PSI-02 Gestión de Soportes

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

0. Objeto

El objeto de este procedimiento trata de definir la sistemática establecida por **CLÍNICA BEIMAN** para controlar y gestionar de manera adecuada los soportes externos (automatizados y no automatizados) utilizados en la organización, para reducir los riesgos sobre los mismos relacionados con pérdidas de integridad, disponibilidad y confidencialidad de los datos que contienen.

0.1. Entradas y salidas del proceso

Entradas:

- Necesidad de gestión de la seguridad de la información almacenada en soportes.
- Necesidad de control de los soportes utilizados por el personal de la organización.
- Necesidades de control de la información documentada almacenada en soportes no automatizados.

Salidas:

- Normas de uso aceptable de soportes.
- Inventario de soportes.
- Registros de distribución de soportes.
- Normas para distribución, acceso, recuperación y uso de soportes.
- Normas para almacenamiento y preservación.
- Normas para destrucción de soportes.

1. Gestión de soportes

Se entiende por soporte cualquier elemento físico con capacidad para almacenar y transportar información lógica con facilidad (discos duros externos, memorias USB, tablets, teléfonos móviles y ordenadores portátiles). En esta ficha de proceso también se tendrán en cuenta, para la aplicación de medidas de seguridad, los soportes que contienen información en formato papel (tanto los propios documentos, como archivadores, carpetas, etc. en las que se almacenen).

La creación y uso de soportes para almacenar o trasladar información o datos de carácter personal, deberá ser conocida y autorizada por el responsable asignado o por la dirección de la organización. No se permitirá el uso no controlado de soportes por parte de los usuarios para tal fin.

Responsable: Responsable de Seguridad de la Información

2. Etiquetado de Soportes

Se procederá al etiquetado de todos los soportes que contengan información confidencial, de uso interno o datos de carácter personal que se identifiquen en la organización. Este proceso

de etiquetado se aplicará tanto a los soportes informáticos, como aquellos soportes (carpetas, archivadores…) que contengan información de carácter personal en formato papel.

El etiquetado se realizará sobre los soportes mediante el uso de códigos individuales y nunca reutilizables, de tal forma que se permita conocer el contenido del soporte (salvo información confidencial) al personal de la empresa y que dificulte conocer su contenido al personal ajeno.

La etiqueta asociada a cada equipo perteneciente a **CLÍNICA BEIMAN** contendrá la siguiente información:

CONTENIDO	DESCRIPCIÓN
Abreviatura de la clínica donde se encuentre asignado inicialmente el activo	• JER: Jerez • CAB: Las Cabezas de San Juan • SEV: Sevilla • HUE: Huelva • COR: Córdoba • JAE: Jaén • GRA: Granada • ALM: Almería
Ubicación inicial	• ADM: Administración • CON: Consultas • REC: Recepción • EXT: Externo
Numeración XXX	Número consecutivo según cantidad de soportes destinados

Responsable: Responsable de Seguridad de la Información

3. Inventario de soportes

Tal y como se ha reflejado en la FPSI02 Gestión de Activos, **CLÍNICA BEIMAN** lleva a cabo el inventario tanto de soportes como de activos, a través del software de gestión ESET EndPoint a fin de tenerlos gestionados adecuadamente.

CLÍNICA BEIMAN no mantiene inventariado los soportes que contienen información en soporte papel, puesto que aquella que es de carácter confidencial y crítica para la empresa, se encuentra perfectamente identificada y almacenada en zona de archivo correspondiente.

En **CLÍNICA BEIMAN** podemos diferenciar entre los siguientes tipos de soportes extraíbles:

TIPO	DESCRIPCIÓN
USB	No se va a permitir la conexión de dispositivos de almacenamiento USB directamente en los equipos de los usuarios. Se realiza mediante un equipo pasarela para su previo escaneo
Discos duros	Los discos duros externos tienen uso exclusivo en determinadas áreas para la realización de copias de seguridad de los datos.
Tablet	Uso exclusivo para la recogida de firmas de pacientes en distintos

	procesos.
Portátiles	– Portátiles de uso interno con posibilidad o no de salir al exterior de las instalaciones – Portátiles de Dirección – Otros por ejemplo: Portátiles securizados para trabajar en instalaciones de colaboradores. – Para uso de determinado personal de la clínica, por movilidad inter-centros, y teletrabajo.
Teléfono móvil corporativo	

Se definirán los responsables adecuados para la gestión de los soportes y el mantenimiento del inventario de los mismos.

Para aquellos soportes de tipo extraíble identificados anteriormente, será preciso realizar un inventario para su correcta gestión. En el inventario se indicará, al menos: la codificación utilizada para el etiquetado, el tipo de soporte, la fecha de creación del mismo, la fecha y los mecanismos de eliminación y, si procede, el tipo de información contenida. El inventariado de soportes extraíbles se realizará según el formato **RSI.0201 Inventario y distribución de soportes extraíbles.**

Responsable: Dirección/Responsable del Sistema/Responsable de Seguridad de la Información

4. Almacenado y uso

Los soportes, previamente etiquetados, serán almacenados asegurando la confidencialidad de los mismos y su protección frente a las amenazas externas o ambientales. Los soportes (informáticos y documentos) se almacenarán en zonas que no sean públicas, y donde el acceso pueda ser controlado y supervisado.

