Buena Práctica de Calidad y PRL

Uso para identificación y firma electrónica reconocida de tarjeta criptográfica con certificado de empleado público en el SAS.

Mayo 2021

Descripción de la tarea

En la actualidad, dentro del Servicio Andaluz de Salud, para la identificación electrónica y la firma de documentos en formato electrónico por parte de los profesionales es habitual el uso de certificados electrónicos, incluyendo el de firma electrónica reconocida emitidos por un prestador de servicios de certificación (por ejemplo, en el caso de la fábrica nacional de moneda y timbre -FNMT-). Según la norma de referencia (Ley 59/2003) se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma, teniendo está el mismo valor en relación a los datos consignados en forma electrónica que la firma manuscrita en relación a los consignados en papel.

Dada la importancia de que una firma electrónica reconocida se genere en un entorno seguro, pero igualmente que se utilice también en un entorno con las mayores garantías de seguridad posibles, en nuestra UPRL decidimos analizar las pautas actuales en las que la mayoría de los profesionales de nuestro entorno utilizan certificados de firma electrónica, que si son personales, pueden ser utilizados tanto en el entorno laboral como para actividades privadas, teniendo en cuenta que en numerosas ocasiones estos certificados se INSTALAN en ordenadores que escapan a su control (por ejemplo en el caso de uso del sistema de información eCO para comunicaciones interiores, se nos indicaba que se requiere la instalación del certificado en el navegador web), dado que la Organización limita muchas capacidades de los equipos lógicamente para salvaguardar la seguridad de los datos en ellos contenidos, y existiendo en ocasiones copias de seguridad de este contenido que escapan igualmente al control de los usuarios de los equipos, siendo estos equipos informáticos controlados incluso por profesionales de empresas externas al SAS (no obstante sujetos a sigilo profesional y con las debidas condiciones de seguridad).

Solución adoptada

Preocupados por conseguir las mejores condiciones de seguridad razonables, en la firma electrónica de documentos, en el uso de certificados de identificación y para la generación de firmas electrónicas reconocidas, realizamos una consulta al Instituto Nacional de Ciberseguridad de España (INCIBE), sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital, como entidad nacional de referencia, solicitando información sobre la conveniencia o no de utilizar certificados digitales PERSONALES instalables en equipos informáticos para temas laborales dentro de una empresa pública (SAS), a lo que nos respondieron que se trataba de una práctica poco adecuada, al generar peores condiciones de seguridad en cuanto a protección de datos personales y firma electrónica de documentos, siendo la opción más adecuada para este caso concreto (empleados públicos y uso de certificados en el entorno laboral) la disponibilidad y uso de una TARJETA CRIPTOGRÁFICA CON CERTIFICADO DE EMPLEADO PÚBLICO, de uso específico para actuar como profesional al servicio de la Administración Pública (y no para uso personal, salvo para relaciones con administraciones públicas cuando estas lo permitan)indicándonos como referencia para mayor información en cuanto a los pasos para obtener un certificado de empleado público a la entidad CERES(entidad pública de certificación).

Desde nuestra UPRL realizamos consulta por escrito a la entidad CERES (24/03/2021) solicitando información en relación a los requisitos necesarios para la obtención del certificado de empleado público,

respondiéndonos la citada entidad que en el caso de que los registradores habilitados no tuviesen activa la política para acreditar los certificados de empleado público (preguntamos en nuestro centro a los responsables de emitir certificados de este tipo y parece que así era) estos podrían activar dicha opción enviando cumplimentado el modelo 070 y solicitando esa activación al área de registro de CERES por correo electrónico a la siguiente dirección: **registroceres@fnmt.es**

El modelo de formulario 070 se puede obtener a la fecha de emisión de este documento en la siguiente dirección web:

https://www.cert.fnmt.es/registro/documentacion-general-registro/formularios/relacion-de-formularios

Adicionalmente CERES nos indicó que el mayor nivel de seguridad (recomendable) se consigue descargando directamente el certificado una vez emitido por la entidad de certificación en la tarjeta criptográfica, en lugar de hacerlo en un ordenador y posteriormente exportando el mismo a la tarjeta criptográfica (opción menos recomendable, ya que se perdía la seguridad asociada al hecho de que la clave privada no hubiese salido de la tarjeta). El actual proceso de obtención del certificado por cada persona trabajadora, permite la descarga directa en la tarjeta criptográfica.

Las tarjetas criptográficas pueden adquirirse directamente a través de la web de CERES, estando disponibles a la fecha de emisión de este documento en la siguiente dirección web (compra obligatoria mediante página web para un número inferior a 300):

https://tienda.fnmt.es/fnmttv/fnmt/es/Productos/Tarjetas-y-Lectores/c/6000

Para completar nuestro análisis realizamos una consulta a una asesoría jurídica especializada en temas laborales, que nos confirmó que la indicación de INCIBE era muy conveniente, y que el enfoque (justificación legal) para solicitar/exigir (en caso de necesidad de de uso de certificados digitales para temas laborales), la disponibilidad de tarjeta criptográfica con certificado de empleado público era hacer alusión a la ley de protección de datos (personales).

Resultados o consecuencias de la implantación de la Buena Práctica

Dada la situación actual en la que al menos una amplia mayoría de profesionales del SAS de entre los que utilizan habitualmente certificado digital utiliza certificados digitales PERSONALES para la identificación y firma electrónica de documentos de carácter laboral, en lugar de certificados de empleado público instalados en tarjetas criptográficas, hemos solicitado el traslado de este tema al seno del Comité de Seguridad Interior y Seguridad de las Tecnologías de la Información y Comunicaciones del Servicio Andaluz de Salud recientemente creado (Resolución 26 marzo 2021 de la Dirección Gerencia del Servicio Andaluz de Salud).

Como conclusión de nuestra análisis, y enfocando siempre el tema a la generación de documentos con firma electrónica reconocida relacionados con la prevención de riesgos laborales en el seno del Servicio Andaluz de Salud, pensamos que a todos los profesionales de servicios de prevención del Servicio Andaluz de Salud se les debería dotar de tarjeta criptográfica con certificado de empleado público en la que dicho certificado se hubiese instalado directamente en la tarjeta.(Esta última opción es controlable por la persona que va a utilizar la tarjeta en el proceso de obtención del certificado según nos comentan).

Estamos valorando elevar una consulta al delegado de protección de datos del Servicio Andaluz de Salud a través de su buzón de consultas.

Estado en el que se encuentra la Buena práctica

En proyecto.

Autoría: Jose Antonio Garrido Muñoz
Área de Gestión Sanitaria Sur de Córdoba