Cómo hacer la copia de seguridad de tu Certificado Electrónico

No pierdas tu certificado

¿Qué es el Certificado Digital?

¿Qué es el Certificado Digital?

1) Un certificado electrónico es un archivo digital que se utiliza para verificar y autenticar la identidad de una entidad en el entorno digital.
2) Contiene información esencial, como el nombre de la entidad o persona, su clave pública y el nombre de la autoridad emisora.
3) Está firmado por la entidad emisora que asegura su veracidad.

Funciones del certificado electrónico

Funciones del certificado electrónico

1) **El certificado electrónico cumple diversas funciones cruciales para la seguridad de la información:**

- **Verifica la identidad declarada en el certificado coincide con la entidad que lo presta.**
- **Permite establecer la confianza necesaria el comunicarse y realizar transacciones en línea.**
- **Proporciona un mecanismo para garantizar la integridad y autenticidad de los documentos digitales.**
- **Permite firmar documentos electrónicos con validez legal y probatoria.**
- **Permite el intercambio seguro de información confidencial.**
- **Los datos cifrados solo pueden ser descifrados por la entidad que posee el certificado correspondiente.**

Tipos de certificados electrónicos más comunes

Tipos de certificados

1) **Certificados de servidor**

- **Los certificados de servidor son utilizados en sitios web para establecer una conexión segura entre el servidor y el navegador del usuario.**
- **Aseguran que los datos transmitidos entre el servidor y el usuario estén protegidos y no sean interceptados o alterados por terceros.**
- **Cuando visitamos un sitio web seguro, en la dirección vemos que aparece "https" en lugar de "http". Esto indica que el sitio web utiliza un certificado de servidor para garantizar la seguridad de la comunicación.**

Tipos de certificados

1) **Certificados de firma**

- **Los certificados de firma son utilizados para firmar digitalmente documentos electrónicos.**
- **Al firmar un documento con un certificado de firma, se garantiza su integridad y autenticidad.**
- **Proporciona una forma de verificar la identidad del firmante.**
- **Son muy utilizados en transacciones comerciales, presentación de documentos legales y otros procesos en línea que requieren una firma auténtica y válida.**

Tipos de certificados

1) **Certificados de cliente**

- **Los certificados de cliente son utilizados por los usuarios para autenticarse en servicios en línea.**
- **Estos certificados permiten a los usuarios demostrar su identidad ante una entidad o plataforma, como la banca electrónica, presentación de declaraciones fiscales, etc.**
- **Los usuarios pueden acceder a servicios en línea de manera segura y confiable, evitando la necesidad de múltiples contraseñas o identificadores tradicionales.**

Importancia de mantener una copia de seguridad

Importancia de la copia de seguridad

1) **Respaldo ante posibles pérdidas**

- **Mantener un copia de seguridad del certificado electrónico es esencial para protegerlo ante posibles pérdidas, accidentes, fallos técnicos o errores humanos.**
- **Nos aseguramos de tener una copia segura de la información en caso de eventos inesperados, como fallos de hardware, formateo accidental o rodo del dispositivo.**

1) **Continuar en nuestras actividades digitales**

- **Nos da la capacidad de mantener la continuidad en nuestras actividades digitales.**
- **Podemos restaurar el certificado desde la copia de seguridad sin interrupciones.**

Importancia de la copia de seguridad

1) **Seguridad y protección de la información**

- **Evitamos el riesgo de que caiga en manos equivocadas o sea utilizado de forma maliciosa por terceros.**
- **Es importante proteger la copia de seguridad del certificado mediante el uso de contraseñas fuertes, cifrado y almacenamiento seguro.**
- **Proteger el acceso para evitar que terceras personas puedan acceder a la información de nuestra copia de seguridad.**

Preparación para la copia de seguridad

Identificar el tipo de certificado electrónico

1) Debemos identificar el tipo de certificado electrónico que tenemos.
2) Permite conocer las características específicas del certificado y los métodos adecuados para realizar tu copia de seguridad.
3) Algunas preguntas que podemos hacernos para identificar el tipo de certificado son:

- ¿Es un certificado de servidor, certificado de firma o certificado de cliente?
- ¿Fue emitido por una autoridad de certificación reconocida?
- ¿Qué información adicional contiene el certificado, como el nombre de la entidad o su clave pública?

Identifica el sistema operativo

1) Dependiendo del sistema operativo, las herramientas utilizadas, la ubicación y el formato de los certificados electrónicos pueden variar.
2) Es importante conocer dónde se almacena el certificado en nuestro sistema.
3) En Windows, los certificados pueden estar almacenados en el almacén de certificados o en el repositorio de claves.
4) En sistemas basados en Unix o Linux, los certificados suelen estar en directorios específicos, como /etc/ssl/certs.

Consulta la documentación o soporte

1) **Si tenemos dificultades para identificar el tipo de certificado o su ubicación en el sistema, es recomendable consultar la documentación del certificado.**

2) **La documentación proporcionada por la entidad emisora puede contener información detallada sobre su manejo y copia de seguridad.**

Identificar los archivos relacionados con el certificado

Identificar los archivos relacionados

1) **Para asegurarnos de realizar una copia de seguridad completa del certificado electrónico, es importante identificar y localizar los archivos relacionados con este:**

- **Archivos de certificados: por lo general, tiene una extensión “.cer” o “.crt” y contiene la información del certificado digital propiamente dicho.**
- **Clave privada: esta es la clave que nos permite usar el certificado para autenticarnos y firmar digitalmente. Por lo general, está protegido por una contraseña y se almacena en un archivo con extensión “.key” o “.pfx”.**
- **Autoridad de certificación (AC) intermedia: en algunos casos, se requiere incluir el certificado de la AC intermedia que emitió nuestro certificado. Este archivo puede tener una extensión “.cer” o “.crt”.**

Almacenamiento seguro de los archivos

Almacenamiento seguro de los archivos

1) Una vez que hemos localizado los archivos relacionados al certificado, debemos asegurarnos de almacenarlos de manera segura.