Se valorará la necesidad (en base al tipo de datos que contengan) de que este almacenamiento se realice bajo llave, o con medidas de seguridad adicionales. En concreto los servidores, discos duros utilizados para realizar las copias de seguridad se encuentran en el CPD dentro del armario Rack, cerrado con llave, siendo sólo posible su acceso por personal autorizado y se realizan las sincronizaciones correspondiente para backups sin necesidad de ser trasladado. En caso del CPD de respaldo se usará la misma dinámica donde este se ubicara sito en las instalaciones de Clínicas Beiman Las Cabezas..

En particular, estos medios estarán cifrados mediante la herramienta Eset Encryption contenido información de uso interno, confidencial o datos personales según la importancia de los datos. En **CLÍNICA BEIMAN** se ha optado por la realización del correspondiente cifrado a nivel de ficheros en todos los dispositivos extraíbles haciendo uso del software **ESET Encryption.**

Cuando un usuario precise el uso de algún soporte para almacenar información confidencial, de uso interno o datos de carácter personal, deberá de solicitar autorización para su uso, en cuyo

caso se le asignará uno de los soportes identificados y se anotará en el registro **RSI.0201 Inventario y distribución de soportes extraíbles**.

Se asegurará el control de acceso a los soportes informáticos, de modo que se pueda conocer qué usuarios acceden o utilizan los mismos. Se valorará llevar igualmente este seguimiento/registro con los soportes que contengan documentación en papel**. (Sería aconsejable cada vez que un usuario interno entrara en estas áreas, registrarlo)**

Durante su uso, los usuarios deben encargarse de custodiar de manera adecuada, evitando su pérdida o el acceso a los mismos por usuarios no autorizados por un deficiente control sobre los mismos.

Responsable: Responable del Sistema/Responsable de Seguridad de la Información

5. Distribución de soportes

La salida o distribución de soportes (automatizados o no) que contengan información confidencial, de uso interno o datos de carácter personal fuera de los locales de la empresa deberá ser solicitada previamente y autorizada por parte del Responsable asignado o por la Dirección de la organización. Para salidas de soportes periódicos, bastará con una autorización genérica que acredite su distribución.

Todas las salidas (de las instalaciones de la organización) de soportes informáticos que contengan información confidencial, de uso interno o datos de carácter personal han de ser autorizadas por el responsable asignado y serán registradas indicando la fecha de salida, destinatario, responsable de envío, tipo de datos, etc. Se distinguen tres tipos de autorizaciones:

- **Periódicas**: Salidas de datos que se producen con una periodicidad concreta (mensual, anual, etc.). Solo se requerirá una autorización, si bien se reflejan todas las salidas en el registro de entrada/salida de soportes.
- **Ordinarias**: Salidas de información que se realizan de forma repetitiva, pero sin periodo de tiempo definido. Como en el caso anterior, bastará con una sola autorización para cada tipo de salida.
- **Extraordinarias**: Salida de datos puntual. Se necesita una autorización para cada salida, y además se refleja la misma en el registro.

Se dispondrá de un registro en el cual se reflejarán todas las salidas y movimientos de soportes y documentos **RSI.0301 Inventario y distribución de soportes extraíbles**, salvo aquellas que no se consideran relevantes para la organización.

Responsable: Responsable del Sistema/Responsable de Seguridad de la Información

6. Eliminación o reutilización de soportes

Cuando se pretenda (ante el cese en su uso) proceder a la baja (para su reutilización o eliminación) de los soportes que contengan datos personales, se requerirá la autorización del Responsable de Seguridad.

En el caso de soportes informáticos, siempre que sean devueltos por el personal a quien se había asignado, y con carácter previo a su asignación para otro uso, se procederá a su

formateo, asegurando la eliminación del mismo de toda la información (incluyendo programas, software, documentos, etc.).

En el caso de que se estime la eliminación o baja definitiva del soporte, además de su formateo, se procederá a su destrucción física, de modo que la información contenida no pueda recuperarse, y se impida el acceso al mismo por parte de personal no autorizado o ajeno a la organización. El método de destrucción dependerá del tipo de soporte utilizado.

En **CLÍNICA BEIMAN** se realiza un borrado lógico y posterior destrucción física del disco duro. Existe una máquina de destrucción de papel y CD/DVD. Los soportes CD, son destruidos siguiendo el procedimiento establecido.

La información correspondiente a las bajas o reutilizaciones de los soportes, deberán de quedar reflejados en el **RSI.0201 Inventario y distribución de soportes extraíbles.**

Los soportes o documentos en papel deberán igualmente de ser destruidos cuando se decida proceder a su eliminación. Para ello se dispondrá en la organización de destructoras de papel. Los empleados de la organización que manejan documentos individuales deberán de responsabilizarse de su destrucción. A tal efecto, en **CLÍNICA BEIMAN** se dispone de una destructora interna de papel. Del mismo modo, se posee contrato con una empresa gestora de residuos la cual certifica la destrucción de toda la documentación señalada anteriormente.

Responsable: Responsable del Sistema/Responsable de Seguridad de la Información

7. Formatos y anexos

Descripción	Tiempo de archivo de los registros que genera	Responsable
RSI.0201 Inventario y distribución de soportes extraíbles	N/A	Resp. del Sistema
Herramienta software ESET EndPoint	N/A	Resp. del Sistema

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