar G

Introducción a la Seguridad Informática



alextovar

Introducción a la Seguridad Informática

Alex Tovar G.

Ing. de Sistemas

Esp. en Auditoría de Sistemas

COBIT - ITIL - CEH

2018. Esto es lo que ocurre cada minuto en Internet



Creado originalmente por:
@LoriLewis
@OfficiallyChadd

1. Objetivos de la Seguridad Informática

- Proteger la infraestructura tecnológica
- Proteger la información

Elementos de un Sistema Informático

INFORMACIÓN

USUARIOS

**TECNOLOGÍAS DE
INFORMACIÓN**

**INFRAESTRUCTURA
FÍSICA**

Principios Fundamentales



Términos de Seguridad

Activo

Es cualquier dato, dispositivo u otro componente del entorno que apoya actividades relacionadas con la información.



Amenaza

Circunstancia que tiene el potencial de causar daños o pérdidas.



Términos de Seguridad

Ataque

Acción organizada con intención de causar daños o problemas a un sistema informático o red.



Control

Acción que se implementa para evitar la materialización de un riesgo



Términos de Seguridad

Impacto

Efecto económico, operativo o reputacional causado por la materialización del riesgo



Riesgo

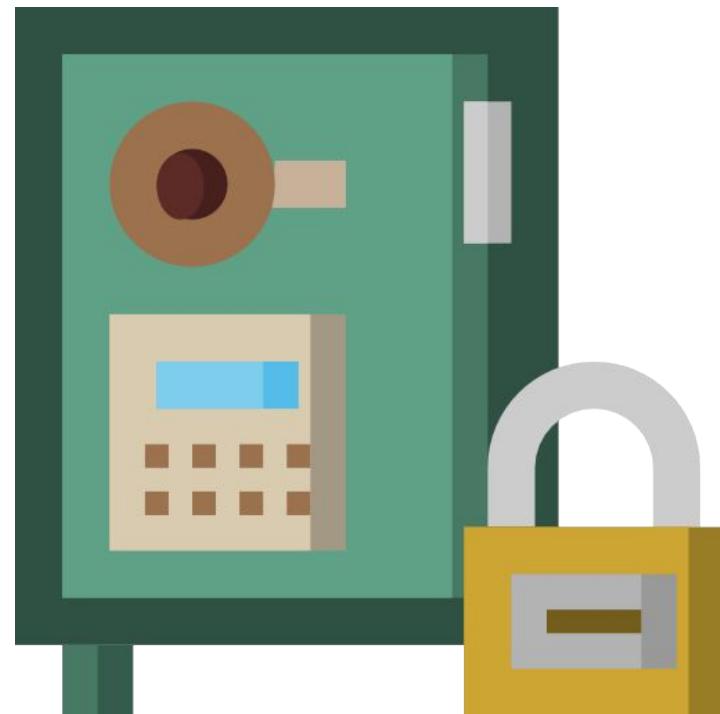
“Evento o condición incierta que, si se produce, tiene un efecto positivo o negativo en los objetivos de un proyecto”, *PMBOK Guide*.



Términos de Seguridad

Vulnerabilidad

Debilidad del sistema informático que puede ser utilizada para causar daño.



Principios básicos en la Seguridad Informática

- Mínimo privilegio
- Eslabón más débil
- Proporcionalidad
- Dinamismo
- Participación Universal

Mínimo privilegio

Se deben otorgar los permisos estrictamente necesarios para efectuar las acciones que se requieran, ni más ni menos de lo solicitado.



“

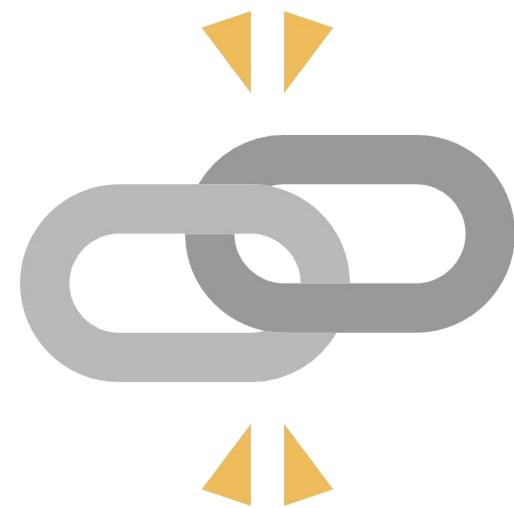
*Lo que no está permitido,
debe estar prohibido.*

”

Eslabón más débil

La seguridad de un sistema es tan fuerte como su parte más débil.

Un atacante primero analiza cuál es el punto más débil del sistema y concentra sus esfuerzos en ese lugar.



IN THIS CORNER, WE HAVE
FIREWALLS, ENCRYPTION,
ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER,
WE HAVE DAVE!!



Proporcionalidad

Las medidas de seguridad estarán en correspondencia con la importancia de lo que se protege y con el nivel de riesgo existente.



Dinamismo

La seguridad informática no es un producto, es un proceso. No se termina con la implementación de los medios tecnológicos, se requiere permanentemente monitoreo y mantenimiento.



Participación universal

Es necesario contar con una participación activa de los colaboradores internos para apoyar el sistema de seguridad establecido.



Laboratorios

- Montaje y configuración de una Máquina Virtual
- Creación de usuarios en Windows y Linux aplicando el principio del menor privilegio

Reto

Crear los siguientes usuarios:

USUARIO	PERMISOS	S.O
Pedro.perez	Administrador	Windows
Ana.rojas	Invitado	Windows
CarlosTorres	Root	Linux
MariaRamírez	Normales	Linux

3. Seguridad en Redes TCP/IP

Protocolos TCP/IP

- Desarrollados a mediados de la década de los 70 como parte del proyecto DARPA
- Objetivo: interconectar redes
- Existen 2 grupos:
 - Control de transmisión
 - Internet

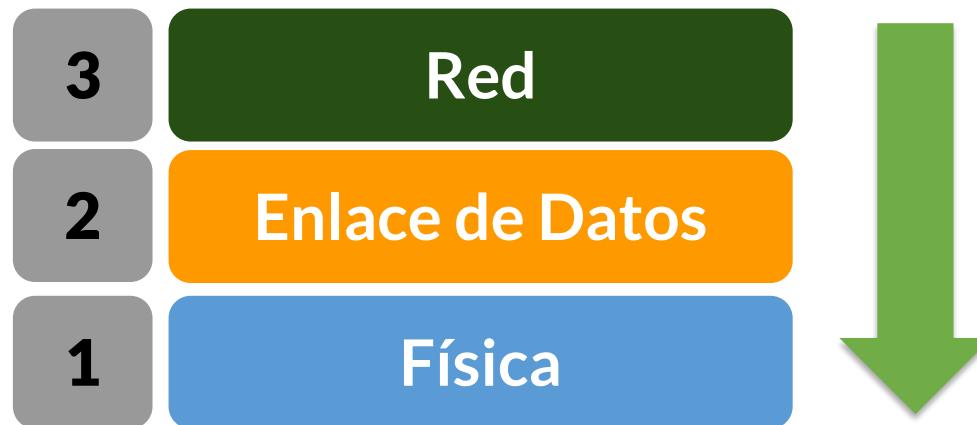
Modelo OSI



MODELO OSI

7	Aplicación	<i>Aplicaciones, Http, FTP, SSH, SMTP, POP3</i>
6	Presentación	<i>Estandariza la forma en que se presentan los datos</i>
5	Sesión	<i>Establecer, administrar y terminar sesiones entre Host</i>
4	Transporte	<i>TCP-UDP</i>
3	Red	<i>Direccionamiento IP, Enrutamiento</i>
2	Enlace de Datos	<i>Switches, Bridge, MAC Address</i>
1	Física	<i>Medios de transmisión: Cables, Radiofrecuencias, F.O, AP, Hubs</i>

Seguridad por debajo de la Capa 3



Capa Física

- **Mecánicos**
 - Medio de transmisión
 - Canal de comunicaciones empleado
- **Eléctricos**
 - Potencia
 - Rango de frecuencias

