PROCEDIMIENTO DE PROTECCIÓN DE LA INFORMACIÓN

Índice

CONTROL DE REVISIONES

VERSIÓN	DESCRIPCIÓN DE CAMBIOS	ELABORADO
1.0	Primera versión del documento	19/06/2020
2.0	Actualización del documento	24/03/2022
3.0	Actualización al RD311/2023	12/12/2023

1 Objeto

El objeto de este procedimiento es definir las medidas de seguridad necesarias para la protección de la información, de acuerdo a lo previsto en las siguientes medidas del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

- op.exp.10 Protección de claves criptográficas
- mp.info.3 Firma electrónica
- mp.info.5 Limpieza de documentos
- mp.info.6 Copias de seguridad

2 Alcance

Este procedimiento aplica a toda la información que interviene en la prestación de servicios de RADMAS TECHNOLOGIES, así como a todos aquellos que tengan acceso a la misma.

3 Referencias

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Política de Seguridad de la Información de RADMAS TECHNOLOGIES.

4 Responsabilidades

Será responsabilidad del Responsable de Seguridad:

- Velar por el efectivo cumplimiento de lo indicado en el presente procedimiento.

Será responsabilidad de los usuarios:

- Llevar a cabo las actuaciones previstas en este procedimiento para la protección de la información.

5 Procedimiento

5.1 Protección de claves criptográficas

La política de uso de los controles criptográficos de **RADMAS** se basa en asegurar la protección de acceso a sistemas, datos y servicios, así como la transmisión de información fuera del ámbito de **RADMAS**. A continuación, se define la política de uso de controles criptográficos.

Las claves criptográficas se protegerán durante todo su ciclo de vida:

- Generación
- Transporte al punto de explotación
- Custodia durante la explotación
- Archivo posterior a su retirada de explotación activa
- Destrucción final

En el caso de la generación de claves criptográficas, los medios utilizados deberán estar aislados de los medios de explotación.

Las claves criptográficas retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación.

Se usarán programas evaluados o dispositivos criptográficos certificados.

Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

Las claves criptográficas empleadas en **RADMAS** son:

a) Cifrados web: certificados SSL adquiridos.

b) Uso de firma electrónica para trámites con la AAPP.

c) Cifrado de comunicaciones: cifrado VPN y cifrado de la Wifi.

d) Cifrado de contraseñas del producto.

e) Claves SSH para el acceso remoto a servidores.

- **Certificados Web:**

Para garantizar la seguridad de las páginas Web publicadas por la organización, así como las aplicaciones web desarrolladas, se hará uso de certificados Web SSL.

Los certificados SSL son siempre adquiridos, en concreto:

- Certificado SSL wildcard para el dominio *.mejoratuciudad.org expedido por una entidad certificadora de confianza (COMODO).

La responsabilidad de mantener vigentes estos certificados es del Responsable de Seguridad.

- **Uso de firma electrónica**:

Se hará uso de la firma electrónica en aquellos escenarios en los que sea imprescindible garantizar la autenticidad y el no repudio de la información, como para realizar trámites con las Administraciones públicas.

La organización dispone de certificados de firma electrónica para:

- Representante

El proveedor de estos certificados es la Fábrica Nacional de Moneda y Timbre (FNMT) y deberán ser renovados cada 2 años.

Las firmas electrónicas se encontrarán instaladas en PC seleccionados y especialmente protegidos para evitar su uso indebido.

- **Cifrado de comunicaciones**:

Se cifrarán las siguientes comunicaciones realizadas:

- Acceso desde el exterior mediante VPN cifrada que garantizan la confidencialidad e integridad de las comunicaciones.

- Cifrado de la Wifi de la empresa mediante el estándar seguro WPA2.

- **Cifrado de contraseñas de producto**:

Todas las contraseñas de los usuarios del producto se almacenan de forma segura utilizando algoritmos de cifrado robustos. Este tratamiento garantiza que las credenciales no sean almacenadas o expuestas en texto plano, protegiéndolas frente a accesos no autorizados.

- **Claves SSH para acceso a servidores**:

El acceso remoto a la infraestructura de servidores por parte del personal autorizado se realiza exclusivamente mediante el uso de claves SSH nominales.

5.2 Firma electrónica

La firma electrónica es un mecanismo de prevención del repudio; es decir, previene frente a la posibilidad de que en el futuro el signatario pudiera desdecirse de la información firmada. Se empleará la firma electrónica como un instrumento capaz de permitir la comprobación de la autenticidad de la procedencia y la integridad de la información ofreciendo las bases para evitar el repudio.

