

# Guía Básica de Ciberseguridad



| Tipo de ataque                           | Descripción   |
|--|---|
| Phishing                                 | Técnica utilizada para engañar a los usuarios y robar información confidencial, como contraseñas y tarjetas de crédito. |
| Malware                                  | Software malicioso diseñado para dañar, explotar o tomar el control de dispositivos sin el conocimiento del usuario.    |
| Ransomware                               | Tipo de malware que cifra los archivos de un usuario o empresa, exigiendo un rescate para desbloquearlos.               |
| Ataques de denegación de servicio (DDoS) | Intento de hacer que un servicio, como un sitio web, sea inaccesible al abrumarlo con una gran cantidad de tráfico.     |

## Consejos de Seguridad en Línea

1. Utiliza contraseñas fuertes y cámbialas regularmente.
2. No hagas clic en enlaces sospechosos o correos electrónicos no solicitados.
3. Mantén tu software y antivirus actualizados.
4. Activa la autenticación en dos pasos siempre que sea posible.
5. Evita conectarte a redes Wi-Fi públicas sin protección.

# Protección en el Mundo Digital



La seguridad en línea se ha convertido en una prioridad esencial en el mundo actual. Conocer las principales amenazas y cómo protegerte es fundamental. A continuación, se presentan algunos recursos, consejos y un formulario de contacto por si tienes alguna consulta.



| Recurso                           | Descripción  | Consejos Relacionados   |
|-----------------------------------|--|---|
| INCIBE<br>[https://www.incibe.es] | Instituto Nacional de Ciberseguridad de España. Proporciona recursos y alertas de seguridad. | <ul style="list-style-type: none"><li>▪ Actualiza siempre tu software.</li><li>▪ Revisa los permisos de las aplicaciones.</li></ul>               |
| OSI<br>[https://www.osi.es]       | Oficina de Seguridad del Internauta. Ofrece herramientas para mejorar tu seguridad en línea. | <ul style="list-style-type: none"><li>▪ No uses redes Wi-Fi públicas sin protección.</li><li>▪ Configura la autenticación en dos pasos.</li></ul> |

## Contáctanos

Nombre:

Nombre

Correo electrónico:

Email






Mensaje:

Mensaje

Enviar

# Tabla de Amenazas Cibernéticas

Un resumen de las principales amenazas de ciberseguridad y sus características.

| Amenaza           | Descripción  | Consejo  | Imagen  |
|-------------------|--|--|---|
| Phishing          | Técnica que intenta robar información sensible como contraseñas mediante correos falsos. | Nunca hagas clic en enlaces de correos no solicitados.           |    |
| Malware           | Software malicioso diseñado para dañar o infiltrarse en un sistema informático.          | Instala un buen antivirus y mantén tu sistema actualizado.       |    |
| Ransomware        | Tipo de malware que secuestra los datos del usuario hasta que se paga un rescate.        | Realiza copias de seguridad frecuentes de tus datos importantes. |    |
| Ataque DDoS       | Ataque masivo para desbordar servidores, causando interrupciones de servicio.            | Utiliza firewalls y servicios de mitigación de ataques DDoS.     |  |
| Ingeniería Social | Manipulación psicológica para obtener información confidencial de manera directa.        | Desconfía de solicitudes inesperadas de información privada.     |  |

# Principales Buenas Prácticas de Ciberseguridad

Siguiendo estas recomendaciones podrás mejorar la seguridad de tus dispositivos y datos.

## Contraseñas Seguras:

- Utiliza combinaciones de letras mayúsculas, minúsculas, números y símbolos.
- Cambia tus contraseñas regularmente.
- Evita utilizar la misma contraseña en diferentes servicios.

## Actualizaciones de Software:

- Mantén siempre tus dispositivos actualizados.
- Activa las actualizaciones automáticas cuando sea posible.

## Copia de Seguridad:

- Realiza copias de seguridad periódicas de tus datos importantes.
- Almacena las copias en ubicaciones seguras y separadas de los dispositivos originales.

