PSI-05 Seguridad Física. Áreas Seguras

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 las reglas para la protección de las instalaciones, de los entornos de trabajo y de las áreas en las que se realizan tratamientos de información, en base a los requerimientos legales, de negocios y de seguridad.

0.1. Entradas y salidas del proceso

Entradas:

- Necesidad de proteger las instalaciones frente a accesos no autorizados y amenazas externas y de origen ambiental
- Necesidad de proteger los equipos frente a accesos no autorizados y amenazas externas y de origen ambiental
- Necesidad de concienciar a los usuarios respecto a los usos.

Salidas:

- Definición de políticas de uso aceptable
- Definición de medidas de control de acceso físico
- Definición de medidas de almacenamiento físico seguro
- Definición de medidas de índole físico sobre equipos (puestos de usuario y servidores)

1. Identificación de áreas seguras.

Las salas, despachos, zonas o áreas de las instalaciones de **CLÍNICA BEIMAN** en las que se realice algún tratamiento de información y de datos personales (incluida la conservación y almacenamiento de los mismos), que sea confidencial o de uso interno, o en las cuales se puede acceder a sistemas de tratamiento de dichos datos (servidores, puestos de usuario, documentos, archivos, etc.) tendrán la consideración de áreas seguras.

En estas zonas, se considerarán las medidas de seguridad indicadas en la presente ficha de proceso, orientadas a preservar la disponibilidad, integridad y, principalmente, la confidencialidad de la información de la cual la empresa es Responsable, debiendo de evitase accesos no autorizados o usos no previstos.

En particular, se consideran las siguientes áreas seguras en **CLÍNICA BEIMAN**:

- Sala de servidores y archivos
- Despachos
- Puestos de trabajo

Los diferentes sistemas de tratamiento (físicos o lógicos) utilizados para el tratamiento de la información y de los datos personales deberán ser adecuadamente protegidos frente a accesos no autorizados, u otros incidentes de índole físico (desastres naturales, accidentes, etc.). Se deberán de aplicar, sobre las áreas consideradas seguras, las medidas necesarias para reducir los riesgos de esta índole.

Responsable: Responsable de Seguridad de la Información

2. Áreas de acceso público

Al mismo tiempo, en **CLÍNICA BEIMAN** existen zonas en las cuales se autoriza el acceso del público en general, o de determinadas personas ajenas a la organización, ya sea por la necesidad de acceso público a pacientes, o por el acceso por parte de entidades externas en el desarrollo de sus tareas (clientes, visitas, proveedores, entregas de mercancía, etc.).

Se debe evitar, en la medida de lo posible, el uso o la colocación en estas zonas de soportes (informáticos o papel) que contengan información confidencial, de uso interno o datos de carácter personal. En caso de que sea imprescindible su uso, la persona responsable se encargará de custodiar y controlar estos soportes, evitando el acceso a los mismos (incluyendo acceso visual) por parte de personal no autorizado.

Se pueden señalar las siguientes zonas de acceso público en **CLÍNICA BEIMAN**:

- Recepción
- Recepción Área Capilar
- Recepción Área Fisioterapia

En estas zonas se minimizará el uso e instalación de puestos de usuario y demás sistemas que permitan el acceso a los datos y a la información de la organización. En caso de que sea imprescindible su uso, estos se deberán ubicar de modo que se evite el acceso visual a los datos, y deberán permanecer controlados por los usuarios responsables de los mismos.

Responsable: Responsable de Seguridad de la Información

3. Controles de ingreso áreas seguras

El personal ajeno a la organización, inicialmente, sólo podrá acceder a estas zonas de recepción anteriormente indicadas. El acceso a las áreas seguras requerirá la autorización por parte de los responsables de la organización, y permanecerán en todo momento acompañados. Se considerarán, por ejemplo, la recepción principal de **CLÍNICA BEIMAN** para la reparación de averías o para la realización de tareas de mantenimiento, instalación de nuevo equipamiento, servicios de limpieza, y cualquier otro acontecimiento, que a su juicio afecte o pudiera afectar a la seguridad de los datos.

El personal de estas empresa, con carácter general realizará sus tareas en la sala de acceso restringido durante los horarios en los que se encuentren presentes responsables de la organización, que velarán por el cumplimiento de las medidas de seguridad de acceso físico y garantizándose por parte de estas empresas la observancia de las medidas de seguridad necesarias para que no se produzca, voluntaria o involuntariamente, incidencia alguna en las dependencias con entrada restringida, siendo aquella responsable de las que se produzcan.

Todas las instancias de **CLÍNICA BEIMAN** se encuentran inicialmente cerradas con llave, en ausencia de personal de la empresa encontrándose su acceso protegido mediante esta medida de ingreso. Únicamente Dirección y aquellos responsables previamente autorizados cuentan con estas llaves. Al inicio de la jornada, son estos quienes proceden a la apertura de todos los despachos en el interior de la oficina.

