POLÍTICAS DE CONTROLES CRIPTOGRÁFICOS

FIRMAS DE REVISIÓN Y APROBACIÓN

	Nombre y Apellido / Cargo	Firma
Elaborado por:	Ing. Geovanny Meza, Mg. **Analista de Tecnologías de la Información 3**	Firmado electrónicamente por: JORGE GEOVANNY MEZA MORALES
Revisado y aprobado por:	Ing. Patricio Padrón **Director de Tecnologías de la Información y Comunicación**	Firmado electrónicamente por: NARDO PATRICIO PADRON CORREA

ÍNDICE

1. Notas de Cambio

Versión	Fecha	Detalle de la modificación
1	29/10/2021	Creación de la política

2. Antecedentes

El Esquema Gubernamental de Seguridad de la Información (EGSI), establece una serie de hitos que contemplan la elaboración, implementación y difusión, de políticas, procedimientos, reglamentos, normas y demás instrumentos técnicos, que garanticen el manejo seguro de la información de las instituciones públicas.

El empleo de elementos criptográficos que permitan garantizar la seguridad de la información, es una práctica común y altamente recomendad en la actualidad; por lo que, establecer políticas claras en base a las cuales efectuar la codificación o cifrado y la decodificación o descifrado de la información considerada susceptible, es de extrema importancia para la institución.

3. Alcance

Las presentes políticas son de cumplimiento obligatorio para las diferentes gestiones de la Dirección de Tecnologías de la Información y Comunicación, de manera particular, la gestión de Diseño e Implementación de Soluciones Informáticas.

4. Propósito

Normar, a través de políticas, el empleo de controles criptográficos para garantizar la seguridad de la información.

5. Definiciones

- **Codificación de información:** Método que permite representar la información utilizando un conjunto de símbolos que se combinan siguiendo determinadas reglas, para ocultar la información y evitar su manipulación.
- **Controles criptográficos:** Formas de codificar información para que no pueda ser alterada, interpretada o dañada, para posteriormente decodificarla y que se presente íntegra y tal cual es.

- **Contraseña:** Código secreto compuesto por una cadena de caracteres que pueden ser especiales y alfanuméricos, que se introduce en un sistema, equipo informático o red para iniciarlo y acceder para operarlo.
- **Credenciales de acceso:** Son el nombre de usuario y contraseña gestionados que dan acceso a un sistema o equipo.
- **Criptografía:** Arte y técnica de escribir con procedimientos o claves secretas o de un modo enigmático, de tal forma que lo escrito solamente sea inteligible para quien sepa descifrarlo.
- **Decodificación de información:** Proceso contrario a la codificación.
- **Sistemas de software:** Programas informáticos diseñados con el propósito de facilitar a los usuarios la realización de determinadas tareas.
- **Red de computadores:** conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.).
- **Usuario:** Nombre o identificador compuesto por una cadena de caracteres alfanuméricos, que emplea una persona para identificarse en un sistema, equipo o red, previo a ingresar la contraseña.

6. Políticas

- Los controles criptográficos se usarán única y exclusivamente en los siguientes casos:
    - Protección de claves de acceso a sistemas, información, datos y servicios.
    - Transmisión de información catalogada como sensible.
    - Resguardo de información.
- La Dirección de Tecnologías de la Información y Comunicación, a través de las diferentes gestiones que la conforman, deberá realizar una política o procedimiento para la gestión de claves; otra para la transmisión de información; y, una para el resguardo de información.
- La programación para el cifrado y descifrado de información, claves, datos, etc., deberá ser efectuada única y exclusivamente por el personal de la gestión de

Diseño e Implementación de Soluciones Informáticas de la Dirección de Tecnologías de Información y Comunicación.

- Todo software de codificación y decodificación que se use en la institución, deberá contar con el aval y autorización de la Dirección de Tecnologías de la Información y Comunicación.
- Los gestores o administradores de sistemas informáticos institucionales, serán responsables de la activación, recepción, protección de las llaves/claves criptográficas públicas y privadas de los sistemas institucionales; además, deberán proteger todas las llaves/claves contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada.
- Los gestores o administradores de sistemas informáticos institucionales, deberán generar claves para diferentes sistemas criptográficos y diferentes aplicaciones incluyendo fechas de inicio y caducidad de las claves, así como generar y obtener certificados de claves públicas.
- Los responsables de las llaves/claves criptográficas deberán almacenar las llaves de forma segura, y se comprometerán a restringir el acceso sólo a los usuarios autorizados. De igual forma, una copia de las llaves (si esta existe) deberá ser almacenada en sitio seguro para su recuperación en caso tal que esta se extravíe.
- El cambio o actualización de las llaves/claves deberá ser solicitado por el personal responsable o quien haga su uso.
- El oficial de seguridad de la información deberá incorporar funcionalidad para recuperar claves perdidas o corruptas, como parte de la gestión de continuidad de los servicios informáticos.
- Las llaves/claves serán revocadas y/o destruidas si lo considera pertinente el oficial de seguridad de la información o persona delegada, cuando exista sospecha de que pudieron ser accedidas por una persona no autorizada, o cuando el colaborador culmine su relación con la institución.
- Para todas y cada una de las actividades pertenecientes a la administración, gestión y eliminación de las llaves/claves criptográficas, se deberá mantener registro de las actividades realizadas en una bitácora a manera de reporte.

- Los sistemas que actualmente cuenten con algún mecanismo de cifrado deberán acogerse a la presente política.
- Los certificados digitales SSL deben ser provistos por una entidad certificadora, la misma que promueve las primary key en cada uno de los servidores, esto a su vez se renuevan cada año, para garantizar la integridad, confidencialidad y autenticidad de las conexiones a los servicios, información o datos que se trasmitan a través de los aplicativos y de la página institucional con un algoritmo de encriptación de hash SHA-2 128 y/o 256 bits.

7. Anexos

Ninguno.