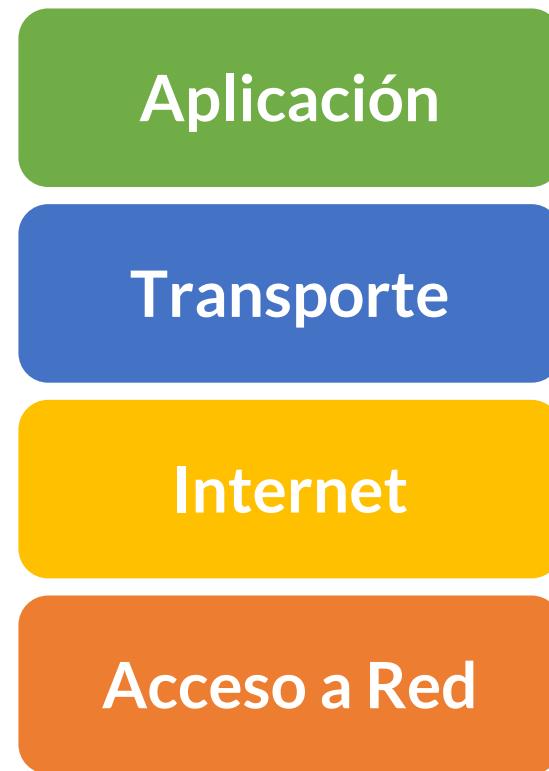
Capa de Enlace

- Control de direcciones de Hardware
- Auditoría de configuración de Bridge o Switch
- Análisis de tráfico y colisiones
- Detección de Sniffers
- Evaluación de puntos de acceso WiFi
- Evaluación de dispositivos Bluetooth

Capa de Red

- Auditorías en Router
- Auditorías de tráfico ICMP
- Auditoría ARP
- Auditoría de
direcccionamiento IP

Modelo TCP/IP



MODELO TCP/IP

Aplicación

incorpora aplicaciones de red estándar (Telnet, SMTP, FTP, etc.).

Transporte

Direccionamiento y mejor ruta

Internet

Entregar paquete de datos

Acceso a Red

Establecer las reglas de envío

COMPARACIÓN ENTRE MODELOS

Modelo OSI



Modelo TCP/IP



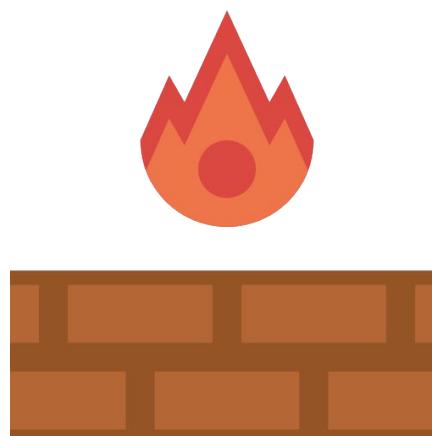
Laboratorios

- Realizar un escaneo de puertos
- Realizar análisis de protocolos con la herramienta Wireshark

Dispositivos de Seguridad Informática

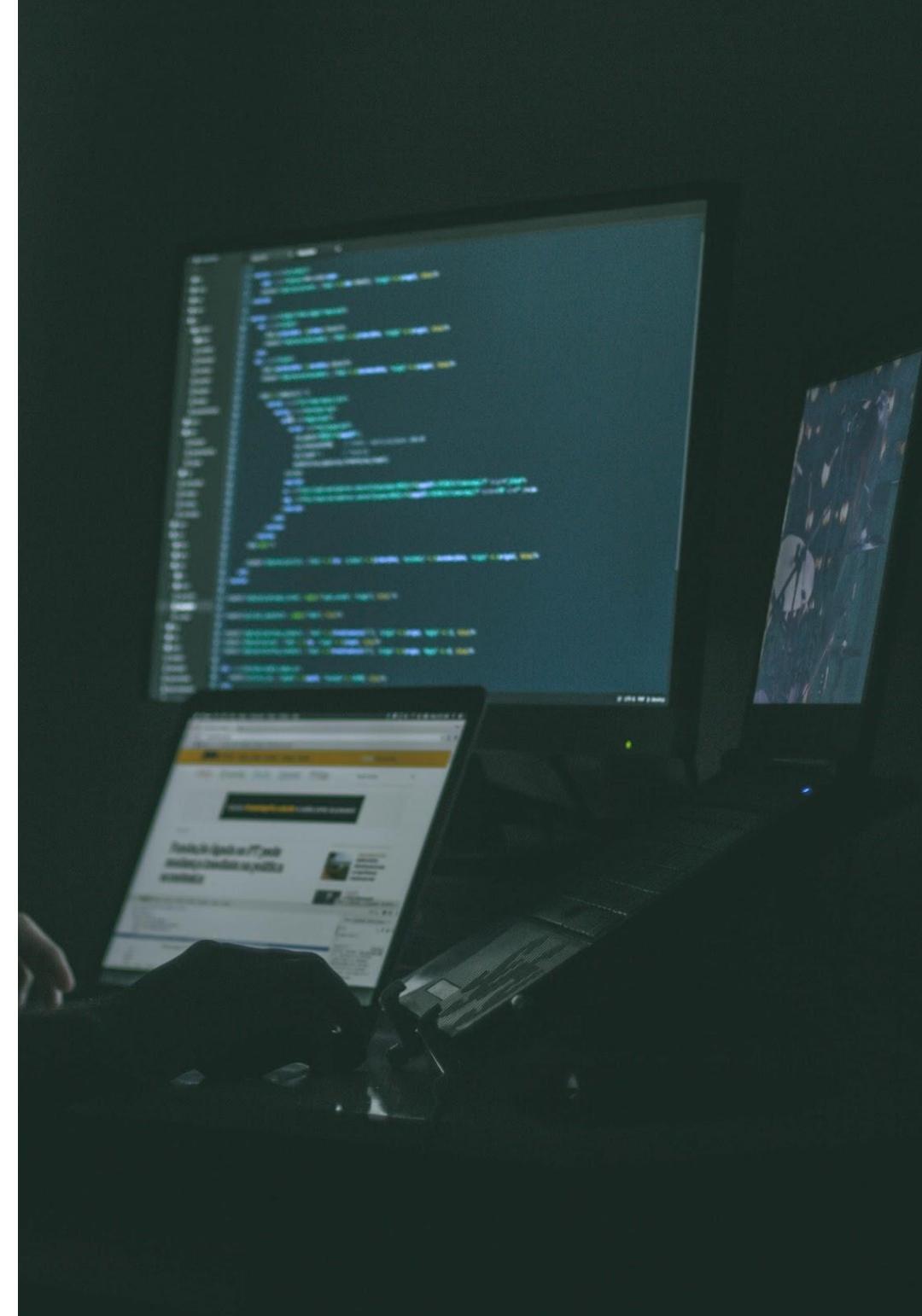
Firewall

Dispositivo de seguridad que monitorea el tráfico de red y decide si permite o bloquea tráfico específico en función de un conjunto de reglas.



Tipos de Firewall

- Software
- Hardware



Honeypot

Sistemas que simulan ser equipos vulnerables y que son perceptibles de ser atacados.



