

# UNIVERSIDAD PARAGUAYO ALEMANA

## Ingeniería en Tecnologías de la Información Empresarial TIE

### Seguridad en TICs

*Prof.: Chrystian Ruiz Diaz*

# DISCLAIMER

Todo el contenido de esta presentación se proporciona **exclusivamente con fines didácticos y educativos en el ámbito académico.**

El uso inapropiado de las técnicas y/o conocimientos expuestos en esta presentación puede violar leyes nacionales e internacionales.

El autor y la institución educativa no se hacen responsables del uso indebido de la información contenida en esta presentación.

Se enfatiza que la información debe ser empleada únicamente para propósitos éticos, legales y con la debida autorización de las autoridades competentes.





# Seguridad Informática

## Contenido

1. VPN
2. Certificados Digitales
3. CERTs
4. Software Malicioso
5. Análisis de Riesgo

# Seguridad Informática

## VPN - *Virtual Private Network*

Es un mecanismo para establecer una conexión segura de acceso remoto a través de una red

### Beneficios

La **conectividad**: disponibiliza acceso a los recursos de manera **oportuna, eficiente y segura** promoviendo la alta productividad



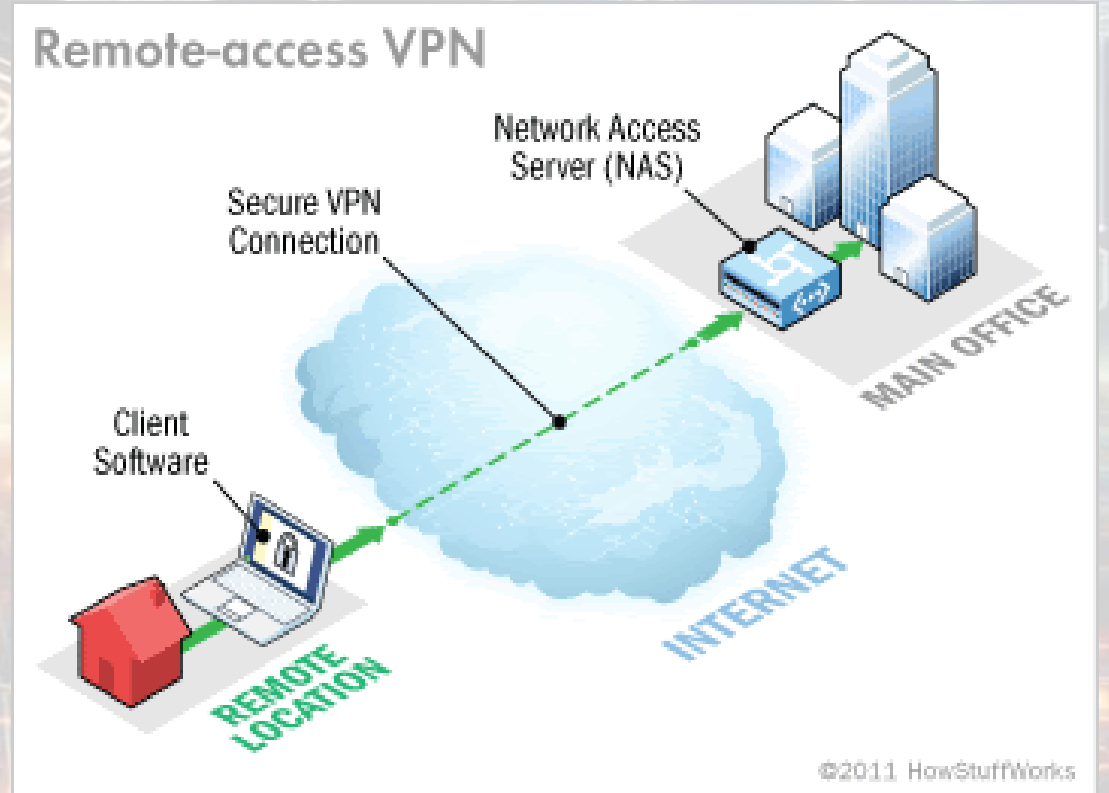


## Seguridad Informática

### VPN - *Virtual Private Network*

#### Arquitecturas VPN

**Remote Access:** admite conexiones VPN de un host a un sitio remoto. Este diseño permite a los teletrabajadores



## Seguridad Informática

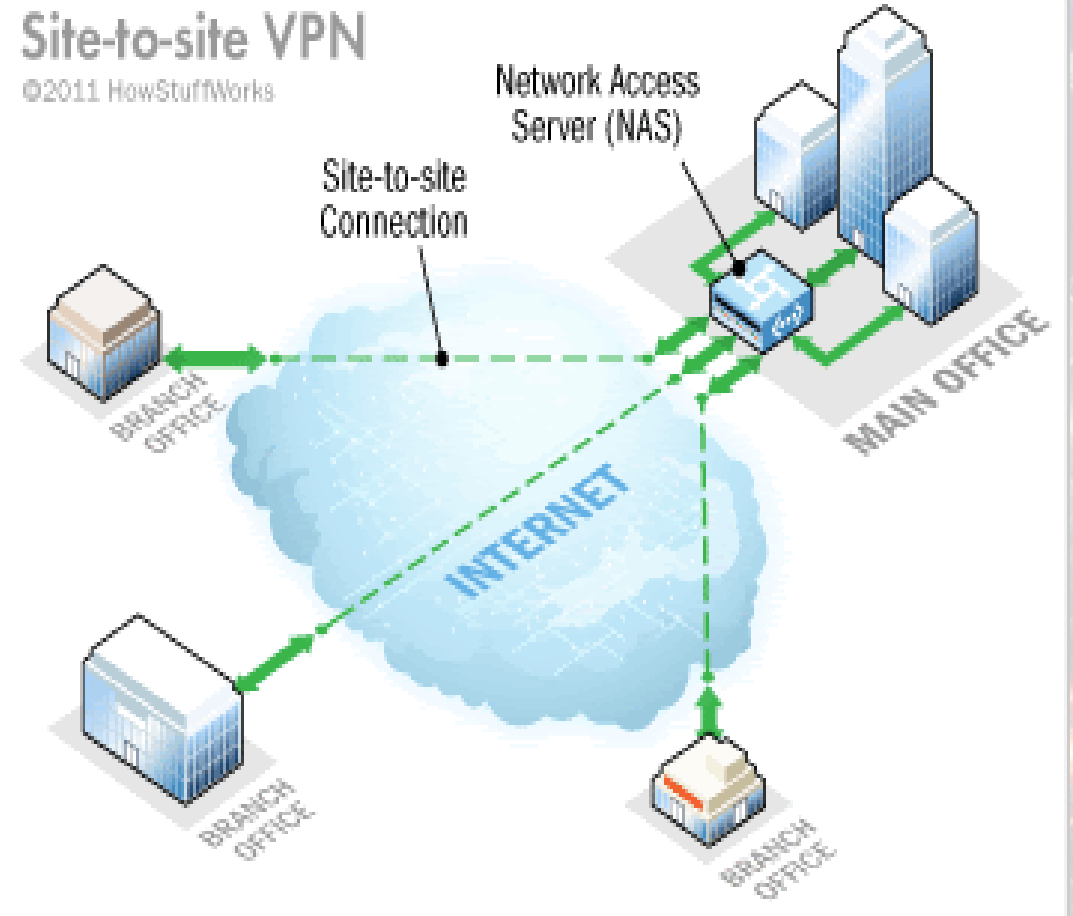
### VPN - *Virtual Private Network*

#### Arquitecturas VPN

**Site-to-Site:** soporta conexiones seguras entre LANs a través de redes públicas intermediarias

#### Site-to-site VPN

©2011 HowStuffWorks



