



**Introducción [RA6]**

* El siguiente entregable está destinado al estudio de los protocolos de la capa de aplicación.
* Consiste en dos partes que serán evaluadas de forma independiente sobre 10 puntos cada una.

1. Apartado A: investigación individual acerca de temas sobre seguridad en la red. Contesta con el mayor detalle posible a las preguntas planteadas.
2. Apartado B: trabajo grupal acerca de un protocolo de la capa de aplicación en concreto (presentación y exposición oral).

**Apartado A: Seguridad en el sistema**

**Ejercicio 1**

¿Cuál es el objetivo de la seguridad informática? ¿Qué tipos de seguridad informática existen, para qué sirve cada una de ellas?

**Indica para cada ejemplo si se trata de seguridad pasiva o activa.**

* **Restaurar las copias de seguridad**
* **Antivirus actualizado**
* **SO con parches de seguridad**
* **Si es necesario restaurar la imagen**
* **Escaneo completo de la máquina**
* **Utilizar usuarios no administradores**

El objetivo principal de la seguridad informática es proteger la confidencialidad, integridad y disponibilidad de los datos y sistemas de información frente a accesos no autorizados, ataques, daños y robos. Esto se logra mediante la implementación de diversas medidas y controles de seguridad.

Tipos de Seguridad Informática y Sus Funciones

**Seguridad de la Información:**

Función: Proteger la información contra accesos no autorizados, alteración y destrucción.

Ejemplo: Encriptación de datos.

Tipo: Activa.

**Seguridad de Redes:**

Función: Proteger la infraestructura de red y el tráfico de datos contra intrusiones y ataques.

Ejemplo: Firewalls y sistemas de detección de intrusos (IDS).

Tipo: Activa.

**Seguridad de Sistemas:**

Función: Proteger los sistemas operativos y aplicaciones contra vulnerabilidades y exploits.

Ejemplo: Aplicar parches de seguridad.

Tipo: Activa.

**Seguridad Física:**

Función: Proteger el hardware y las instalaciones físicas contra daños y accesos no autorizados.

Ejemplo: Controles de acceso y cámaras de vigilancia.

Tipo: Activa.

**Seguridad en la Nube:**

Función: Proteger los datos y aplicaciones almacenados en servicios de nube.

Ejemplo: Controles de acceso y cifrado en la nube.

Tipo: Activa

<https://www.nist.gov/cyberframework>

<https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/>

**Ejercicio 2**

¿Qué es BitLocker? ¿Para qué sirve? ¿Cómo se usa? ¿Qué ventajas e inconvenientes tiene su uso?

BitLocker es una herramienta de cifrado de disco completa de Microsoft que protege los datos almacenados en discos duros mediante cifrado. Sirve para prevenir accesos no autorizados y proteger datos en caso de pérdida o robo del dispositivo. Se usa habilitando desde el panel de control de Windows o a través de la línea de comandos, y requiere una clave de recuperación para desbloquear los datos. Sus ventajas incluyen alta seguridad y facilidad de integración en sistemas Windows, pero puede afectar el rendimiento y es irrelevante si se olvida la clave de recuperación.

<https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/>

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf>

**Ejercicio 3**

¿Qué es un firewall o cortafuegos en informática? ¿Para qué sirve? ¿Cómo funciona? ¿Qué limitaciones presenta?

Un firewall o cortafuegos es un dispositivo de seguridad de red que monitoriza y controla el tráfico de red entrante y saliente basado en reglas de seguridad predefinidas.Sirve para proteger la red , control de acceso, monitoreo y registro, prevención de amenazas.Funciona evaluando el tráfico de red contra un conjunto de reglas predefinidas.Presenta limitaciones como el nivel de red, la incapacidad para detectar amenazas más avanzadas, falsos positivos y negativos y el impacto en el rendimiento.

<https://www.ibm.com/docs/en/i/7.1?topic=options-firewalls>

<https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>

**Ejercicio 4**

¿Cuáles con los principales ataques y cómo podemos protegernos de estos?

Pon 3 casos reales de ataques informáticos y qué podemos hacer para protegernos de ellos.

**Phishing:**

Ataque en el que los atacantes se hacen pasar por entidades de confianza para obtener información sensible, como contraseñas y datos financieros.

Protección:

Educación y Conciencia: Capacitar a los usuarios para reconocer correos electrónicos y mensajes sospechosos.

Autenticación Multifactor (MFA): Añadir capas adicionales de verificación.

**Malware:**

Software malicioso diseñado para dañar, interrumpir o tomar control de sistemas y redes.

Protección:

Software Antivirus: Instalar y mantener actualizado un buen antivirus.

Actualizaciones: Mantener todos los sistemas y aplicaciones actualizadas para corregir vulnerabilidades.