2) Algunas recomendaciones son:

- Utiliza medios de almacenamiento seguros: como discos duros externos, unidades USB cifradas o servicios en la nube con encriptación.
- Proteger los archivos con contraseña: aplicar contraseñas fuertes a los archivos de respaldo para evitar accesos no autorizados.
- Mantener copias de respaldo en diferentes ubicaciones: distribuir las copias de respaldo en diferentes lugares físicos o servicios en la nube para evitar la perdida completa en caso de desastres o fallos técnicos.

Comprobación de la validez del certificado

Comprobar la validez del certificado

1) **Antes de hacer la copia de seguridad, es recomendable realizar las siguientes pasos de verificación:**

- **Verificar la fecha de vencimiento: comprueba que el certificado no haya expirado. Los certificados caducados pueden ser rechazados por los servicios en línea y no funcionarán correctamente.**
- **Validar la autoridad de certificación: asegúrate de que el certificado haya sido emitido por una autoridad de certificación confiable y reconocida. Esto garantiza la autenticidad y la confianza del certificado.**
- **Verificar la integridad del certificado: realiza una verificación de integridad del certificado para asegurarte de que no haya sido alterado.**

Métodos de copia de seguridad

Almacenamiento físico

1) **Tipos de dispositivos:**

- **Disco duro externo: proporciona una gran capacidad de almacenamiento y velocidad de transferencia de datos.**
- **Unidad USB: es portátil y fácil de transportar, ideal para copias de seguridad en movimiento.**
- **Tarjeta de memoria: adecuada para dispositivos móviles o cámaras que admiten este tipo de almacenamiento.**

Almacenamiento físico

1) **Pasos para realizar la copia de seguridad:**

- **Conectar el dispositivo: conecta el dispositivo al puerto correspondiente de tu ordenador.**
- **Identificar los archivos a respaldar: localizar los archivos relacionados con el certificado que deseamos respaldar, incluyendo el archivo del certificado, la clave privada y cualquier archivo adicional necesario.**
- **Copiar los archivos: seleccionamos los archivos y los copiamos al dispositivo de almacenamiento físico. Es posible que pide algún tipo de contraseña de autenticación para realizar este paso.**
- **Verificar la copia de seguridad: después de realizar la copia, asegurarnos de que los archivos se han transferido correctamente al dispositivo.**

Almacenamiento físico

1) **Consideraciones de seguridad:**

- **Utilizar una contraseña: si el dispositivo de almacenamiento lo permite, establece una contraseña para proteger el acceso a los archivos respaldados.**
- **Mantener el dispositivo seguro: almacena el dispositivo de manera segura en un lugar físico o utiliza cajas de seguridad para evitar su pérdida o robo.**
- **Realizar copias de seguridad adicionales: si es posible, considera realizar copias de seguridad adicionales en dispositivos de almacenamiento separados para evitar la pérdida completa en caso de fallo o daño del dispositivo principal.**

Almacenamiento en la nube

1) **Utilizar un servicio de almacenamiento en la nube nos permite guardar nuestros datos en servidores remotos y acceder a ellos desde cualquier lugar con conexión a internet.**

2) **Selecciona un servidor de almacenamiento confiable:**

- **Reputación y confiabilidad: busca recomendaciones de confianza.**
- **Seguridad y encriptación: asegúrate de que el proveedor utilice medidas de seguridad robustas, como el cifrado de extremo a extremo, para proteger tus archivos.**
- **Políticas de privacidad: revisa las políticas de privacidad del proveedor para asegurarte de que cumplan con tus estándares de confidencialidad.**
- **Funcionalidades y capacidades: evalúa las funcionalidades y capacidades del servicio, como el espacio de almacenamiento ofrecido, la posibilidad de programar respaldos automáticos.**

Almacenamiento en la nube

1) **Ventajas:**

- **Accesibilidad: puedes acceder a tus archivos respaldados en cualquier momento y desde cualquier dispositivo con conexión a internet.**
- **Seguridad de los datos: los proveedores de almacenamiento en la nube suelen ofrecer altos niveles de seguridad y encriptación para proteger tus archivos.**
- **Respaldo automático: algunos servicios de almacenamiento pueden realizar respaldos automáticos.**

1) **Desventajas:**

- **Dependencia de la conexión a internet: para acceder a tus archivos es necesario tener una conexión a internet estable.**
- **Coste: algunos servicios pueden tener un coste de mantenimiento.**
- **Privacidad y confidencialidad: existe el riesgo de que los datos almacenados en la nube puedan ser vulnerado.**

Almacenamiento en la nube

1) **Pasos para realizar la copia de seguridad:**

- **Registro en el servicio.**
- **Identificación de los archivos a respaldar.**
- **Subir los archivos a la plataforma online.**
- **Organiza tus archivos para encontrarlos fácilmente.**
- **Verificar la copia de seguridad.**

Más clases y vídeos en: https://canalsenior.es

¡¡Muchas Gracias!!

CanalSénior

GOBIERNO DE ESPAÑA
MINISTERIO DE DERECHOS SOCIALES Y AGENDA 2030
POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL