PSI-04 Control Criptográfico

Revisado por:	Aprobado por: Dirección	Elaborado por: Resp. de Sistema
Fecha:	**Fecha:**	**Fecha:**
Firma:	**Firma:**	**Firma:**

0. Objeto

El objeto de este procedimiento es definir el uso de sistemas y técnicas criptográficas para la protección de la información ubicada en **CLÍNICA BEIMAN**, con el fin de garantizar su confidencialidad, integridad y disponibilidad.

0.1. Entradas y salidas del proceso

Entradas:

- Necesidad de proteger la información confidencial
- Herramientas de cifrado
- Necesidad de gestionar las claves de cifrado

Salidas:

- Sistemas cifrados.
- Política de controles criptográficos.
- Normas para la gestión de claves.

1. Controles criptográficos. Necesidades de cifrado.

De acuerdo con **RSI.0101 Clasificación de la información**, como también con obligaciones legales y contractuales, la organización debe proteger a los sistemas individuales o a la información a través de los siguientes controles criptográficos definidos en el registro correspondiente.

En particular, se consideran mecanismos de cifrado en los siguientes casos:

- Datos definidos como CONFIDENCIALES Y SANITARIOS según los especificado en el procedimiento Clasificación de la Información y Gestión de Activos, en su almacenamiento en equipos y en soportes externos
- Acceso remoto a través de VPN (mediante SSL).
- Información que se sirva desde las aplicaciones web que lo requieran, así como de la transferencia de ficheros debe realizarse a través del protocolo seguro HTTPS.
- Todas las redes Wifi deberán utilizar cifrado a través del protocolo WPA2 excepto 1 que será puesto a disposición a personal que no forme parte de CLÍNICA BEIMAN mediante portal cautivo y tendrán su acceso habilitado por un tiempo preestablecido.
- Todas las comunicaciones con la Administración Pública se realizarán a través de certificados digitales.
- Datos de autentificación (contraseñas, números secretos personales).
- Firma electrónica de documentos: contratos, acuerdos, etc.
- Comunicación con cliente a través de canales seguros (SharePoint).
- Comunicación con organismos públicos.
- Transferencias bancarias.

Los sistemas que se ajusten a estas operaciones se registrarán en RSI.0402 Controles criptográficos.

Las herramientas utilizadas para estos controles son:

- Active directory
- Eset Endpoint Encryption
- Duplicati
- Handy Backup

Los propietarios de los activos individuales sobre los cuales se aplican controles criptográficos, son los responsables de la correcta aplicación de los controles criptográficos particulares.

Responsable: Responsable de Seguridad de la Información

2. Gestión de claves

La configuración de los sistemas de cifrado es responsabilidad del departamento de sistemas que en ningún momento almacena contraseñas ni claves de cifrado.

Las claves y elementos criptográficos serán almacenados de forma segura, en función del elemento en cuestión.

Se establecerán las siguientes reglas sobre la gestión de claves:

- Métodos de Generación de claves criptográficas privadas y públicas.
- Métodos de Activación y distribución de claves criptográficas.
- Definición del plazo para el uso de las claves y de su actualización periódica (de acuerdo con la evaluación de riesgos).
- Archivo de claves inactivas que son necesarias para archivos electrónicos encriptados.
- Métodos de Destrucción de claves.
- Número de intentos limitado. Tras un número de intentos fallidos, pueden tomarse distintas medidas:
    - Obligar a reescribir el nombre de usuario (lo más común).
    - Bloquear el acceso durante un tiempo.
    - Enviar un mensaje al administrador y/o mantener un registro especial.
- Longitud mínima. Las contraseñas deben tener un número mínimo de caracteres (se recomienda 7 u 8 como mínimo).
- Restricciones de formato. Las contraseñas deben combinar un mínimo de letras y números, no pueden contener el nombre del usuario ni estar en blanco.
- Envejecimiento y expiración de contraseñas. Cada 3 meses se fuerza a cambiar la contraseña. Se mantiene un periodo forzoso entre cambios, para evitar que se vuelva a cambiar inmediatamente y se repita la anterior. La vigencia mínima de validez de una clave es 24h
- Las claves son administradas por sus propietarios, en conformidad con las reglas mencionadas precedentemente.

Las claves criptográficas serán protegidas mediante contraseña. En el caso de pérdida, corrupción o destrucción, las claves serán recuperadas de la copia generada en el servidor de **CLÍNICA BEIMAN.**

Responsable: Responsable de Seguridad de la Información

3. Formatos y anexos

Descripción	Tiempo de archivo de los registros que genera	Responsable
RSI.0401 Política de controles criptográficos.	3 años	Resp. del Sistema
RSI.0402 Controles criptográficos.	3 años	Resp. del Sistema

Registro de las modificaciones		
Revisión	**Fecha**	**Naturaleza de la revisión**
00	10/08/2022	Edición Inicial