**Ataques DDoS:**

Ataques que sobrecargan un sistema con tráfico, impidiendo su funcionamiento normal.

Protección:

CDN y Redes de Distribución: Usar redes de distribución de contenido que puedan mitigar el tráfico excesivo.

Firewall y Sistemas de Prevención de Intrusiones (IPS): Configurar para detectar y bloquear tráfico malicioso.

**Casos Reales**

Ataque a Sony Pictures (2014):

Un ataque devastador que resultó en la filtración de datos confidenciales, correos electrónicos internos y películas inéditas.

WannaCry Ransomware (2017):

Ransomware que explotó una vulnerabilidad en Windows para infectar y cifrar archivos en miles de sistemas en todo el mundo, pidiendo rescates en bitcoin.

Equifax Data Breach (2017):

Violación masiva de datos que expuso información personal de aproximadamente 147 millones de personas debido a una vulnerabilidad no parcheada.

**Ejercicio 5**

¿Qué es el Cloud Computing? ¿Qué tipos hay? ¿Qué ventajas ofrece?

El Cloud Computing, o computación en la nube, es un modelo que permite el acceso remoto a servicios y recursos de computación a través de internet.

**Modelos de Servicio:**

Infraestructura como Servicio (IaaS)

Proporciona recursos básicos de computación, como máquinas virtuales, almacenamiento y redes.

Plataforma como Servicio (PaaS):

Ofrece herramientas y plataformas para desarrollar, probar y desplegar aplicaciones sin gestionar la infraestructura subyacente.

Software como Servicio (SaaS):

Proporciona aplicaciones completas y gestionadas que los usuarios pueden usar a través de internet.

**Modelos de Implementación:**

Nube Pública:

Servicios ofrecidos a través de internet por proveedores externos y compartidos entre múltiples organizaciones.

Nube Privada:

Infraestructura dedicada exclusivamente a una organización, ya sea gestionada internamente o por un tercero.

Ejemplo: una empresa que tiene su propio centro de datos privado.

Nube Híbrida:

Combinación de nubes públicas y privadas, permitiendo la transferencia de datos y aplicaciones entre ellas.

Ejemplo: una empresa que usa una nube privada para datos sensibles y una nube pública para operaciones menos críticas.

Nube Comunitaria:

Infraestructura compartida entre varias organizaciones con intereses comunes, como misiones de seguridad o requisitos de cumplimiento.

<https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing/>

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

**Apartado B: Trabajo de investigación**

El trabajo de investigación es grupal y deberá estudiar en profundidad uno de los temas (sorteados en clase).

Deberá realizar un trabajo de presentación y una exposición de 10-15 minutos aproximadamente.

* 7 puntos se destinará a la evaluación del documento de la presentación (grupal).
* 3 puntos individuales según la exposición de cada una.

Para cada uno de los protocolos a estudiar, se ofrece una orientación de los puntos clave a estudiar. Puedes añadir si lo crees conveniente o adaptarlos.

Añade:

* Portada.
* Presentación del grupo
* Índice
* Conclusión
* Bibliografía.

**Índice del estudio del protocolo DNS (Domain Name System)**

1. ¿Qué es el DNS?
2. Funcionamiento del DNS.
3. Resolución de nombres de dominio.
4. Servidores DNS raíz y servidores autoritativos.

**Índice del estudio del protocolo DHCP (Dynamic Host Configuration Protocol)**

1. Introducción al DHCP.
2. Asignación dinámica de direcciones IP.
3. Funcionamiento del servidor DHCP.
4. Ventajas y desventajas del DHCP.

**Índice del estudio del protocolo SMTP (Simple Mail Transfer Protocol)**

1. ¿Qué es el SMTP?
2. Proceso de envío de correos electrónicos.
3. Servidores SMTP y clientes de correo.
4. Seguridad y autenticación en el SMTP.

**Índice del estudio del protocolo FTP (File Transfer Protocol)**

1. Concepto de FTP.
2. Transferencia de archivos mediante FTP.
3. Modos de transferencia (activo y pasivo).
4. Servidores FTP y clientes FTP.

**Índice del estudio del protocolo HTTP (Hypertext Transfer Protocol)**

* 1. Introducción al HTTP.
  2. Funcionamiento de las solicitudes y respuestas HTTP.
  3. Métodos HTTP (GET, POST, PUT, DELETE, etc.).
  4. HTTPS y seguridad en las comunicaciones web.

**Paso 1: Solicitud de Información**

**Paso 2: Servidores de Nombres**

**Paso 3: Servidores de Nombres de Dominios de Primer Nivel (TLD o Top Level Domain).**

**Paso 4: Servidores de DNS Autorizados**

**Paso 5: Recuperar el Registro**

**Paso 6: Acceder al Sitio Web**