Honeypot

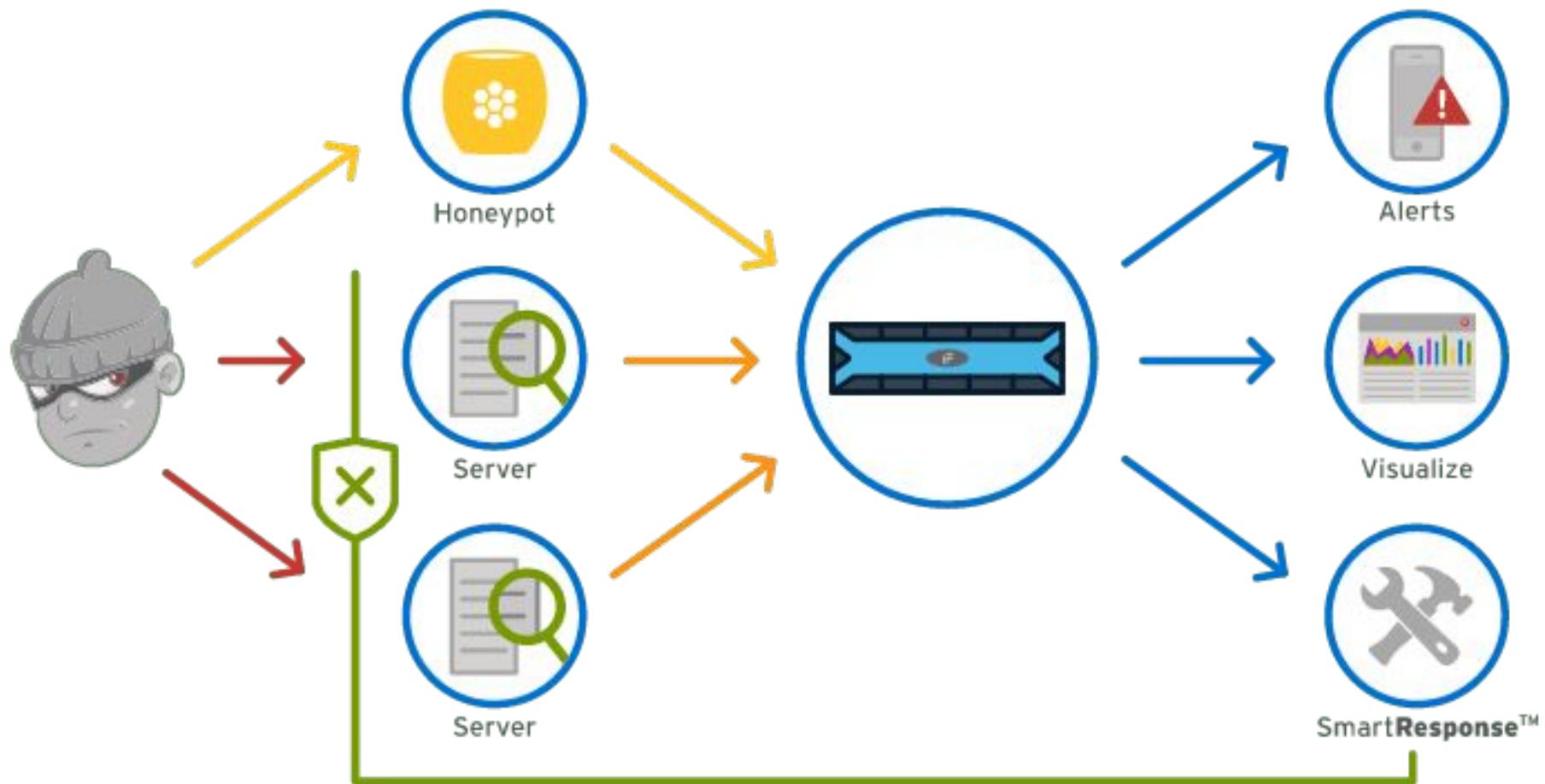
Honeypot



Un equipo informático cualquiera que analice el tráfico entrante y saliente hacia Internet.

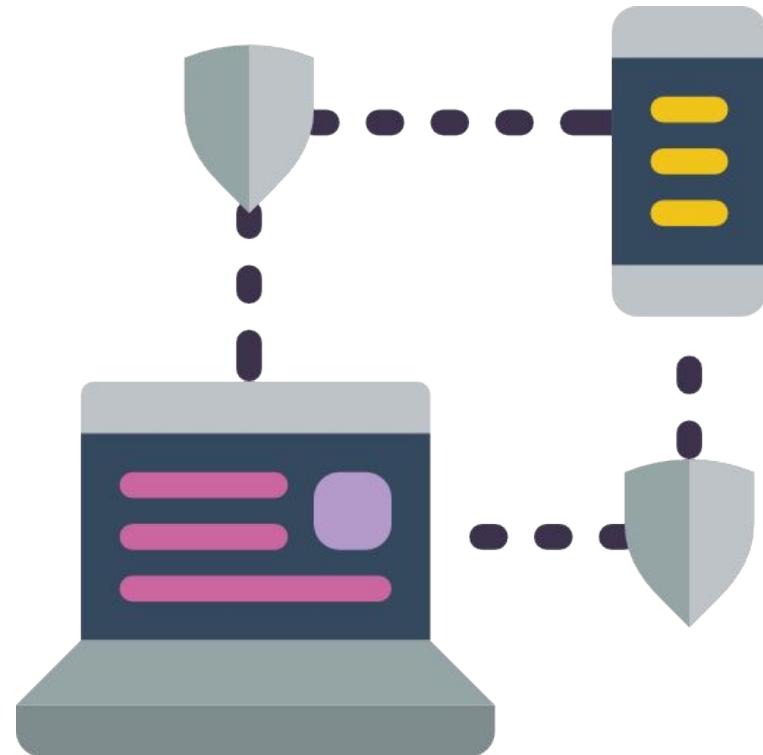


Red de equipos, con diversos sistemas, y servicios, cuando uno de los equipos es atacado inmediatamente es informado el administrador de sistemas.



Antivirus

Es un programa que tiene el propósito de detectar software malicioso que puede perjudicar el sistema de un equipo.



Los antivirus pueden revisar todos los archivos que se encuentran dentro del sistema como aquellos que quieren ingresar o ejercer una interacción con el mismo.



Antispam

Filtra los correos electrónicos y evita que los usuarios estén expuestos a los riesgos asociados con el uso del recurso.



Antispam

Analiza los mensajes mediante la aplicación de una serie de capas de seguridad, reduciendo la recepción de spam en un 99%



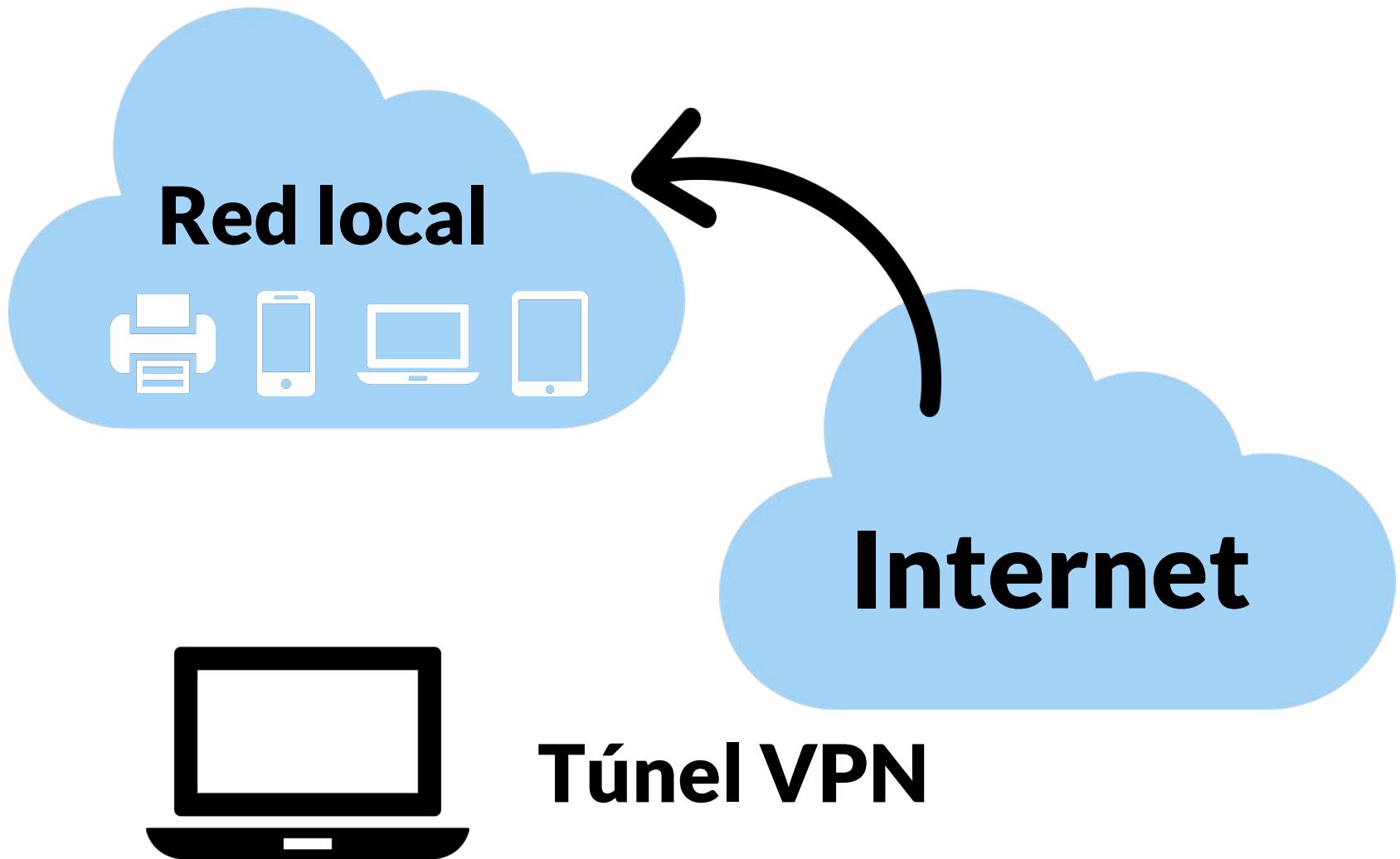
VPN

Las siglas VPN provienen del término en inglés *Virtual Private Network*, lo que en español significa: red virtual privada.



