ANEXO VI

USO DE HERRAMIENTAS CRIPTOGRÁFICAS

1. OBJETIVO

Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, no repudio, la autenticidad e integridad de la información, así como establecer una adecuada gestión de claves.

2. ALCANCE

Comprende toda la información del Organismo que por su clasificación requiere de mecanismos adicionales de seguridad, tanto si se encuentra almacenada como cuando es transmitida.

3. DEFINICIONES

Certificado Digital: autentica la identidad de un sitio web y habilita una conexión cifrada. Por ejemplo, existen los certificados SSL, cuya sigla significa *Secure Sockets Layer*, un protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web.

Cifrado: proceso para convertir información en un formato ilegible aplicando un algoritmo criptográfico. Se utiliza para proteger la información de la divulgación no autorizada.

Claves criptográficas: es una cadena de bits utilizada por un algoritmo criptográfico para transformar texto plano en texto cifrado o viceversa.

Claves privadas o secretas: es una técnica de cifrado (criptografía simétrica) que utiliza llaves diferentes para cifrado y descifrado, lo que permite que las computadoras se comuniquen de forma segura, entre sí, a través de Internet.

Claves públicas: es una técnica de cifrado (criptografía asimétrica), que se generará de forma que vincule de manera única la información relativa a la/el propietaria/o del par de claves pública/privada con la clave pública cuando cada usuaria/o tiene un par de claves: una (1) clave pública (que puede ser revelada a cualquier persona) utilizada para cifrar y una (1) clave privada (que debe mantenerse en secreto) utilizada para descifrar. Las claves asimétricas utilizadas para cifrado no deben ser las mismas que se utilizan para firmar digitalmente.

Controles criptográficos: conjunto de técnicas criptográficas para proteger información sensible y confidencial ya sea en tránsito o cuando está almacenada, tales como bases de datos, registros de usuarios, backups, credenciales de acceso y para pagos online, entre otros, que puedan ubicarse en computadoras, dispositivos extraíbles y en teléfonos móviles.

Criptografía: técnica que consiste en cifrar un mensaje (texto en claro) convirtiéndolo en un mensaje cifrado o criptograma que resulta ilegible para todo aquel que no conoce la clave para descifrar el mensaje.

Firma Digital: es una solución tecnológica, segura y confiable que permite firmar digitalmente documentos electrónicos. Es el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su control absoluto. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

4. RESPONSABILIDADES

El Responsable de Seguridad de la Información (RSI) deberá definir los métodos de encriptación a utilizarse, de acuerdo a la criticidad de la información.

El RSI deberá gestionar el sistema de claves criptográficas y elaborar procedimientos necesarios para la efectiva gestión de dichas claves.

La Subgerencia de Sistemas (S.S.) colaborará en la definición de los métodos de encriptación a ser utilizados de acuerdo a la criticidad de la información. Asimismo, coordinará la implementación de las medidas de encriptación definidas previamente.

Asimismo, la S.S. deberá implementar procedimientos para la asignación de firma digital al personal de la S.R.T., de conformidad con la normativa vigente.

5. CONTENIDO

5.1 PROTECCIÓN DE LA INFORMACIÓN MEDIANTE TÉCNICAS DE CIFRADO

5.1.1 Definición y uso de técnicas de cifrado

Se deberán definir y establecer mecanismos de claves criptográficas, teniendo en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar, con el fin de adicionar medidas de seguridad sobre aquella información que lo requiera.

En esa línea, se deben implementar técnicas criptográficas en los siguientes casos, cuando el nivel de protección sea requerido:

- Para la protección de claves de acceso a dispositivos, datos y servicios;
- Para la transmisión de información, fuera del ámbito de la S.R.T.;
- Para el resguardo de información, incluyendo los dispositivos que le dan soporte;
- Para todos los sitios web del Organismo, utilizando certificados digitales.

Por último, se deben considerar los controles aplicables a la exportación e importación de tecnología criptográfica y establecer procedimientos respecto de la administración de claves.

5.1.2 Protección de claves criptográficas

Se deberá implementar un sistema de administración de claves para gestionar el ciclo de vida de las claves criptográficas.

Respecto a la protección de las mismas durante su uso, se deberán considerar los siguientes lineamientos:

- Todas las claves deben ser protegidas contra modificación y destrucción;
- Las claves secretas y privadas deben ser protegidas contra copia o divulgación no autorizada;
- Se debe proporcionar una protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves.

Además de la administración segura de las claves secretas y privadas, deberá tenerse en cuenta la protección de las claves públicas mediante el uso de su correspondiente certificado. Se deberán establecer los lineamientos necesarios para:

- Generar claves diferenciadas de acuerdo al tipo de información y para los dispositivos que las albergan;
- Implementar la normativa vigente respecto a firma digital.

Asimismo, se deberán elaborar procedimientos que se desprendan del sistema de gestión de claves, que consideren los siguientes aspectos:

- Distribuir claves de forma segura a las/los usuarias/os que corresponda, incluyendo información sobre cómo deben activarse cuando se reciban;
- Almacenar claves, incluyendo la forma de acceso a éstas por parte de las/los usuarias/os autorizadas/os;

- Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las mismas;
- Revocar claves, incluyendo cómo deben retirarse o desactivarse, por ejemplo, cuando las claves están comprometidas o cuando un empleado se desvincula de la S.R.T. (en cuyo caso las claves también deben archivarse);
- Recuperar claves pérdidas o alteradas como parte de la administración de la continuidad de las actividades de la S.R.T., por ejemplo, para la recuperación de la información cifrada;
- Archivar claves, por ejemplo, para la información sensible archivada o resguardada;
- Destruir claves;
- Registrar y controlar las actividades relativas a la administración de claves.

5.1.3 Firma digital

Las firmas y certificados digitales se rigen por la legislación nacional vigente (Ley de Firma Digital Nº 25.506), que determina las condiciones bajo las cuales una firma digital es legalmente válida.

Por ello se deberá respetar y aplicar los recaudos establecidos por la normativa citada para proteger la confidencialidad de las claves privadas. Asimismo, es importante proteger la integridad de la clave pública mediante el uso de un certificado de clave pública. Dichas claves deben ser resguardadas bajo el control exclusivo de su titular.

Por último, se deberán elaborar los procedimientos correspondientes para la adquisición de la firma digital para el personal de la S.R.T. que así lo requiera.

República Argentina - Poder Ejecutivo Nacional
1983/2023 - 40 AÑOS DE DEMOCRACIA

Hoja Adicional de Firmas
Anexo firma conjunta

Número: IF-2023-66578558-APN-GT#SRT

CIUDAD DE BUENOS AIRES
Viernes 9 de Junio de 2023

Referencia: ANEXO VI Uso de Herramientas Criptográficas-EX-2023-56789749-APN-GT#SRT

El documento fue importado por el sistema GEDO con un total de 4 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:39:51 -03:00

Diego Maximiliano Segovia
Subgerente
Subgerencia de Sistemas
Superintendencia de Riesgos del Trabajo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:45:46 -03:00

Marcelo Angel Cainzos
Gerente
Gerencia Técnica
Superintendencia de Riesgos del Trabajo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:45:48 -03:00