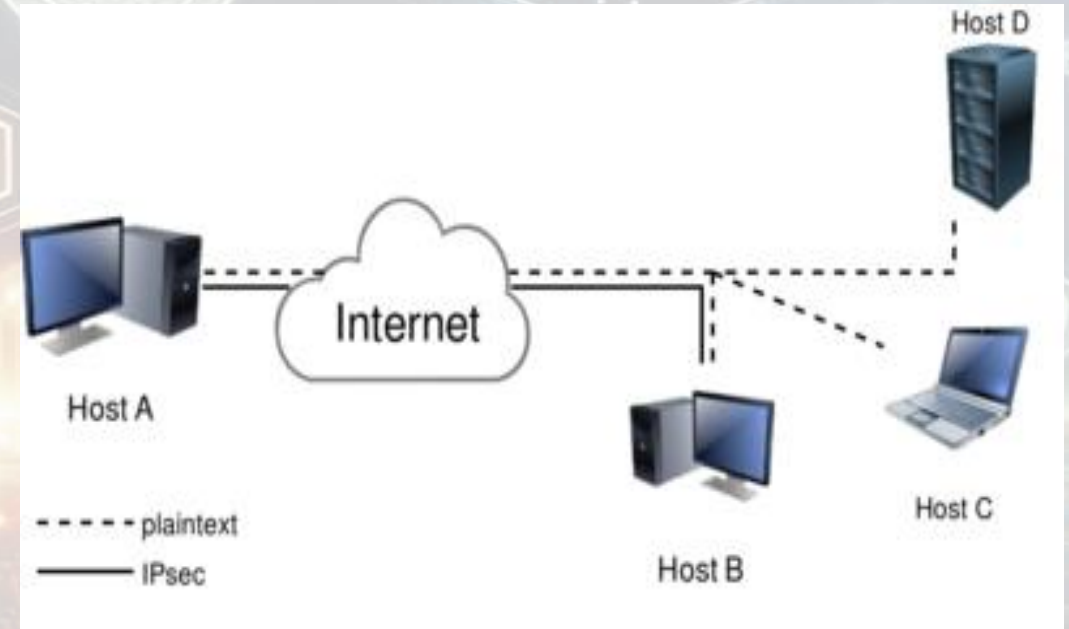


# Seguridad Informática

## VPN - *Virtual Private Network*

### Arquitecturas VPN

**Host-to-Host:** es una conexión VPN directa entre un host y otro

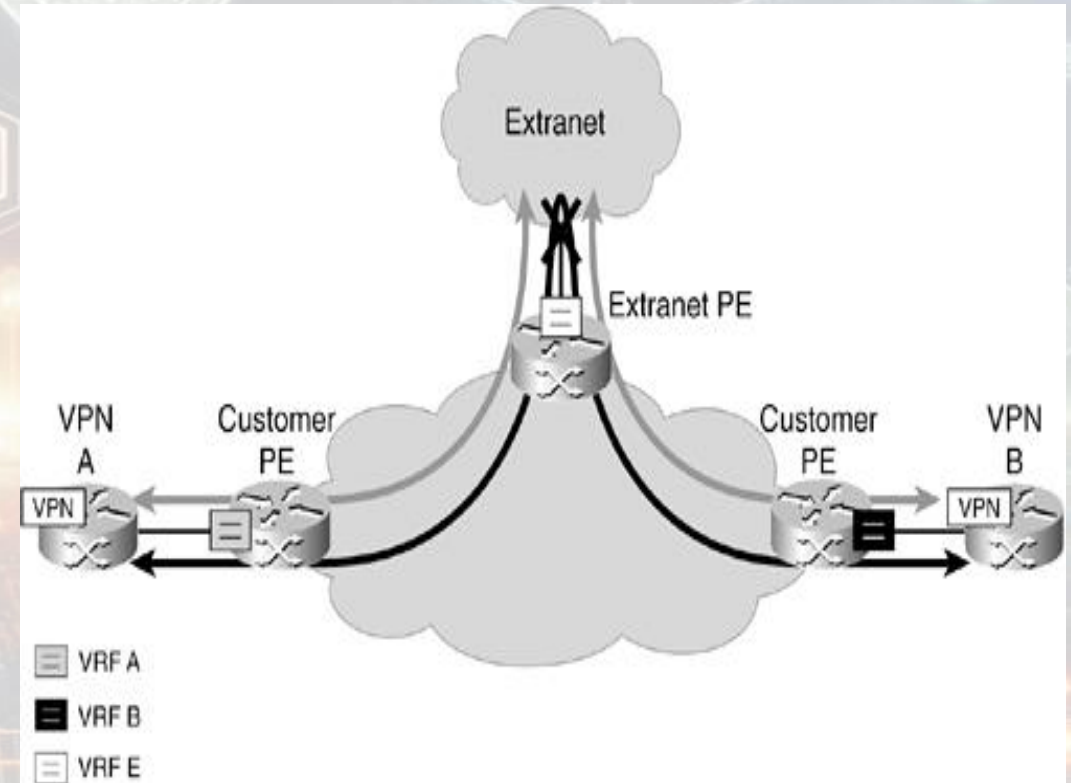


## Seguridad Informática

### VPN - *Virtual Private Network*

#### Arquitecturas VPN

**Extranet Access:** es una conexión VPN directa entre un host y otro. Con un punto final de túnel VPN situado en el perímetro de una extranet o dentro de él, esta opción sirve como vía para que los socios comerciales, distribuidores, proveedores, etc. para acceder a los recursos corporativos sin exponer su tráfico a Internet ni o concederles un acceso innecesario a la LAN privada.





