intiza

Norma de Cifrado de la Información

Versión: 1.1

Confeccionó	Revisó	Aprobó
BDO **Consultoría Externa**	 **Carla Leiva - CISO**	 **Francisco Canale - Director**

NORMA DE CIFRADO DE LA INFORMACIÓN	intiza Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 10/07/2024
Código: NO-SI-20- Cifrado de la Información	Versión: 1.1

Contenido

1. Objetivo **3**

2. Alcance **3**

3. Responsabilidades **3**

4. Desarrollo **3**

4.1. Generalidades 4

4.2. Cifrado de datos en reposo 5

4.3. Cifrado de Datos en tránsito 5

4.4. Algoritmo de Cifrado 6

5. Referencias **7**

5.1. Normativa Relacionada 7

5.2. Definiciones 7

6. Historial de Versiones **8**

1. Objetivo

Establecer los lineamientos de la Administración de Cifrado de la Información y Claves Criptográficas con el fin de asegurar una gestión y mantenimiento de la información crítica y datos personales de INTIZA, según la clasificación de información.

2. Alcance

Este documento abarca la gestión de Cifrado de la información de INTIZA, gestión de claves de cifrado y otros sistemas que requieren administración de Claves Criptográficas.

3. Responsabilidades

Seguridad de la Información es la responsable de controlar y monitorear la gestión de claves de cifrado.

Gerente de Tecnología es el responsable de la generación, distribución, almacenamiento o la delegación de la gestión de claves de cifrado.

4. Desarrollo

Se denomina cifrar al proceso mediante el cual un texto legible, denominado “texto en claro”, se transforma en “texto cifrado”, el cual resulta ilegible para quienes no se encuentren autorizados a acceder a él. Para llevar adelante este proceso, se utiliza una clave secreta.

Las herramientas criptográficas en consiguiente protegen las transacciones y los documentos de ser visualizados o accedidos para un eventual tratamiento, por terceros no autorizados.

Descifrar en contraposición, es el proceso que tiene lugar para restablecer el texto cifrado a su estado inicial, es decir como texto en claro, permitiendo que sea visto y accedido para su

eventual tratamiento. Para ello también se requiere el uso de una clave secreta. Para ambos procesos se utiliza un algoritmo.

Una vez cifrada, dicha información sólo podrá ser visualizada o accedida si se utiliza dicha clave, que debe conocer tanto el que cifra como el que descifra. De esta manera, se pueden utilizar los siguientes mecanismos de criptografía:

- Criptografía Simétrica: La criptografía simétrica se caracteriza entre otros aspectos, por utilizar una única clave, que puede ser un número, una palabra o un conjunto de caracteres resultado del azar. La clave debe ser conocida tanto por el emisor como por el receptor del dato y se la utiliza tanto para cifrar como para descifrar.
- Criptografía asimétrica: La criptografía de clave pública o asimétrica es aquella que utiliza dos claves diferentes para cada usuario, denominadas “clave pública” y “clave privada''.
- Uso de Hashes o Digestos: Un uso particular de la criptografía lo representan los hashes o digestos. Se trata de una función diseñada para tomar un conjunto o “string” de datos de cualquier tamaño y tipo y producir a partir de él, un nuevo string de longitud fija, denominado “hash”, el cual se encuentra relacionado con el conjunto inicial, de modo tal que cualquier modificación que se le haga, provoca un cambio en dicho hash.

4.1. Generalidades

- Deberá existir una gestión de Cifrado y claves criptográficas para asegurar que toda la información confidencial de la compañía se encuentre protegida y con los accesos a la misma solo a los usuarios autorizados.
- Se debe tener en cuenta el nivel de protección requerido por la información para establecer el tipo, la robustez y la calidad del algoritmo de cifrado que se utilizará para dicha protección.

- Métodos de protección apropiados para resguardar las claves de cifrado y para la recuperación de información cifrada en caso de pérdida o daño de las claves utilizadas.
- Todos los datos confidenciales o que contengan datos personales y se almacenen en medios extraíbles se deben cifrar en cualquier lugar donde se almacenen.
- Se debe restringir el acceso a las claves criptográficas a la menor cantidad de custodios necesarios.