VPN

Al conectarnos a una VPN, lo hacemos utilizando **una especie de túnel**, término que se emplea para indicar que los datos se encuentran cifrados en todo momento, desde que entran hasta que salen de la VPN.



IPS

Las siglas IPS provienen del término en inglés *Intrusion Prevention System* que español significa: sistema de prevención de intrusos.



IPS

Conjunto de acciones predefinidas que tienen como objetivo prevenir actividades sospechosas que provienen tanto de las redes externas/internas como del mismo host de manera proactiva.

Características



La detección de intrusos se realiza comparando las firmas de las actividades sospechosas con las firmas de las actividades ya conocidas y que se incluyen en un fichero de identificadores.



Un sistema IPS debe disponer de un sistema de actualización continuo mediante el cual, el fichero que contiene los identificadores de intrusiones se actualizará en todo momento.

Tipos

Red:

- Proteger segmentos enteros de la red o zonas a las que tienen acceso.
- Capturan paquetes del tráfico de red (sniffers) y los analizan en busca de patrones que puedan suponer algún tipo de ataque.
- Trabajan no solo a nivel TCP/IP, sino que también lo pueden hacer a nivel de aplicación.

Tipos

Host:

- Se limitan a proteger un solo equipo.
- Monitorean gran cantidad de eventos y actividades con una gran precisión.
- Recaban información del sistema como ficheros, logs y recursos para su posterior análisis en busca de posibles incidencias dentro del propio sistema, en modo local.

Laboratorios

- Implementar y configurar el Honeypot: *Dionaea*

5. Hackers y Fases de un Hacking

¿Qué es un Hacker?

Término utilizado para referirse a una persona que posee conocimientos técnicos avanzados y se dedica a acceder a sistemas informáticos.



Hacker

-  Hacker = “*Expertos en seguridad informática*”
-  Cracker = “*Pirata Informático*”

Clases de Hacker

1. Black Hats

Personas con altas habilidades técnicas usadas para actividades maliciosas o destructivas.

Crackers

2. White Hats

Personas con habilidades de hacking usadas para propósitos defensivos

3. Gray Hats

Personas que trabajan en acciones defensivas y ofensivas varias veces.

4. Suicide Hackers

Son aquellos que piratean con algún propósito pero no se preocupan por caer en la cárcel.

Clases de Hacker

5. Script Kiddies

Hacker aficionado sin mucho conocimiento en programación de herramientas.

6. Cyber Terrorist

Hacker que irrumpen en los sistemas informáticos como forma de terrorismo cibernético.

7. Hacktivist

Hacker que piensa que piratear puede provocar algunos cambios sociales y piratea al gobierno y a las organizaciones para mostrar su incomodidad por algunos temas.

¿Qué es Hacking?

Se refiere a explotar las vulnerabilidades del sistema y poner en peligro los controles de seguridad para obtener acceso no autorizado o inapropiado a los recursos del sistema.

¿Qué es Hacking?

Implica modificar las características del sistema o de la aplicación para lograr un objetivo fuera del propósito original de los creadores.



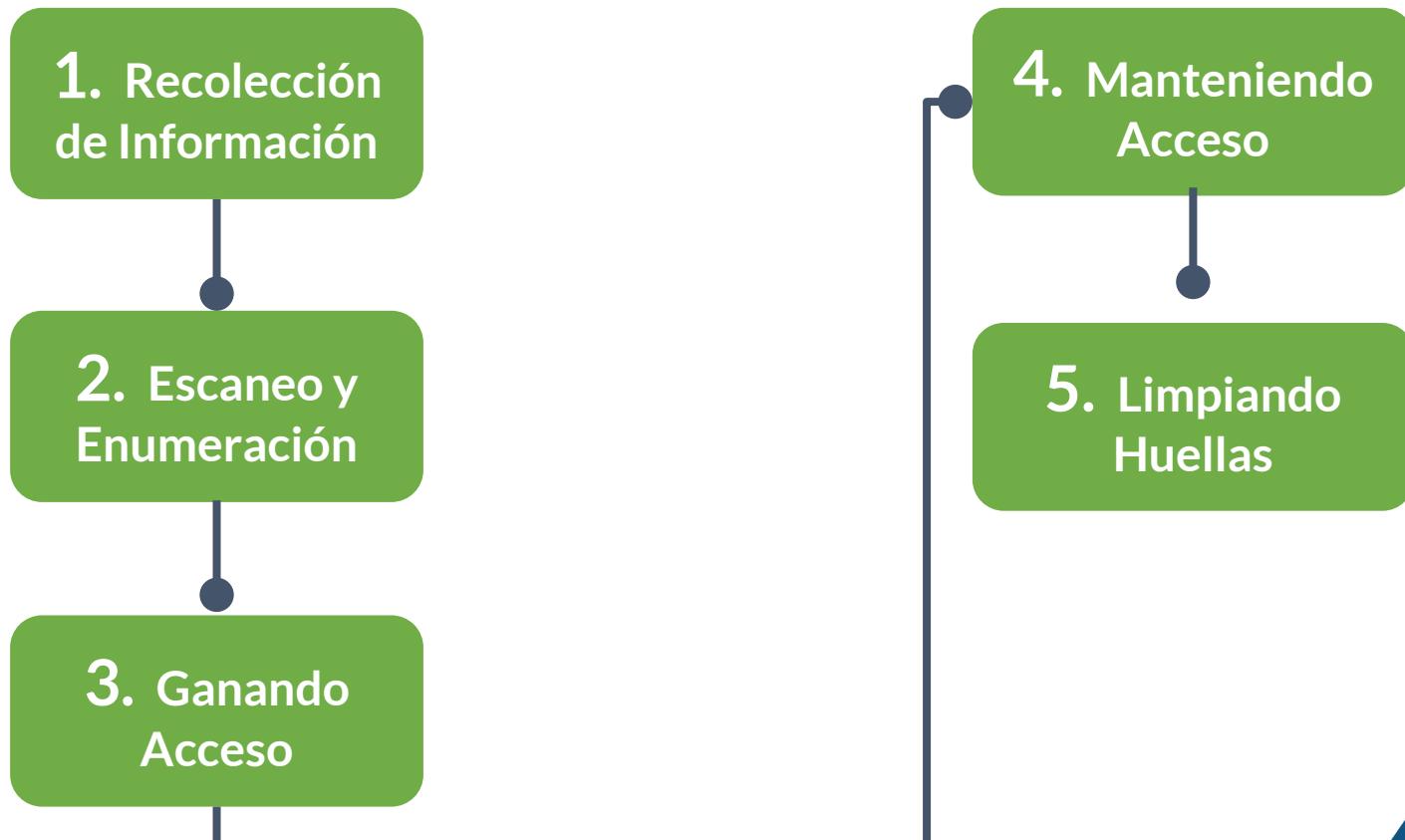
Confidencialidad



Integridad

Disponibilidad

Fases del Hacking



Fases del Hacking

FOOTPRINTING

1. Recolección de información

La fase preparatoria en la que un atacante busca reunir información sobre un objetivo antes de lanzar un ataque

Puede incluir la recolección de información sobre clientes, empleados, operaciones, red y sistemas del objetivo

PASOS

- Encontrar URL's
- Búsqueda de detalles
- Buscar nombres y datos en el sitio
- Extraer archivos del sitio
- Buscar noticias del objetivo
- Buscar datos personales
- Rastreo de e-mails

TIPOS

- Pasivo
- Activo



Fases del Hacking

2. Escaneo y enumeración

ESCANEO

Es la fase del pre-ataque cuando el atacante escanea la red del objetivo basándose en la información recopilada durante el footprinting.

