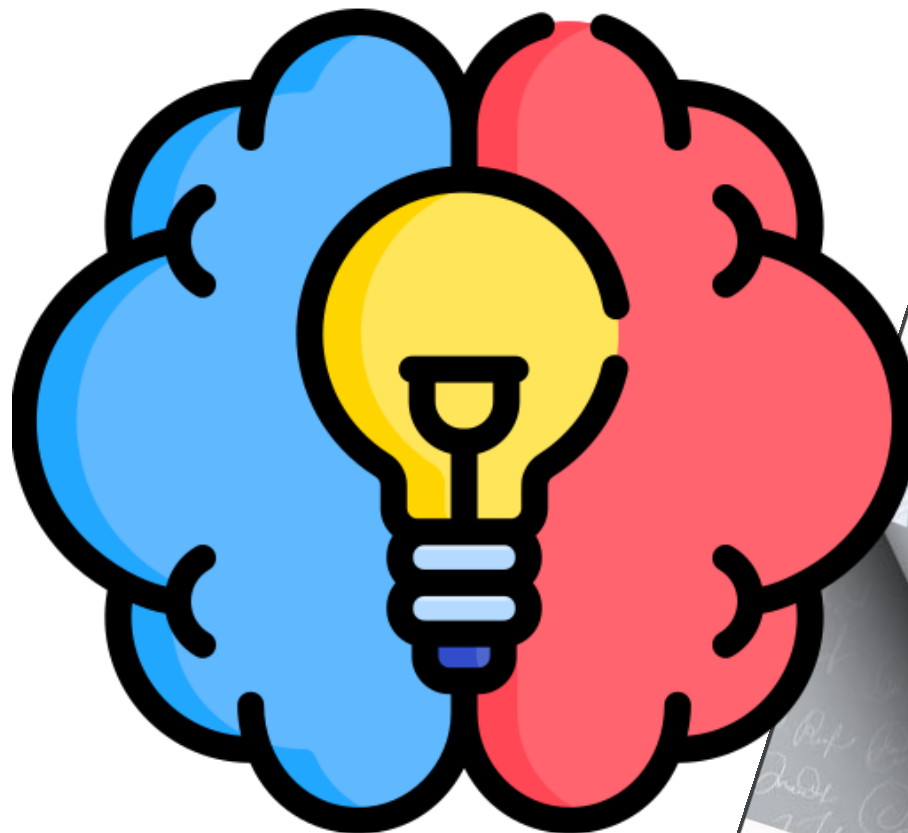


FIRMA ELECTRÓNICA EN PÍLDORAS



FIRMA ELECTRÓNICA EN PÍLDORAS



1. Punto de Emisión de Certificados



¿Punto de emisión de certificados en la propia organización?

- Flexibilidad e inmediatez emisión de certificados de empleado público.
- Oportunidad de dar servicio a ciudadanos. Reducción de la brecha digital.
- Alianza con prestadores de servicios electrónicos de confianza.

¿Qué tipo de certificados? ¿Unidad encargada?

- Certificados de empleado público: RR.HH.
- Certificados de ciudadano: OAMR.

¿Por qué no TIC/Informática?

- Certificados de empleado público: no son los encargados de la gestión de recursos humanos.
- Certificados de ciudadano: no es una unidad de atención al público.

¿Dónde Regulamos el Punto de Emisión de Certificados?

- Normativa de Uso de Sistemas de Información y recursos TIC
- Política de Firma Electrónica



Tomo II

4.3. Prestadores de Servicios de Confianza

Preguntas Frecuentes

En la localidad de la entidad donde trabajo no hay oficina en la que pueda presentarme para identificarme para la solicitud de emisión de un certificado digital ¿Puedo constituir en mi entidad una oficina de registro para la emisión de certificados? ¿Qué tipo de certificados se podrían emitir?



2. Gestión del ciclo de vida de los certificados



Ciclo de vida

- Emisión, Revocación y Caducidad.

Procedimientos

- El empleado se incorpora a la organización.
- El empleado cambia de puesto o cargo dentro de la organización.
- El empleado abandona la organización. Devolución de la tarjeta.
- Incidente de seguridad. Pérdida o compromiso de las credenciales.
- Identidad Digital de Cargos electos: ¿Emisión automática y revocación automática? ¿Es obligatorio incluir el cargo en el certificado digital?

¿Dónde Regulamos la Gestión del Ciclo de Vida de los Certificados?

- Normativa de Uso de Sistemas de Información y recursos TIC.
Procedimientos.
- Política de Firma Electrónica

Enciclopedia



Tomo I

5.2.2. Procesos de obtención

5.2.3. Responsabilidades

Tomo II

4.3. Prestadores de Servicios de Confianza

Preguntas Frecuentes

- ¿Por qué los Certificados Electrónicos tienen fecha de caducidad?
- ¿Qué significa revocar un Certificado? ¿Qué pasos he de seguir para revocar un certificado?



3. Definición del ámbito de uso de los certificados



Certificados de ciudadano o DNI electrónico

- ¿Permitimos su uso a los empleados públicos en sus actos administrativos?

Certificado de empleado público

- Permitimos para la identificación en webs dentro de su ámbito privado?
Ej. consulta de notificaciones personales, consulta de su vida laboral, acceso a plataformas de formación, etc.
- ¿Firma en el ámbito privado?
- La AGE sí restringe (Artículo 22. RD 1671/2009 – no derogado)

¡Certificado de representante!

¿Dónde Regulamos el ámbito de uso de los certificados?