# Seguridad Informática

## VPN - *Virtual Private Network*

### Tipos principales de encapsulación de cifrado

#### Transport Mode vs. Tunnel Mode

##### Transport Mode

- IP payload is encrypted
- IP header is not encrypted
- Original IP header is used for routing decisions
- Provides protection for the payload from end to end

##### Tunnel Mode

- IP payload is encrypted
- IP header is encrypted
- New IP packet encapsulates the encrypted one with a new header that is used for routing decisions



## Seguridad Informática

### VPN - *Virtual Private Network*

¿VPN sin cifrar?

Una VPN solo existe si el trafico esta cifrado



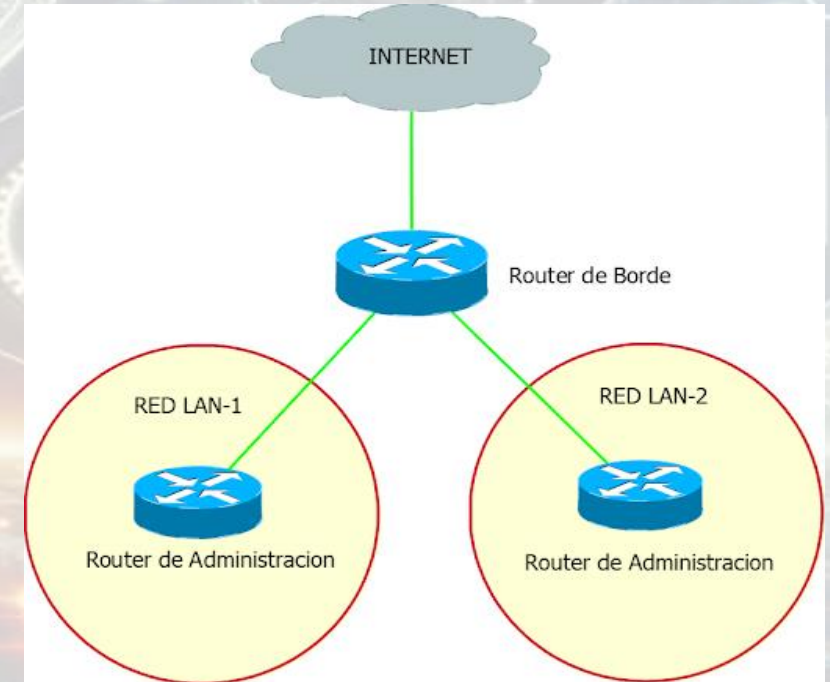
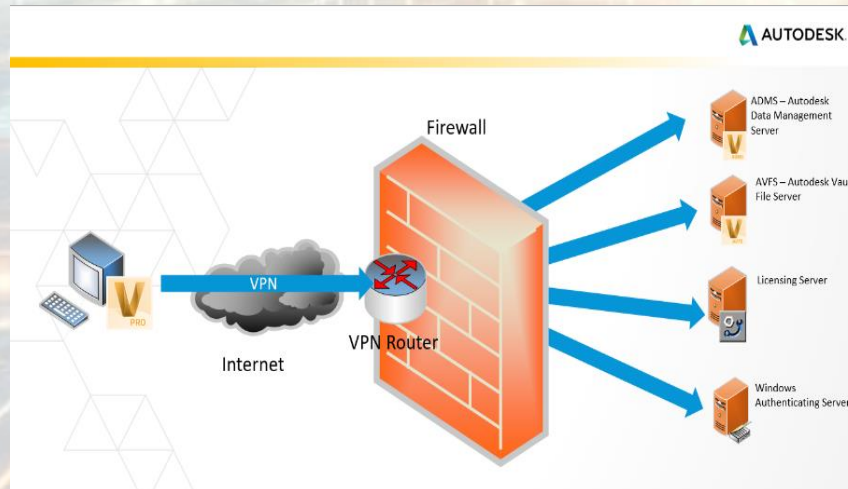


# Seguridad Informática

## VPN - *Virtual Private Network*

### Despliegue de una VPN

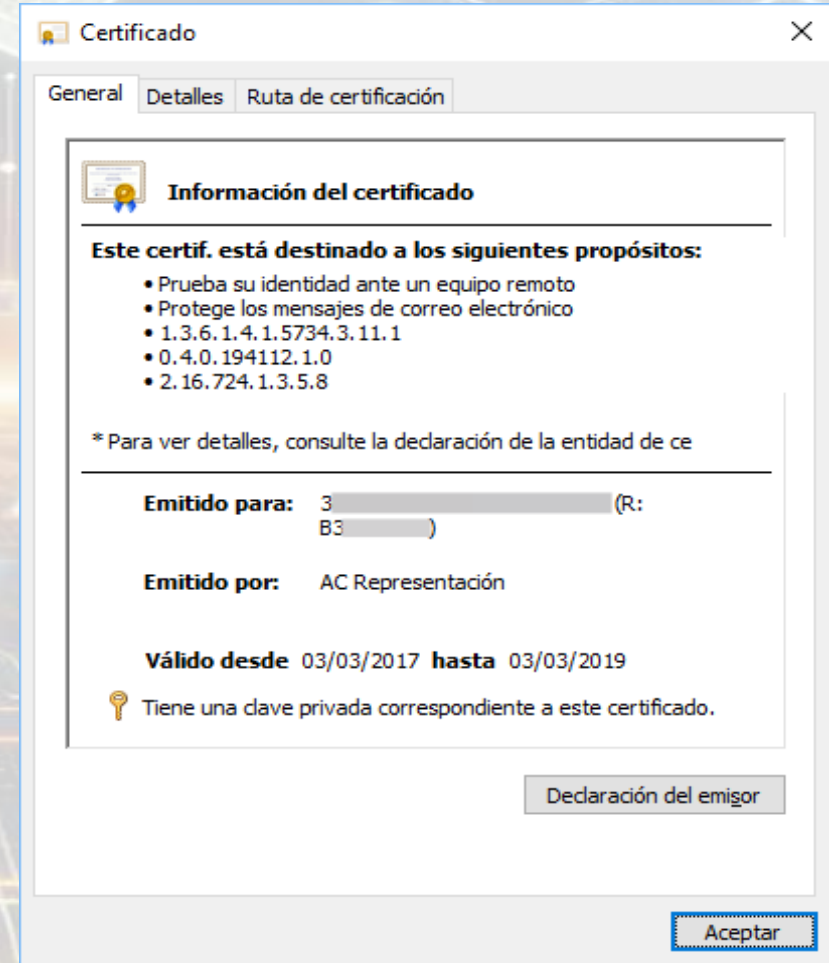
- Edge Router
- Firewall corporativo
- VPN Appliance



# Seguridad Informática

## Certificados Digitales

Es un documento electrónico, identificado por un **número de serie único** y con un **periodo de validez** incluido en el propio certificado, que contiene varios datos. Está emitido por una entidad de confianza, denominada **autoridad de certificación** y vincula a su propietario con una **clave pública**.



The screenshot shows a window titled "Certificado" with three tabs: "General", "Detalles", and "Ruta de certificación". The "General" tab is active, displaying the following information:

**Información del certificado**

**Este certif. está destinado a los siguientes propósitos:**

- Prueba su identidad ante un equipo remoto
- Protege los mensajes de correo electrónico
- 1.3.6.1.4.1.5734.3.11.1
- 0.4.0.194112.1.0
- 2.16.724.1.3.5.8

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

**Emitido para:** 3 (R: B3 )

**Emitido por:** AC Representación

**Válido desde** 03/03/2017 **hasta** 03/03/2019

• Tiene una clave privada correspondiente a este certificado.