TIPOS

Puertos: Búsqueda de puertos en estado escucha “listener”

Red: Búsqueda de equipos activos

Vulnerabilidades: Debilidades en los sistemas que son susceptibles de ataque.



Fases de un Hacking

ACCESO

3. Ganando Acceso

Se refiere al punto donde el atacante obtiene acceso al sistema operativo o aplicaciones en la computadora o la red.

El atacante puede en el proceso escalar privilegios para obtener un control total del sistema.

NIVELES DE ACCESO

- Aplicación
- Sistema Operativo
- Red

*Password Craking
Buffer Overflows
DNS
Session Hijacking, etc*



Fases del Hacking

MANTENIENDO ACCESO

4. Manteniendo Acceso



- Es la fase en la que el atacante intenta retener su “propiedad” en el sistema
- Los atacantes pueden cargar, descargar o manipular datos, aplicaciones y configuraciones en las propiedades del sistema
- Los atacantes usan el sistema comprometido para lanzar nuevos ataques

Fases de un Hacking

4. Limpiando Huellas



LIMPIANDO HUELLAS

- Las intenciones del atacante incluyen: continuar con el acceso al sistema de la víctima, permanecer desapercibido y no ser detectado, borrar las pruebas que puedan conducir a su enjuiciamiento.
- El atacante sobrescribe los registros del servidor, del sistema o los de la aplicación para evitar sospechas.

Laboratorios

- Utilizando la herramienta FOCA, obtener todos los metadatos posibles de archivos de diversos formatos
- Obtener todos los datos disponibles de algunos sitios web mediante la utilización de herramientas online
- Realizar Email Tracking

6. Manejo de Incidentes de Seguridad

Incidente de Seguridad

“Un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.”



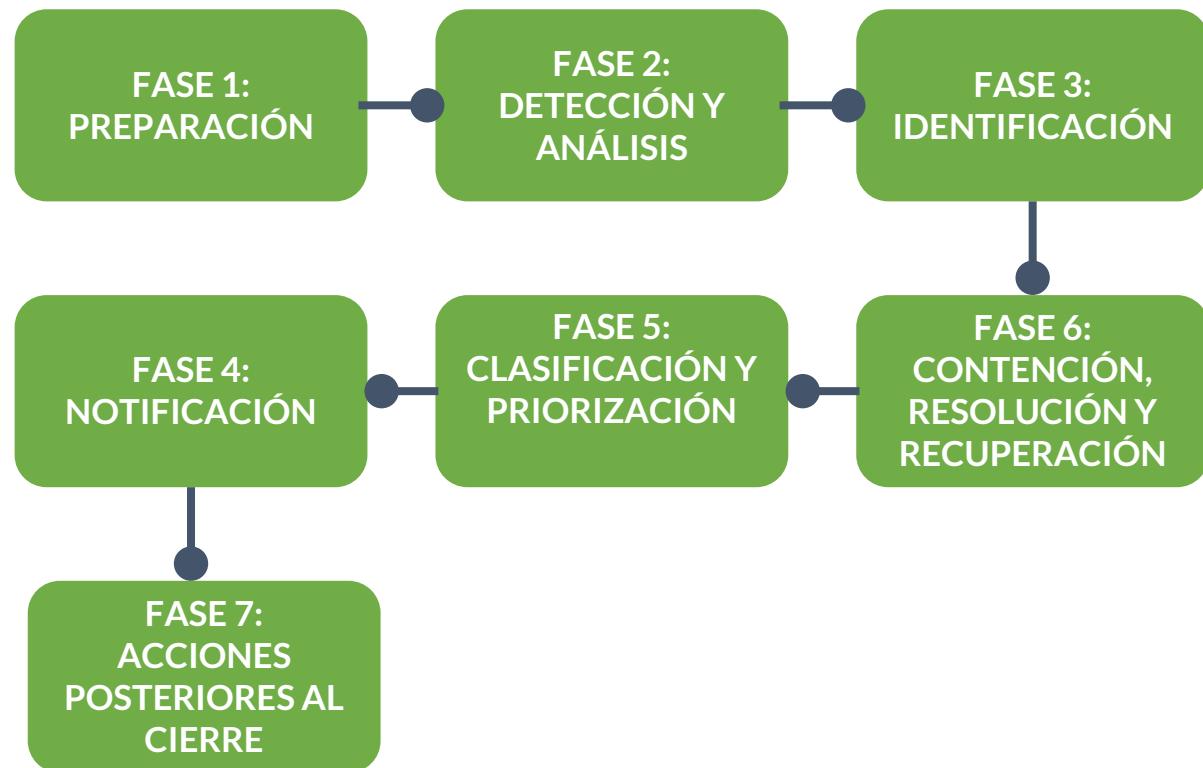
¿Evento de Seguridad?



“Una ocurrencia identificada del estado de un sistema, indicando una posible violación de la política de seguridad de la información, o una situación previamente desconocida que puede ser relevante para la seguridad.”

¿Cómo
responder ante
un incidente de
seguridad?

Administración de Incidentes de Seguridad



FASE 1: PREPARACIÓN

ESTIMAR NECESIDADES

- Colaboradores que va a realizar la gestión de incidentes
- Documentación de los sistemas y redes que se usan en la empresa
- Centros de respuesta ante incidentes de organismos externos en los cuales apoyarnos

ESTABLECER PROCEDIMIENTOS

- Definir una política de gestión de incidentes
- Acciones a seguir en caso de que se presente una ocurrencia.
- Monitoreo y clasificación de las incidencias que tengan mayor probabilidad de ocurrir

FASE 2: DETECCIÓN Y ANÁLISIS

Los signos de detección de un incidente pueden ser:

Indicadores: Son aquellos que ponen de manifiesto que un incidente ha ocurrido o puede estar ocurriendo.

Precursores: Son los que nos pueden indicar que un incidente tiene posibilidades de ocurrir en el futuro

FASE 3: IDENTIFICACIÓN

Identificar el tipo de incidente ocurrido y si ha ocurrido más de uno, priorizarlos dependiendo de su gravedad.

FASE 4: NOTIFICACIÓN

El proceso de notificación de incidentes de seguridad pasa por las siguientes acciones: reportar, notificar y registrar el incidente.

FASE 5: CLASIFICACIÓN Y PRIORIZACIÓN

Una vez detectado un incidente, hay que clasificarlo, utilizando para la clasificación los siguientes atributos:

- Tipo de amenaza
- Origen de la amenaza
- Categoría de seguridad o criticidad de los sistemas afectados
- El perfil de los usuarios afectados
- El número y tipología de los sistemas afectados.

FASE 5: CLASIFICACIÓN Y PRIORIZACIÓN

Ahora es necesario priorizar dependiendo del proceso soportado dentro de la entidad, por ejemplo:

NIVEL DE CRITICIDAD	VALOR	DEFINICIÓN
Inferior	0,10	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas.
Bajo	0,25	Sistemas que apoyan a una sola dependencia o proceso de una entidad.
Medio	0,50	Sistemas que apoyan más de una dependencia o proceso de la entidad.
Alto	0,75	Sistemas pertenecientes al área de tecnología y estaciones de trabajo de usuarios con funciones críticas
Superior	1,00	Sistemas críticos.

FASE 6: CONTENCIÓN, RESOLUCIÓN Y RECUPERACIÓN

Es importante para la entidad implementar una estrategia que permita tomar decisiones oportunamente para evitar la propagación del incidente y así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información.

FASE 6: CONTENCIÓN, RESOLUCIÓN Y RECUPERACIÓN

CONTENCIÓN: Esta actividad busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI

RECUPERACIÓN: El administrador de TI debe restablecer la funcionalidad de los sistemas o servicios afectados.

