PSI-01 Gestión de Activos

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 la sistemática establecida por la organización para el inventario de los activos, el etiquetado, clasificación y manipulado de la información.

Se entenderá como Activos de información, al contrario que en el proceso de apreciación de riesgos, a la totalidad de recursos informáticos existentes en **CLÍNICA BEIMAN** y utilizados para el tratamiento de la información. En este caso, no realizaremos "agrupaciones" de activos (por ejemplo, considerar en general" Puestos de usuario") sino que identificamos e inventariamos cada equipo o recurso informático para una adecuada gestión y seguimiento de los mismos.

0.1. Entradas y salidas del proceso

Entradas:

- Necesidad de identificar y controlar los activos de información.
- Equipamiento informático y procesos de la organización.
- Necesidad de definir normas de uso aceptable de activos de la información.
- Necesidad de clasificar la información en base a su criticidad.

Salidas:

- Inventariado de activos.
- Clasificación de la información.
- Normas de uso aceptable de activos.

1. Inventario de activos

CLÍNICA BEIMAN identifica todos los activos y recursos para el tratamiento y almacenamiento de la información y los documenta e inventaría a través de ESET endpoint, a fin de tenerlos gestionados adecuadamente, para lo cual deberá de mantenerlo permanentemente actualizado. En el inventario de activos de seguridad se incluirá la información necesaria que permita identificarlo, describirlo, clasificarlo y ubicarlo. Cada activo dispondrá de una configuración de seguridad orientada a reducir los riesgos, debiendo de verificar que esta se mantiene.

Al menos con una periodicidad trimestral o cuando se produzcan cambios significativos, se revisará el inventario de activos con el fin de mantenerlo actualizado.

Responsable: Responsable de Seguridad de la Información

2. Propiedad de los activos

A cada activo de información identificado se le asignará un único propietario que será referenciado en el inventario de activos, que será el responsable de asegurar la adecuada gestión del mismo, y de verificar que dispone de la configuración de seguridad adecuada.

Responsable: Responsable de Seguridad de la Información

3. Uso aceptable de activos

CLÍNICA BEIMAN ha definido una **RSI.0102 Política de uso aceptable de activos**. Cada Responsable de departamento deberá ser formado y a su vez formar e informar a las personas de su área de las medidas necesarias para el uso aceptable de los activos.

Todos los trabajadores, internos o externos, y las terceras personas implicadas tienen que seguir la política definida por la empresa para utilizar de forma aceptable la información y los activos que se encuentran asociados a las instalaciones del procesamiento de información, así como la RSI.0101 Guía de usuario, perteneciente a la PSI-00 Organización de Seguridad de la Información.

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

4. Devolución de activos

Se solicitará la devolución de los activos que se le hayan entregado a lo largo de su vida en la empresa, bajo la custodia y/o derechos de acceso del trabajador que causa baja por renuncia voluntaria o rescisión del contrato, o por cambio de las actividades o del puesto de trabajo.

La devolución de los activos se realizará según lo indicado en **PSI.04 Control de acceso**, debiendo de quedar documentado en el formato **RSI.0401 Accesos de usuarios**.

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

5. Directrices de clasificación de la información

CLÍNICA BEIMAN define las bases para la clasificación de la información, las reglas de acceso para los documentos y registros y las medidas de seguridad a aplicar a los activos de información.

El acceso a estos contenidos se limita de acuerdo con el nivel de clasificación asignado a las personas que ocupan determinados puestos en la empresa, restringiéndose también su uso.

En el registro **RSI.0101 Clasificación de la información** se identifican los diferentes tipos de información existentes en la organización y las medidas de seguridad que son necesarias para el tratamiento de cada uno de estos tipos de información.

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

6. Etiquetado y manipulado de la información

La información, ya sea digital o física, se etiquetará de modo que el personal con acceso a la misma conozca el tipo de información a la que está accediendo y pueda aplicar las medidas adecuadas. Las medidas adecuadas a cada nivel de clasificación para una adecuada manipulación de la información se documentará en el **RSI.0101 Clasificación de la información** de forma inequívoca. Para el etiquetado se utilizarán marcas de agua, etiquetas físicas, codificación de colores, códigos identificativos, etc.

Toda la información asociada a pacientes queda clasificada como de carácter sanitario en el servidor.

Cabe señalar que toda la documentación en formato papel con cualquier tipo de información asociada a pacientes, así como, su acceso queda restringido a personal de la empresa mediante autorización correspondiente del Responsable de Departamento.

En **CLÍNICA BEIMAN** se utiliza sistema de Active Directory para uso en redes de dominio de Windows Server contando con funciones de autenticación, autorización y proporciona un framework para otros servicios similares. Básicamente, el directorio consiste en una base de datos LDAP que contiene objetos en red con los requisitos de seguridad a tal fin establecidos por el Responsable de Seguridad. Para controlar el acceso de equipos o dispositivos no validados se hará una validación de la MAC correspondiente, por lo que tan sólo podrán conectarse los equipos cuya MAC esté previamente registrada y aceptada. Si no es posible o no se considera oportuno el etiquetado de alguna documentación física o digital (pej. documentación física para su uso en borrador), se deberá formar adecuadamente al personal para que conozca el nivel de criticidad de estos documentos y pueda aplicar las medidas de seguridad adecuadas.

Responsable: Responsable de RRHH/Responsable de Seguridad de la Información

7. Formatos y anexos

Descripción	Tiempo de archivo de los registros que genera	Responsable
RSI.0101 Clasificación de la Información	3 años	Resp. del Sistema
RSI.0102 Política de uso aceptable de activos	3 años	Resp. del Sistema
Software ESET EndPoint para registro de activos	3 años	Resp. del Sistema

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