4.2. Cifrado de datos en reposo

- Cuando hablamos de “datos en reposo”, nos referimos a información que permanecerá en un medio específico como ser: magnético, óptico, etc. Implica entonces que no están siendo transferidos de un lugar a otro.
- Los datos que se encuentran en reposo y se consideren confidenciales o críticos para INTIZA deben permanecer cifrados mientras se encuentren almacenados en un medio específico, como, por ejemplo, una computadora, servidor o un dispositivo móvil o extraíble o la nube.

4.3. Cifrado de Datos en tránsito

- Siempre que se transmita información y más aún si se trata de datos personales y/o confidenciales tanto de la compañía como de sus clientes, es necesario cifrarlos y protegerlos para asegurar que no sean interceptados por personas mal intencionadas o vulnerables a ataques.
- El cifrado de extremo a extremo protege los mensajes en tránsito desde el remitente hasta el receptor. Garantiza que la información sea transformada por el remitente original en un mensaje secreto (el primer "extremo") y que sólo pueda ser decodificado por su destinatario final (el segundo "extremo").

4.4. Algoritmo de Cifrado

- Las claves criptográficas deberán estar protegidas contra modificación, pérdida y destrucción. Asimismo, las claves secretas y privadas requieren protección contra divulgación no autorizada de las mismas.
- Los activos de TI que sean utilizados para generar, almacenar y archivar las claves debe ser protegido contra accesos no autorizados.
- Deberá existir un proceso de Administración de claves que permita:
  - Generar claves para su utilización en diferentes aplicaciones;
  - Generar y obtener certificados de clave pública y privada;
  - Solicitar claves;
  - Cambiar o actualizar claves incluyendo un procedimiento de cómo deben ser modificadas las mismas;
  - Almacenamiento de claves;
- Algoritmo utilizado por Microsoft Azure para los servidores cloud:

Algoritmo de Encriptación	Longitud mínima de clave aceptable
AES	256 bits

- Algoritmo utilizado por BitLocker de Microsoft para equipos portátiles :

Algoritmo de Encriptación	Longitud mínima de clave aceptable
AES-CBC	128 bits
AES-CBC	256 bits
XTS-AES	128 bits
XTS-AES	256 bits

- Proceso de administración de claves
- Generación de claves de cifrado: se debe asegurar que las claves de cifrado que se generen sean sólidas.

- Distribución segura de claves de cifrado: se debe asegurar que la administración de claves especifique cómo distribuir las claves de manera segura.
- Almacenamiento seguro de claves de cifrado: se debe asegurar que la administración de claves especifique cómo almacenar claves de manera segura.

5. Referencias

5.1. Normativa Relacionada

Categoría	Título	Código
N/A	N/A	**N/A**

5.2. Definiciones

Término	Descripción
Cifrar	El cifrado o encriptación de datos, es un método de seguridad que permite la codificación de datos mediante el uso de algoritmos matemáticos, elevando el nivel de seguridad y confidencialidad. Generalmente esta técnica se realiza mediante el uso de una clave, de modo que los datos cifrados, no sean legibles para quienes no posean dicha clave. Esta técnica protege la información sensible de una organización, evitando la fuga de información o interceptación de datos.
Cifrado Simétrico	Es un método criptográfico que utiliza una misma clave tanto para cifrar como para descifrar, la cual debe ser intercambiada mediante un canal seguro.
Cifrado Asimétrico	Es el método criptográfico que utiliza un par de claves. Ambas claves pertenecen al mismo usuario, una de ellas llamada “clave pública” que puede ser entregada a cualquier persona, mientras

	que la otra “clave privada” que debe ser resguardada y solo conocida por el propietario. Una de sus características principales es que lo cifrado con la clave pública puede ser descifrado con la privada y viceversa.

6. Historial de Versiones

Versión	Fecha	Resumen de Cambios
1.0	21/01/2022	Creación de la norma de Cifrado de la Información.
1.0	06/06/2022	Aprobado por Comité de Dirección: MI-DI-04 Minuta de Comité de Dirección N° 4.
1.1	27/06/2024	Se revisó el documento, se modificó tipo de letra calibri en todo el documento. Se agregó clasificación del documento en el encabezado y se eliminó del pie de página. Se reclasificó el documento a “Restringido”.