RESOLUCIÓN: Después de que el incidente ha sido contenido se debe realizar una erradicación y eliminación de cualquier rastro dejado por el incidente como código malicioso

FASE 7: ACCIONES POSTERIORES AL CIERRE

El cierre de un incidente de seguridad y el fin de su gestión debe incluir un conjunto de evidencias que acrediten:

- las acciones que se han realizado
- los procesos que se han ejecutado
- todas las personas que han estado involucradas

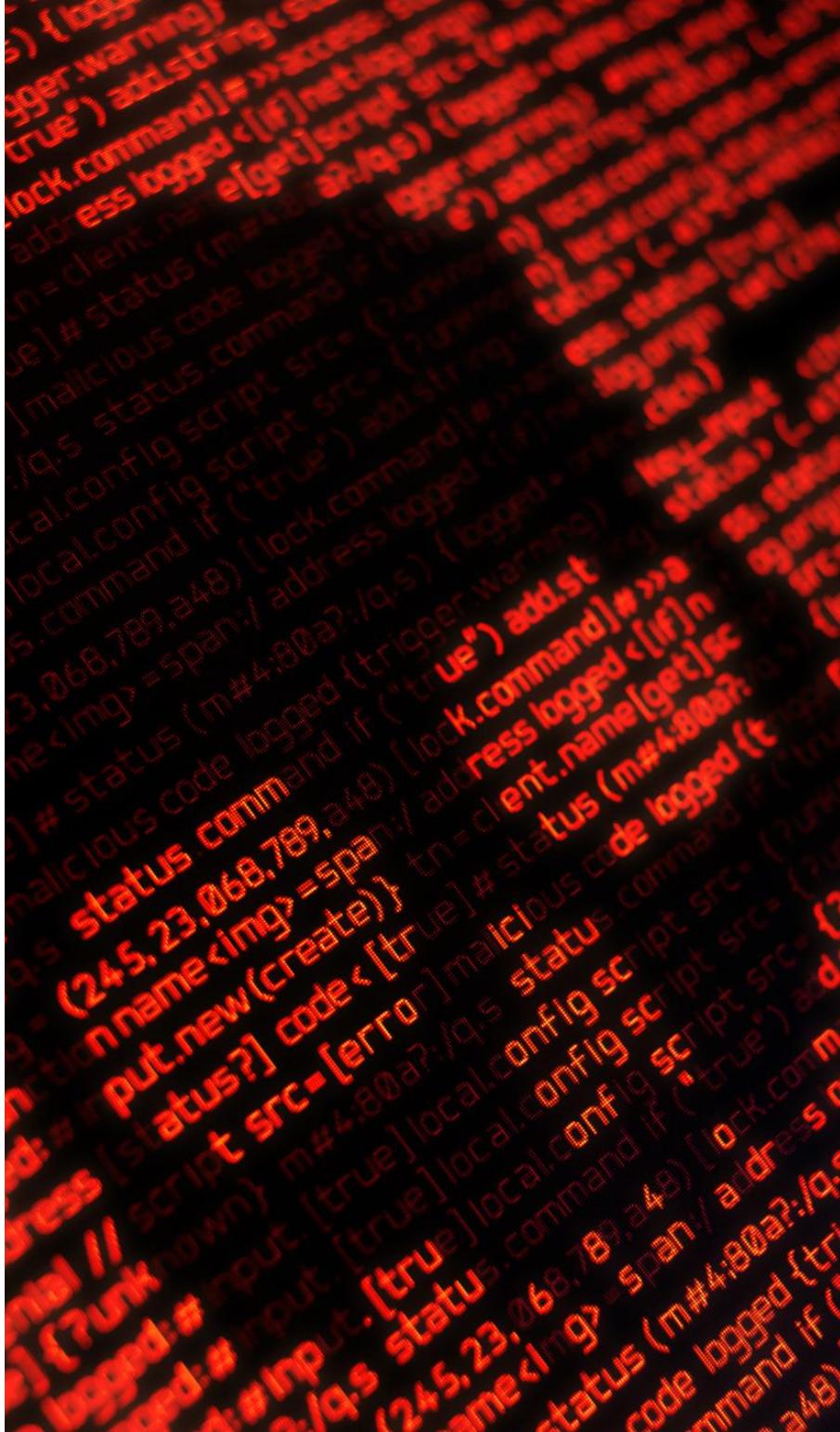
Laboratorio

- Aplicar el ciclo visto a un incidente de seguridad simulado

Introducción al Malware

¿Qué es Malware?

Es un software malicioso que daña o deshabilita los sistemas informáticos y otorga un control limitado o total de los sistemas al creador del malware con el propósito de robo o fraude.

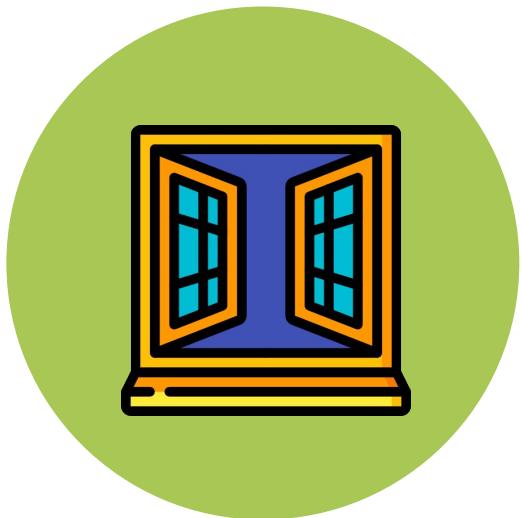


Tipos de Malware



Troyanos

Se presenta al usuario como un programa aparentemente legítimo, pero que, al ejecutarlo, le brinda al atacante acceso remoto al equipo infectado



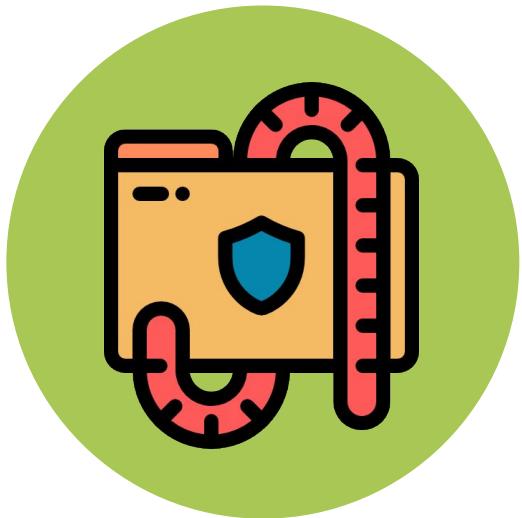
Backdoor

Se introduce en el equipo y establece una puerta trasera a través de la cual es posible controlar el sistema afectado sin conocimiento del usuario



Ransomware

Permite bloquear un dispositivo desde una ubicación remota y encriptar archivos quitando el acceso a la información y datos almacenados



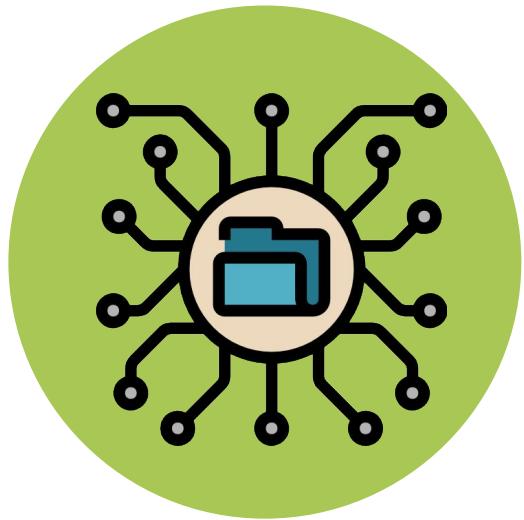
Gusanos

Puede replicarse a sí mismo en los equipos o a través de redes de computadores sin que te des cuenta de que el equipo está infectado



Spyware

Recopila información de un equipo y después transmite esa información a una entidad externa sin el consentimiento del propietario de la información



Botnet

Es una red de equipos que han sido infectados por malware y se ejecutan de manera autónoma y automática



Crypter

Tipo de software que puede encriptar y manipular malware, para que sea más difícil de detectar mediante programas de seguridad



Virus

Software que tiene por objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático

Contramedidas para el Malware

1 - Instalar un software antivirus

2 - Generar una política de antivirus

3 - Mantener actualizado el software de antivirus

4 - Evitar abrir archivos adjuntos de remitentes desconocidos

5 - Mantener con regularidad Backups de la información

6 - Programar escaneos regulares para todos los dispositivos

7 - No abrir dispositivos o programas sin analizarlos por el antivirus

8 - No utilizar software pirata

Laboratorios

- Crear un virus sencillo utilizando la consola de comandos y herramientas automatizadas
- Crear un troyano sencillo

Ingeniería Social

¿Qué es Ingeniería Social?