Declaración del emisor

Aceptar



# Seguridad Informática

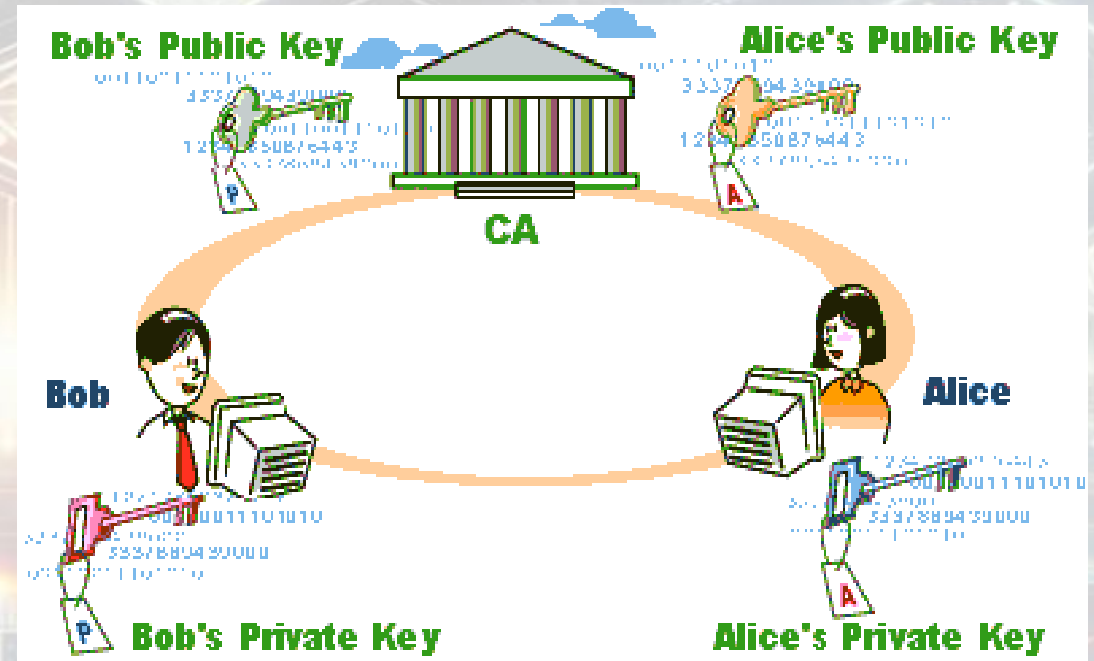
## Certificados Digitales

### Autoridades de certificación

CA - *Certification Authority*: es una entidad a la que uno o más usuarios **confían la creación, asignación y revocación** de los certificados digitales. Su **misión** es **asegurar** que un certificado es **válido**, está **vigente** y corresponde al usuario poseedor del mismo. Por tanto, permiten **garantizar la autenticidad y veracidad de los datos** que aparecen en los certificados digitales

### Autoridades de certificación en Paraguay

- <https://www.digito.com.py/>
- <https://www.code100.com.py/>
- <https://www.efirma.com.py/>



## Seguridad Informática

### CERTs - *Computer Emergency Response Team*

CERT o Equipo de Respuesta ante Emergencias Informáticas es un centro de respuesta a incidentes de seguridad en tecnologías de la información.





## Seguridad Informática

### CERT-PY - *Computer Emergency Response Team*

#### Funciones

- Implementar mecanismos de **gestión, coordinación, respuesta e investigación de incidentes** cibernéticos que pongan en riesgo el ecosistema digital nacional.
- Implementar y promover los mecanismos de **monitoreo y detección de incidentes** cibernéticos en organismos y entidades del Estado, así como también en las infraestructuras críticas nacionales
- Establecer e incentivar mecanismos de **intercambio de información** relacionado a incidentes cibernéticos y amenazas, entre el **sector gubernamental, privado, regional e internacional**.
- Implementar mecanismos y desarrollar **actividades para la generación, captación, procesamiento y análisis de información** de ciberseguridad entre actores del ecosistema.
- Implementar y promover mecanismos de **alerta temprana a incidentes y amenazas**.





## Seguridad Informática

### SOFTWARE MALICIOSO

Son virus, gusanos, troyanos y en general todos los tipos de programas que han sido desarrollados para entrar en ordenadores sin permiso de su propietario, y producir efectos no deseados

#### Clasificación según se Capacidad de Propagación

**Virus:** Su nombre es una analogía a los virus reales ya que infectan otros archivos, es decir, sólo pueden existir en un equipo dentro de otro fichero.

**Gusanos.** Son programas cuya característica principal es realizar el máximo número de copias posible de sí mismos para facilitar su propagación.