## Cuidado con los Correos Electrónicos:

- No abras archivos adjuntos de correos no solicitados.
- Verifica la autenticidad del remitente antes de hacer clic en enlaces.

# Notificación de Brecha de Seguridad de Datos Personales

Por favor, complete el siguiente formulario para informar sobre una posible violación de seguridad de datos.

Nombre de la Empresa/Entidad:

Nombre de la Persona de Contacto:

Correo Electrónico:

Tipo de Brecha de Seguridad:

Acceso no autorizado



Fecha en que se detectó la brecha:



Descripción de la Brecha:

Describe brevemente la brecha de seguridad...

Enviar Notificación

Tipo de Brecha de Seguridad:

Acceso no autorizado



Acceso no autorizado

Divulgación no autorizada

Pérdida de datos

Alteración de datos

Otro

## Horario de Actividades

| HORA                 | DÍA 1                                       |                     | DÍA 2                     |                     |
|----------------------|---|---------------------|---------------------------|---------------------|
|                      | ACTIVIDAD                                   | INSTRUCTOR          | ACTIVIDAD                 | INSTRUCTOR          |
| 09:00 - 10:30        | Introducción a la Ciberseguridad            | Juan Seguridad      | Análisis de Amenazas      | María Protegida     |
| DESCANSO             |   |                     |                           |                     |
| 11:15 - 12:45        | Cumpliendo con el RGPD                      | Ana Protegida       | Prevención de Intrusiones | Carlos Seguridad    |
| 12:45 - 14:00        | Implementación de Seguridad en Aplicaciones | Carlos Seguridad    | Gestión de Incidentes     | Sandra Colaborativa |
| DESCANSO PARA COMIDA |   |                     |                           |                     |
| 15:30 - 17:00        | Trabajo en Equipo para la Ciberseguridad    | Sandra Colaborativa | Auditoría de Seguridad    | Laura Auditora      |

## Incidentes de Red - Cesur Málaga Este

| ID  | TIPO | DESCRIPCIÓN                                      | ESTADO      | FECHA      |
|-----|------|--|-------------|------------|
| 001 | WiFi | Fallo de conexión en aula 101                    | En Progreso | 2024-10-10 |
| 002 | Red  | Interrupción en la conexión de red en biblioteca | Resuelta    | 2024-10-09 |
| 003 | WiFi | Señal débil en pasillo principal                 | Pendiente   | 2024-10-08 |
| 004 | Red  | Problemas de velocidad en aulas 103 y 104        | En Progreso | 2024-10-11 |
| 005 | WiFi | Conexión intermitente en sala de profesores      | Resuelta    | 2024-10-12 |

### Añadir Nueva Incidencia

Tipo de Incidencia:

WiFi

Descripción:

Estado:

Pendiente

Fecha:

dd/mm/aaaa

Añadir Incidencia

# Guía de Instalación de Kali Linux

## Paso 1: Descarga de la Imagen ISO



Visita el sitio oficial de Kali Linux y descarga la imagen ISO correspondiente a tu sistema (32 o 64 bits).

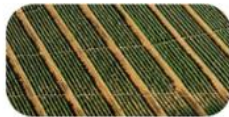
## Paso 2: Crear un USB de Instalación

Utiliza herramientas como Rufus (Windows) o Etcher (macOS y Linux) para crear un USB de instalación con la imagen ISO descargada.



## Paso 3: Configurar el BIOS/UEFI

Reinicia tu computadora y entra en la configuración de BIOS/UEFI. Configura la opción de arranque para que inicie desde el USB.



## Paso 4: Instalación de Kali Linux

Una vez que arranques desde el USB, selecciona la opción de instalación de Kali Linux y sigue las instrucciones en pantalla para completar la instalación.



## Paso 5: Configuración Final

Después de la instalación, configura tu red y actualiza el sistema utilizando el comando `sudo apt update && sudo apt upgrade` en la terminal.