Es el arte de convencer a las personas para que revelen información confidencial. Los objetivos comunes de la ingeniería social incluyen personal de mesa de ayuda, agentes de soporte técnico.

Fases de un ataque

1.
OBTENER
INFORMACIÓN

2.
SELECCIONAR
LA VÍCTIMA

3.
DESARROLLAR
LA RELACIÓN

4.
EXPLOTAR LA
RELACIÓN

Tipos de Ataques

-  Basada en seres humanos y relaciones interpersonales
-  Basada en sistemas

Basada en Seres Humanos

- Suplantación
- Disfraz
- En persona

En Persona



Shoulder surfing



Dumpster diving

Shoulder Surfing

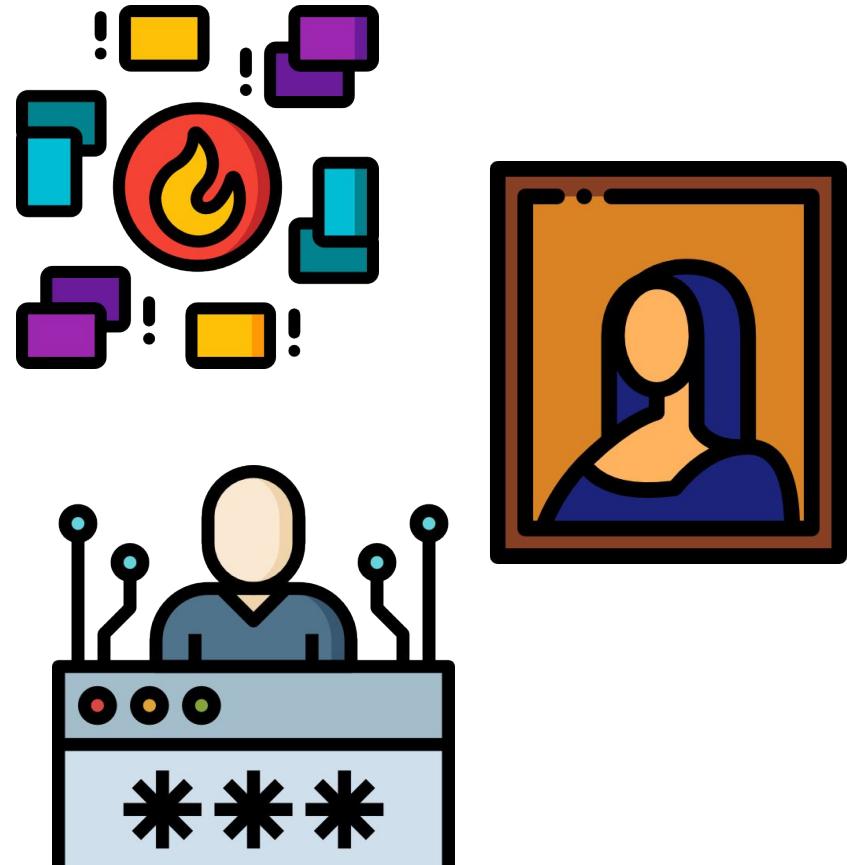


Dumpster Diving



2. Basada en Sistemas

- Ventanas pop-up
- Archivos adjuntos
 - Esteganografía
- Sitios Web
 - Phishing



¿Cómo Defenderse?

Contramedidas para la Ingeniería Social

1 - Definición de políticas de password

2 – Políticas de seguridad física

3 – Entrenamiento a empleados

4 – Clasificación de información

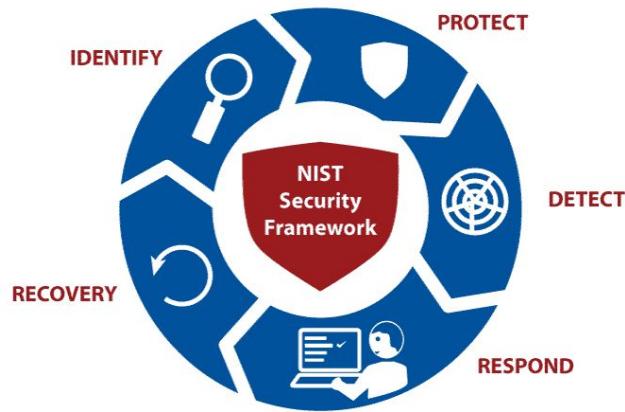
5 – Definición de lineamientos operacionales

6 – Doble factor de autenticación

7 – Instalación de software Antivirus

8 – Terminación adecuada de relaciones laborales

Estándares Internacionales de Seguridad



Modelo de Referencia de Procesos

Evaluar, Dirigir, Supervisar (EDM) - Procesos Gobierno de TI

EDM01 Definir y Mantener el Marco de Gobierno	EDM02 Asegurar Entrega de Beneficios	EDM03 Asegurar Optimización de Riesgo	EDM04 Asegurar Optimización de Recursos	EDM05 Asegurar Transparencia para los Interesados
---	--------------------------------------	---------------------------------------	---	---

Alinear, Planear, Organizar (APO) - Procesos Gestión de TI

APO01 Gestionar el Marco de Gestión de TI	APO02 Gestionar la Estrategia	APO03 Gestionar la Arquitectura Empresarial	APO04 Gestionar Innovación	APO05 Gestionar Cartera	APO06 Gestionar Presupuesto y Costos	APO07 Gestionar Recursos Humanos
APO08 Gestionar Relaciones	APO09 Gestionar Acuerdos de Servicio	APO10 Gestionar Proveedores	APO11 Gestionar Calidad	APO12 Gestionar Riesgo	AP13 Gestionar Seguridad	

Construir, Adquirir, Implantar (BAI) – Procesos Gestión de TI

BAI01 Gestionar Programas y Proyectos	BAI02 Gestionar Definición de Requerimiento	BAI03 Gestionar Identificación de Soluciones y Construir	BAI04 Gestionar Disponibilidad y Capacidad	BAI05 Gestionar Facilitación del Cambio Organizacional	BAI06 Gestionar Cambios	BAI07 Gestionar Aceptación del Cambio y Transición
BAI08 Gestionar Conocimiento	BAI09 Gestionar Activos	BAI10 Gestionar Configuración				

Entrega, Servicio, Soporte (DSS) – Procesos Gestión de TI

DSS01 Gestionar Operaciones	DSS02 Gestionar Requerimientos de Servicio e Incidentes	DSS03 Gestionar Problemas	DSS04 Gestionar Continuidad	DSS05 Gestionar Servicios de Seguridad	DSS06 Gestionar Control de Procesos de Negocio
-----------------------------	---	---------------------------	-----------------------------	--	--