- Ordenanza Reguladora de la Administración Electrónica.
- Política de Firma Electrónica

3. Definición del ámbito del certificado de representante



Nos los exigen otras Administraciones (el Representante no realiza personalmente el trámite): Catastro. Notificaciones PAG/060/DEH. TGSS. AEAT.

Representación total: Cuidado. Limitar el uso mediante decreto. Informar al empleado.

Alternativas a su uso

- Plataforma de Intermediación de Datos.
- Registro Electrónico de Apoderamientos (@podera/REA).

Medidas Técnicas: Gestión centralizada de Certificados

- Permiten el control y restricción del uso de los certificados, incluso a nivel de aplicación, URL de internet o franja horaria.
- Portabilidad identidad: disponible en cualquier dispositivo (PC, móvil,...)

Enciclopedia



Tomo I

5. Certificados. Tipos de Certificados

Tomo II

4.3. Prestadores de Servicios de Confianza

Preguntas Frecuentes

- ¿Cuáles son los certificados cualificados de mayor interés para una entidad o administración pública?
- ¿Qué certificado debe utilizar mi entidad para relacionarse con otras administraciones?
- Soy un empleado público ¿Qué certificado se requiere para consultar las notificaciones e información de mi entidad recogidas en la Carpeta del Punto de Acceso General?



4. Protegiendo la identidad digital y los certificados



Normas de uso de contraseñas y PIN

- No se comparten.
- Separación ámbito personal y laboral (contraseñas web, banco, tarjeta crédito).
- Contraseña de acceso al equipo diferente a la contraseña de las aplicaciones.
- Políticas de renovación de contraseñas.

Normas para el establecimiento de contraseñas seguras

- Fortaleza de contraseñas (importa más la longitud que los caracteres).
- Evitar patrones (miguel2019, miguel2020,...)
- Almacén de contraseñas.

Normas para el establecimiento de PIN seguro

- 0000, 1234, 9999, número de empleado, fechas “conocidas”
- Bloqueo al tercer intento fallido. PUK.

¿Dónde regulamos estos aspectos?

- Normativa de Uso de Sistemas de Información y recursos TIC
- Política de Firma Electrónica

Enciclopedia



Tomo I

5.2.3. Responsabilidades

Preguntas Frecuentes

- Cómo establecer o cambiar las contraseñas/PIN en certificados de diferentes sistemas operativos y navegadores.



5. Certificado de empleado en tarjeta criptográfica



PROS: Seguridad. Doble factor de autenticación. Portabilidad de la identidad digital (limitada)

CONTRAS: Gestión del certificado (entrega y renovación física). Uso en dispositivos en movilidad limitado (NFC). Coste: certificado + tarjeta + lector.

¿Dónde regulamos el uso del certificado en tarjeta criptográfica?

- Política de Firma Electrónica
- Viene determinado por la Categorización del Sistemas de Información (Esquema Nacional de Seguridad)

Medidas Técnicas: Gestión centralizada de Certificados

- Permiten el control y restricción del uso de los certificados, incluso a nivel de aplicación, URL de internet o franja horaria.
- Portabilidad identidad: disponible en cualquier dispositivo (PC, móvil,...)



Tomo I

6.1.3. Soportes Criptográficos y HSM

Preguntas frecuentes

- ¿Qué tipo de certificado de empleado público debemos utilizar en nuestra entidad?
¿Hardware o software?
- Preguntas relativas a la gestión de certificados en tarjeta criptográfica (PIN, desbloqueo, importación, etc.)



6. Firma biométrica



Es importante definir un buen sistema de CSV

- ¿CSV como localizador o como sistema de firma?
- Transparencia y Protección de Datos.
- Seguridad e interoperabilidad – Generación del código. Firma con sello de órgano
- Código QR / Código de barras – Suministro de lectores

¿ Como se respalda la autenticidad del documento CSV?

- Original + Firma + CSV

¿Debe incluir el NIF de los firmantes?

- Protección de Datos: minimización del tratamiento – Nombre, Apellidos y cargo.
- Pero... ¡Cuando se valida el CSV puedo comprobar la firma electrónica y ésta sí incluye el NIF!

¿Dónde regulamos el Sistema de CSV?

- Política de Firma Electrónica
- Ordenanza Reguladora de la Administración Electrónica

Enciclopedia



Tomo I

6.1.2. Soporte a la firma Biométrica y en movilidad

Glosario

Definición de firma biométrica



5. Sistema de CSV



Es importante definir un buen sistema de CSV

- ¿CSV como simple localizador o como sistema de firma? ENI – Tipo de firma
- Seguridad e interoperabilidad – Generación del código. Firma con sello de órgano
- Código QR / Código de barras – Suministro de lectores
- Transparencia y Protección de Datos.

¿ Como se respalda la autenticidad del documento CSV?

- Original + Firma + CSV

¿Debe incluir el NIF de los firmantes?

- Protección de Datos: minimización del tratamiento – Nombre, Apellidos y cargo.
- Criterio Interpretativo AEPD de 23 de julio de 2015.
- Pero... ¿Cuando se valida el CSV puedo comprobar la firma electrónica y ésta sí incluye el NIF!

¿Dónde regulamos el Sistema de CSV?

- Política de Firma Electrónica
- Ordenanza Reguladora de la Administración Electrónica

Enciclopedia



Tomo I

7 Procesos de firma y Política de Firma e identidad digital. CSV.

9.5. Códigos Seguros de Verificación

Preguntas Frecuentes

- ¿Qué se entiende por un documento con CSV?
- ¿Cómo se valida un documento con CSV?
- ¿Se debe superponer una firma de sello electrónico a un documento con CSV?