**Troyanos.** Carecen de rutina propia de propagación, pueden llegar al sistema de diferentes formas, las más comunes son:

- Descargado por otro programa malicioso.
- Descargado sin el conocimiento del usuario al visitar una página web maliciosa.
- Dentro de otro programa que simula ser inofensivo





# SOFTWARE MALICIOSO

Clasificación según las acciones que realiza

**Bloqueador.** Impide la ejecución de determinados programas o aplicaciones

**Bomba lógica.** Programa o parte de un programa que se instala en un ordenador y no se ejecuta hasta que se cumple determinada condición. Ej Fecha

**Broma (Joke).**

**Bulo (Hoax).** Mensaje electrónico enviado por un conocido que intenta hacer creer al destinatario algo que es falso, como alertar de virus inexistentes



## SOFTWARE MALICIOSO

Clasificación según las acciones que realiza

***Capturador de pulsaciones (Keylogger).*** Monitoriza las pulsaciones del teclado que se hagan en el ordenador infectado

***Clicker.*** Redirecciona las páginas de Internet a las que intenta acceder el usuario, de este modo logra aumentar el número de visitas a la página redireccionada

***Criptovirus (Ransomware).*** Hace inaccesibles determinados ficheros en el ordenador y coacciona al usuario víctima a pagar un “rescate”.

***Exploit.*** Tipo del software que se aprovecha de un agujero o de una vulnerabilidad en el sistema de un usuario para tener el acceso desautorizado al sistema

***Instalador (Dropper).*** Instala y ejecuta otros programas, generalmente maliciosos, en el ordenador

***Puerta trasera (Backdoor).*** Permite el acceso de forma remota a un sistema operativo, página web o aplicación, haciendo que el usuario evite las restricciones de control y autenticación que haya por defecto

***Rootkit.*** Toma control de Administrador (“root” en sistemas Unix/Linux) en el sistema, generalmente para ocultar su presencia y la de otros programas maliciosos

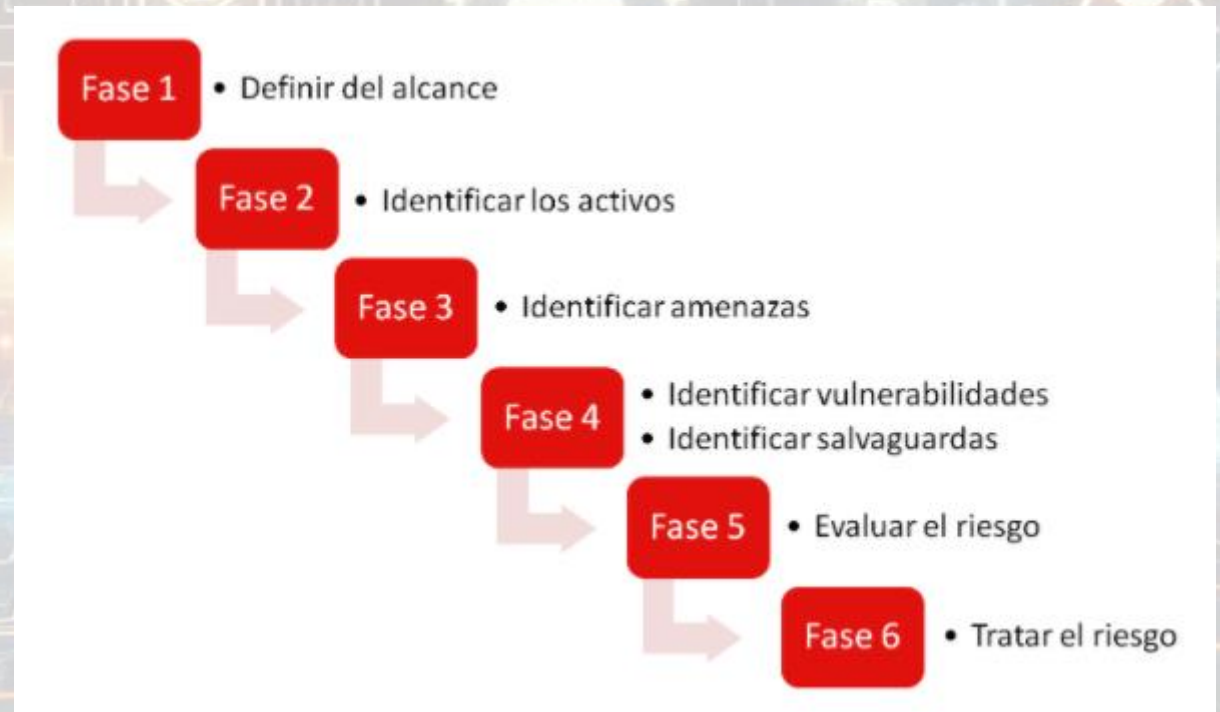


# Seguridad Informática

## ANALISIS DE RIESGOS

Es la evaluación de los distintos peligros que afectan a nivel informático y que pueden producir situaciones de amenaza al negocio, como robos o intrusiones que comprometan los datos o ataques externos que impidan el funcionamiento de los sistemas propiciando periodos de inactividad empresarial