Supervisar, Evaluar, Valorar (MEA)
Procesos Gestión de TI

MEA01
Desempeño y Conformidad

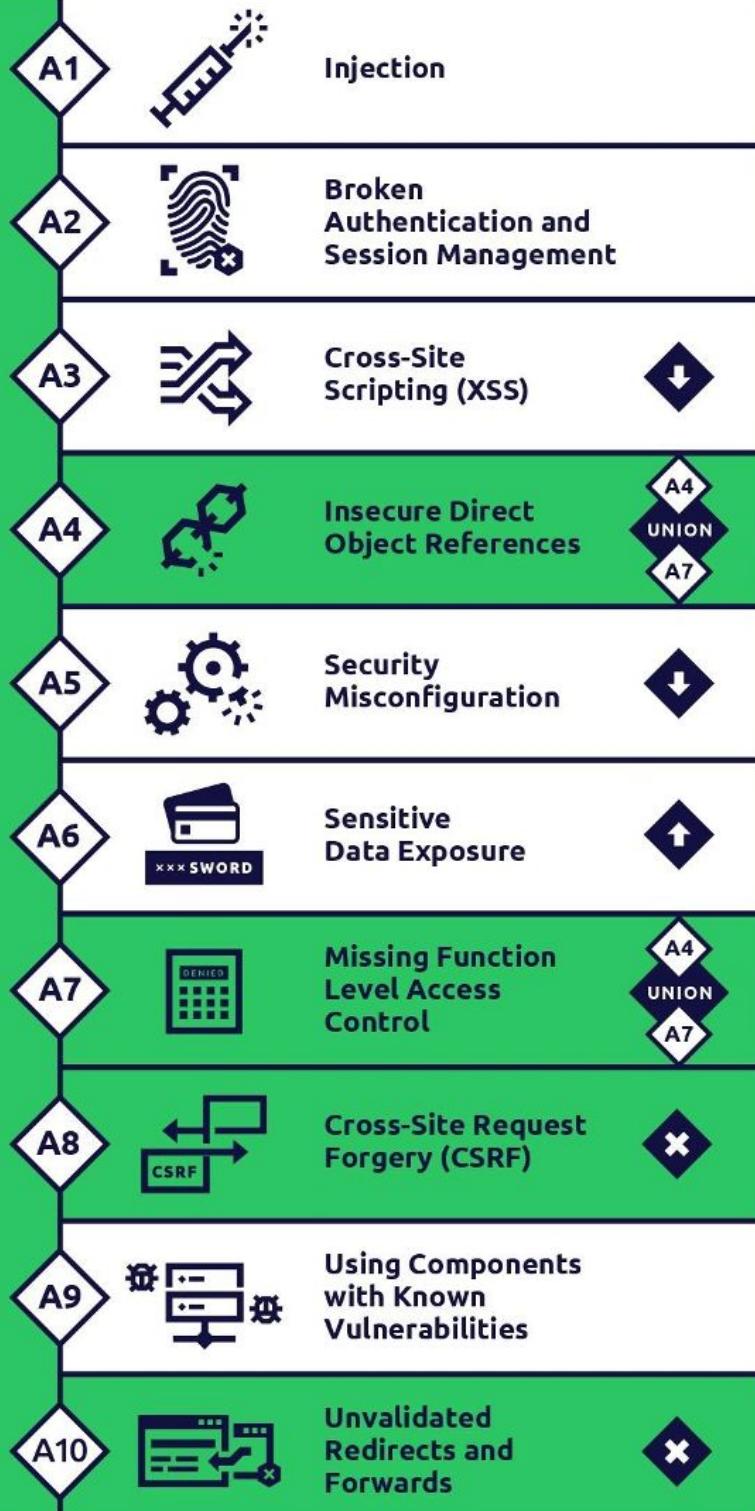
MEA02
Sistema de Control Interno

MEA03
Cumplimiento Requerimientos

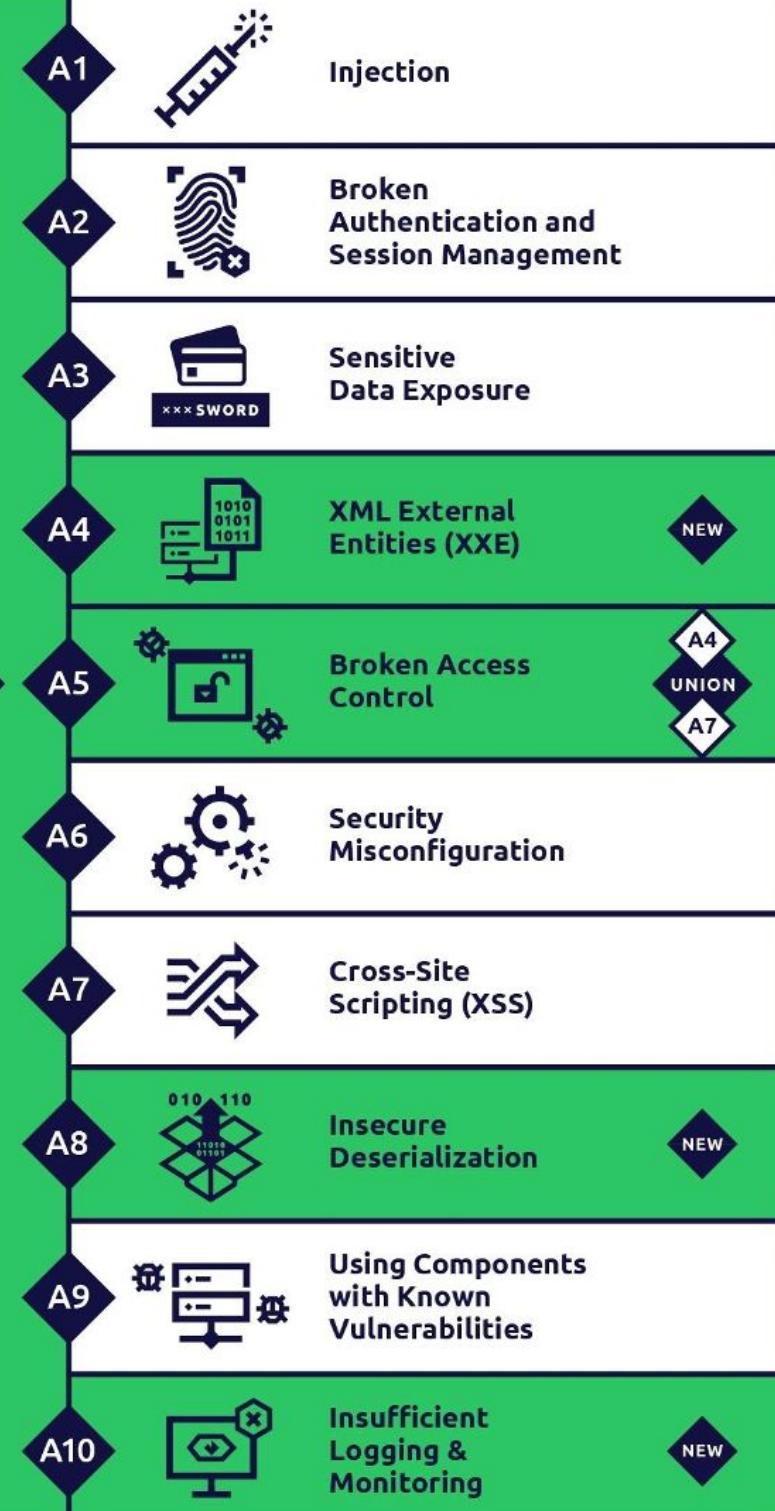


**GESTIÓN DE LA
SEGURIDAD DE LA
INFORMACIÓN**

2013



2017



Basic CIS Controls

- 1 Inventory and Control of Hardware Assets
- 3 Continuous Vulnerability Management
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 2 Inventory and Control of Software Assets
- 4 Controlled Use of Administrative Privileges
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational CIS Controls

- 7 Email and Web Browser Protections
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches
- 13 Data Protection
- 15 Wireless Access Control
- 8 Malware Defenses
- 10 Data Recovery Capabilities
- 12 Boundary Defense
- 14 Controlled Access Based on the Need to Know
- 16 Account Monitoring and Control

Organizational CIS Controls

- 17 Implement a Security Awareness and Training Program
- 19 Incident Response and Management
- 18 Application Software Security
- 20 Penetration Tests and Red Team Exercises

NIST Cybersecurity Framework

IDENTIFY

Asset management

Business environment

Governance

Risk assessment

Risk management strategy

PROTECT

Awareness control

Awareness and training

Data security

Info protection and procedures

Maintenance

Protective technology

DETECT

Anomalies and events

Security continuous monitoring

Detection process

RESPOND

Response Planning

Communications

Analysis

Mitigation

Improvements

RECOVER

Recover planning

Improvements

Communications

Anexo "A" ISO 27001:2013 Objetivos de Control

- A.5 Políticas de seguridad
- A.6 Organización de la información
- A.7 Seguridad en recursos humanos
- A.8 Gestión de activos
- A.9 Control de accesos
- A.10 Criptografía
- A.11 Seguridad física y ambiental
- A.12 Seguridad en las operaciones
- A.13 Transferencia de información
- A.14 Adquisición de sistemas, desarrollo y mantenimiento
- A.15 Relación con proveedores
- A.16 Gestión de los incidentes de seguridad
- A.17 Continuidad de negocio
- A.18 Cumplimiento con requerimientos legales y contractuales