INSTITUTO KHIPU

Sesión 11

UNIDAD DIDÁCTICA

COMPETENCIAS DIGITALES

Tema

SEGURIDAD EN EL MANEJO DE DOCUMENTOS SENSIBLES

SEGURIDAD EN EL MANEJO DE DOCUMENTOS SENSIBLES

La seguridad en el manejo de documentos sensibles se refiere a las prácticas, políticas y tecnologías implementadas para proteger la integridad, confidencialidad y disponibilidad de documentos que contienen información delicada o confidencial. Aquí se describen los aspectos clave de esta seguridad:

1. **Confidencialidad**:
    - **Acceso Controlado**: Solo personas autorizadas deben tener acceso a los documentos sensibles. Esto se logra mediante sistemas de control de acceso, autenticación y autorización.
    - **Cifrado**: Los documentos deben ser cifrados tanto en tránsito como en reposo para protegerlos de accesos no autorizados durante su almacenamiento y transferencia.
2. **Integridad**:
    - **Verificación de Integridad**: Uso de hash y firmas digitales para asegurar que los documentos no han sido alterados desde su creación o última modificación.
    - **Control de Versiones**: Implementación de un sistema de control de versiones que permita rastrear y revertir cambios no autorizados o no deseados.
    -

3. **Disponibilidad**:
    - **Backups Regulares**: Realización de copias de seguridad regulares para prevenir pérdida de datos debido a fallos técnicos, desastres naturales o ciberataques.
    - **Planes de Recuperación de Desastres**: Desarrollo y mantenimiento de un plan de recuperación ante desastres para garantizar que los documentos estén disponibles incluso en situaciones adversas.
4. **Manejo Físico**:
    - **Almacenamiento Seguro**: Los documentos en formato físico deben guardarse en lugares seguros, como cajas fuertes o archivos con acceso restringido.
    - **Destrucción Segura**: Implementar procedimientos para la destrucción segura de documentos cuando ya no sean necesarios, como el uso de trituradoras de documentos certificadas.
5. **Manejo Electrónico**:
    - **Sistemas de Gestión de Documentos (DMS)**: Utilización de DMS para organizar, almacenar y gestionar documentos de manera segura, con capacidades de auditoría y monitoreo de accesos y modificaciones.
    - **Monitoreo y Auditoría**: Implementación de herramientas de monitoreo y auditoría para registrar y analizar el acceso y uso de documentos sensibles, identificando cualquier actividad inusual o sospechosa.

6. **Educación y Concienciación**:
    - **Capacitación del Personal**: Proveer formación continua a los empleados sobre la importancia de la seguridad en el manejo de documentos sensibles y las mejores prácticas para proteger esta información.
    - **Políticas y Procedimientos**: Desarrollo y comunicación clara de políticas y procedimientos para el manejo seguro de documentos sensibles, asegurando que todo el personal esté al tanto de sus responsabilidades.
7. **Cumplimiento Normativo**:
    - **Regulaciones y Normas**: Asegurar que las prácticas de manejo de documentos cumplen con las leyes, regulaciones y normas aplicables, como GDPR, HIPAA, ISO/IEC 27001, entre otras.

Implementar estos principios y prácticas ayuda a mitigar los riesgos asociados con la pérdida, robo o divulgación no autorizada de información sensible, protegiendo así a la organización y a las personas relacionadas con estos documentos.

USO DE CONTRASEÑAS Y CIFRADO PARA PROTEGER ARCHIVOS DE WORD

El uso de contraseñas y cifrado para proteger archivos de Word es una medida fundamental para garantizar la seguridad de los documentos sensibles. Aquí te detallo las mejores prácticas y cómo implementarlas:

Uso de Contraseñas en Archivos de Word

1. **Asignar una Contraseña para Abrir el Archivo**:
    - Abre el documento de Word.
    - Ve a **Archivo > Información > Proteger documento > Cifrar con contraseña**.
    - Introduce la contraseña deseada y confírmala.
    - Guarda el archivo. A partir de este momento, se requerirá la contraseña para abrir el documento.
2. **Asignar una Contraseña para Modificar el Archivo**:
    - Abre el documento de Word.
    - Ve a **Archivo > Guardar como** y selecciona una ubicación.
    - En el cuadro de diálogo **Guardar como**, haz clic en **Herramientas > Opciones generales**.
    - Introduce una contraseña en el campo **Contraseña de modificación** y, si lo deseas, también en **Contraseña de apertura**.
    - Guarda el archivo.

Cifrado de Archivos de Word

Word utiliza cifrado avanzado para proteger los archivos mediante contraseñas. La versión de Microsoft Office 2007 y posteriores emplea el cifrado AES de 128 bits, que es robusto y adecuado para la mayoría de las necesidades de seguridad.

Mejores Prácticas para Contraseñas y Cifrado

1. **Crear Contraseñas Fuertes**:
    - Utiliza una combinación de letras mayúsculas y minúsculas, números y símbolos.

- Evita contraseñas obvias como nombres, fechas de nacimiento o palabras comunes.

2. **Almacenamiento Seguro de Contraseñas**:
    - Usa un administrador de contraseñas para almacenar y gestionar tus contraseñas de manera segura.
    - No compartas las contraseñas a través de medios inseguros como correos electrónicos no cifrados.
3. **Cambiar Contraseñas Regularmente**:
    - Actualiza las contraseñas periódicamente para minimizar el riesgo de acceso no autorizado.
4. **Mantener el Software Actualizado**:
    - Asegúrate de utilizar la última versión de Microsoft Office para beneficiarte de las últimas actualizaciones de seguridad y mejoras en el cifrado.

Procedimiento para Cifrar un Archivo de Word

1. **Abrir el Documento**:
    - Abre el documento de Word que deseas proteger.
2. **Cifrar con Contraseña**:
    - Haz clic en **Archivo** en la esquina superior izquierda.
    - Selecciona **Información**.
    - Haz clic en **Proteger documento**.
    - Elige **Cifrar con contraseña** del menú desplegable.
    - Introduce una contraseña en el cuadro de diálogo y confírmala.
    - Haz clic en **Aceptar**.
    - Guarda el documento para aplicar la protección.

DESVENTAJAS Y CONSIDERACIONES

- **Recuperación de Contraseñas**: Si olvidas la contraseña, no hay manera de recuperarla, lo que significa que perderás el acceso al documento.
- **Compatibilidad**: Asegúrate de que la persona que necesita acceder al documento tenga una versión compatible de Microsoft Word que soporte el cifrado.

Uso de Herramientas Adicionales

Para una seguridad adicional, considera el uso de herramientas de cifrado externas como **VeraCrypt** o **7-Zip** para cifrar los archivos antes de enviarlos por correo electrónico o almacenarlos en la nube.

1. **VeraCrypt**:
    - Crea un volumen cifrado y guarda el archivo de Word dentro de este volumen.
2. **7-Zip**:
    - Usa la opción de cifrado de archivos en 7-Zip para proteger el archivo de Word con una contraseña.

Implementar estas medidas ayudará a proteger tus documentos de Word contra accesos no autorizados, asegurando la confidencialidad y la integridad de la información contenida.

INSTITUTO

KHIPU