### Fases



# Seguridad Informática

## ANALISIS DE RIESGOS

**Fase 1. Definir el alcance:** análisis de riesgos sobre los procesos del departamento Administración, análisis de riesgos sobre los procesos de producción y gestión de almacén o análisis de riesgos sobre los sistemas TIC

### Fase 2. Identificar los activos

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
ID_01	Servidor 01	Servidor de contabilidad.	Director Financiero	Servidor (Físico)	Sala de CPD1	Sí
ID_02	RouterWifi	Router para la red WiFi de cortesía a los clientes.	Dept. Informática	Router (Físico)	Sala de CPD1	No
ID_03	Servidor 02	Servidor para la página web corporativa.	Dept. Informática	Servidor (Físico)	CPD externo	Sí
...						

**Fase 3. Identificar / seleccionar las amenazas:** si nuestra intención es evaluar el riesgo que corremos frente a la destrucción de nuestro servidor de ficheros, es conveniente, considerar las averías del servidor



## Seguridad Informática

# ANALISIS DE RIESGOS

**Fase 4. Identificar vulnerabilidades y salvaguardas:** Ej una posible vulnerabilidad puede ser identificar un conjunto de ordenadores o servidores cuyo sistemas antivirus no están actualizados o una serie de activos para los que no existe soporte

**Fase 5. Evaluar el riesgo:** Para cada par activo-amenaza, estimaremos la probabilidad de que la amenaza se materialice y el impacto sobre el negocio que esto produciría

### Tabla para el cálculo de la probabilidad

Cualitativo	Cuantitativo	Descripción
Baja	1	La amenaza se materializa a lo sumo una vez cada año.
Media	2	La amenaza se materializa a lo sumo una vez cada mes.
Alta	3	La amenaza se materializa a lo sumo una vez cada semana.

### Tabla para el cálculo del impacto

Cualitativo	Cuantitativo	Descripción
Bajo	1	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio	2	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto	3	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

$$\text{RIESGO} = \text{PROBABILIDAD} \times \text{IMPACTO}$$

# Seguridad Informática

## ANALISIS DE RIESGOS

### Fase 6. Tratar el riesgo

**Transferir el riesgo a un tercero.** Ej. contratando un seguro que cubra los daños a terceros ocasionados por fugas de información.

**Eliminar el riesgo.** Ej. eliminando un proceso o sistema que está sujeto a un riesgo elevado.

**Asumir el riesgo,** siempre justificadamente. Por ejemplo, el coste de instalar un grupo electrógeno puede ser demasiado alto y por tanto, la organización puede optar por asumir.

**Implantar medidas para mitigarlo.** Ej, contratando un acceso a internet de respaldo para poder acceder a los servicios en la nube en caso de que la línea principal haya caído.

### Ejemplo análisis cualitativo

		IMPACTO		
		Bajo	Medio	Alto
PROBABILIDAD	Baja	Muy bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy alto



# ***¿PREGUNTAS?***

# Actividad de Proceso



- Elaborar la tarea “***C4 - Configuración y Uso MSAT (6 puntos)***”

Realizar la tarea y seguir las instrucciones indicadas en Google Classroom.



## Referencias

- BUENDIA, J. F. (2013). *Seguridad informática*. España: McGraw-Hill.
- COSTAS SANTOS, J. (2014). *Seguridad informática*. RA-MA, SA.
- ESCRIVA, G. R. (2013). *Seguridad Informática*. España: Macmillan Iberia SA .
- *GMV SECTORES Ciberseguridad*. (18 de 03 de 0221). Obtenido de GMV SECTORES Ciberseguridad
- INCIBE. (18 de 03 de 2021). *INCIBE - Taxonomia*. Obtenido de <https://www.incibe-cert.es/taxonomia>
- INCIBE-Riesgos. (18 de 03 de 2021). Obtenido de Analisis de Riesgos: <https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo>
- MITIC. (23 de 03 de 2021). Obtenido de CERT-PY: <https://www.cert.gov.py/institucional>
- STEWART, J. M. (2013). *Network Security, Firewalls and VPNs*. Jones & Bartlett Publishers.
- VIEITES, Á. G. (2014). *Gestión de Incidentes de Seguridad Informática*. . RA-MA Editorial.

*Muchas Gracias..!!*