La firma electrónica garantiza la autenticidad del signatario y la integridad del contenido.

RADMAS TECHNOLOGIES adopta la **Política de Firma Electrónica y de Certificados** de la Administración General del Estado (AGE), versión 1.9. Puede consultarse en el siguiente enlace la política de firma y una guía rápida de aplicación:

https://administracionelectronica.gob.es/ctt/politicafirma/descargas#.XLAwRZgzZ1s

Se emplean certificados de representante emitidos por la FNMT-RCM (Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda) y únicamente para trámites con la Administración.

5.3 Limpieza de documentos

Se retira de todos los documentos a publicar o enviar fuera de RADMAS TECHNOLOGIES, toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.

Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorio de información.

Se tendrá presente que el incumplimiento de esta medida puede perjudicar:

- Al mantenimiento de la confidencialidad de información que no debería haberse revelado al receptor del documento.
- Al mantenimiento de la confidencialidad de las fuentes u orígenes de la información, que no debe conocer el receptor del documento.
- A la buena imagen de la organización que difunde el documento por cuanto demuestra un descuido en su buen hacer.

En el caso de documentos ofimáticos, se utilizan las propias herramientas de la suite ofimática utilizada para realizar la limpieza de la meta información.

En el caso de aplicaciones que generen documentos electrónicos, se considerará este aspecto en la especificación de requisitos, de acuerdo a lo previsto en el procedimiento "**PO.SEG.04 Desarrollo de Software**".

El Responsable de Seguridad de **RADMAS**, se encargará de formar al usuario al respecto a través de la distribución de la instrucción técnica: **ITS-PO.SEG.1501 Borrado de metadatos**.

5.4 Proceso de copias de seguridad

5.4.1 Realización de copias de seguridad

Con el objetivo de recuperar datos perdidos accidental o intencionadamente, en **RADMAS** se realizan copias de seguridad periódicamente.

La frecuencia con la que se deben realizar las copias se ha definido en función de la sensibilidad de las aplicaciones, de los datos o de los clientes. Dicha periodicidad se ha determinado sobre la base de las consecuencias que tendría la pérdida de la información.

Como norma general, las copias de seguridad de **RADMAS** abarcarán:

- Información de trabajo de la organización.
- Aplicaciones en explotación, incluyendo los sistemas operativos.
- Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.
- Claves utilizadas para preservar la confidencialidad de la información.

5.4.2 Política de copias de seguridad

Con el objetivo de establecer los criterios de copia de seguridad apropiados a cada sistema de información, **RADMAS** define la siguiente política de copias de seguridad:

- **Documentación en Google Drive**
  - Las copias de seguridad de la información contenida en Google Drive son responsabilidad del proveedor Google, que cuenta con una certificación en ENS nivel alto para dicho servicio.
- **Amazon**
  - Copias de seguridad diarias de la BBDD de la aplicación MTC.
  - Para la copia de seguridad de la base de datos se utiliza la herramienta Mongodump. Se ejecuta todos los días a las 4:00h

- **DockerHub**
  - Imágenes guardadas periódicamente de los servidores.
- **SonicWall**
  - Copia de seguridad en el propio equipo
- **Bitbucket**
  - Las copias de seguridad de la información contenida en Bitbucket (código fuente) son responsabilidad del proveedor.
- **Equipos de usuario:**
  - No se realizará copia de los documentos locales de usuarios.

En la definición de esta política de copias de seguridad se cuenta, en cualquier caso, con la colaboración de las distintas áreas de **RADMAS**, especialmente en lo concerniente a la periodicidad de las copias.

El Responsable de Seguridad, con una periodicidad anual, realiza una revisión de la Política de Copias de Seguridad para determinar si es necesario reajustarla, por motivo de cambios en la actividad o su entorno.

5.4.3 Pruebas de restauración

El personal asignado por el Responsable del Sistema verifica diariamente que las diversas operaciones de copia de seguridad realizadas se han producido de la forma, con la precisión y en el tiempo esperado.

Además, semestralmente, se realiza una prueba de restauración de la última copia de seguridad realizada para verificar que el mecanismo implantado funciona correctamente.

El registro de la realización de las pruebas de restauración se plasma en el Jira.

6 Anexos

- ITS-PO.SEG.1501 Borrado de metadatos