Cabe mencionar en este apartado, que **CLÍNICA BEIMAN** está dividida en varias áreas en función del personal que ejerce su actividad en las mismas:

- **Área Clínica**: El acceso a esta zona se encuentra regulado por el personal de recepción de cada área de acceso público. La recepción de los pacientes es registrada en el software de gestión clínica KYROS.

- **Área de Administración**: Esta área se encuentra en otros edificios diferenciados de aquel en el que se encuentra el área clínica. El acceso a los mismos se encuentra regulado por personal propio de administración. En estos edificios, se encuentra la sala de servidores y archivo fin en la que se aloja de información clasificada como de carácter confidencial y/o sanitaria.

El acceso a estas áreas por parte del personal interno de la organización, se encontrará igualmente restringido al personal autorizado. El personal de la organización no podrá disponer de acceso a las áreas seguras que no precise para el desarrollo de sus funciones, salvo autorización expresa del responsable del sistema o los responsables facultados para ello. La autorización de acceso a las áreas seguras para cada usuario, quedará reflejada en el **RSI-0303 REGISTRO DE ACCESO Y AUTORIZACIONES DE USUARIO.**

El responsable de seguridad reflejará en el registro de incidencias los accesos no autorizados o controlados a los espacios restringidos.

Independientemente, existe personal de la empresa con privilegios de acceso a todas las zonas citadas anteriormente:

1. Dirección.
2. Calidad y recursos humanos.
3. Personal de IT.
4. Dirección Médica

Responsable: Responsable de Seguridad de la Información/Responsables de Área

4. Protección frente amenazas externas y de origen ambiental

CLÍNICA BEIMAN se asegura que las instalaciones y los sistemas de seguridad física cumplen con las leyes y regulaciones aplicables tanto en materia de edificación como de control de accesos y protección frente a amenazas externas (sistemas antiincendios, suministro eléctrico, etc.)

Se han asegurado las áreas de la organización de acuerdo a la legislación vigente. Los sistemas de control medioambiental (como extintores) y de acceso (como alarmas) son mantenidos y probados periódicamente por los proveedores que reportan los registros de sus tareas según lo especificado en contrato en vigor.

Todas las áreas cuentan con las siguientes medidas técnicas:

- **Sistemas de videovigilancia**
- **Sistemas de extinción de incendios**

- **Sistemas de detección y alarma de incendios:** Adicionalmente se dispone de detectores de humo en la sala del CPD.
- **Sistema de ventilación:** Se dispone de sistemas de extracción/ventilación en todas las áreas de la organización.
- **Señalización:** Asimismo, todas las zonas cuentan con su debida señalización de extintores, de pulsadores de alarma y avisadores sonoros, señalización de uso de mascarilla y uso de dispensadores higiénicos, de salidas de emergencia y pasillos de evacuación.

En las áreas seguras, además, se ha decidido la implementación de mecanismos de protección adicionales dada la criticidad de estas áreas y de la información que contienen:

- **Sistema de alimentación ininterrumpida:** Presente únicamente en la sala del CPD.
- **Sistema de detección de incendios:** La sala CPD dispone de detectores de humo.
- **Sistema de aire acondicionado:** La sala de CPD disponen de un sistema de acondicionamiento que mantiene la temperatura de la sala en los niveles establecidos para evitar el calentamiento de los servidores. Además dispone de sensores de temperatura que alertan en caso de desviaciones.

Responsable: Responsable de Seguridad de la Información

5. Actividades prohibidas en áreas seguras

En las áreas seguras no está permitido:

- Realizar ningún tipo de grabación fotográfica, de audio o de vídeo.
- Conectar ningún dispositivo a una red a menos que esté específicamente autorizado para hacerlo.
- Manipular los equipos instalados en áreas seguras a menos que esté específicamente autorizado.
- Archivar grandes cantidades de papeles excepto en las áreas a tal fin destinadas y siguiendo en todo momento las indicaciones correspondientes.
- Guardar materiales o equipos inflamables.
- Utilizar cualquier tipo de dispositivo de calefacción.
- Fumar, comer o beber.

Responsable: Responsable de Seguridad de la Información

6. Instalaciones de suministro

Los sistemas de abastecimiento de potencia que soportan la totalidad del suministro eléctrico de los equipos y servidores, cumplen con las especificaciones de los fabricantes y con la normativa

aplicable. Además, para los servidores se dispone de Sistemas de Alimentación Ininterrumpida (SAI) que mantienen su funcionamiento en caso de fallos en la alimentación, y protege de fluctuaciones y picos de tensión. Estos sistemas son verificados periódicamente para comprobar su funcionamiento.

Responsable: Responsable de Seguridad de la Información

7. Registro, supervisión y auditoría

Se deben establecer los criterios necesarios para el registro de los eventos relacionados con la seguridad física o de las instalaciones y con la generación de incidencias al respecto.

En **CLÍNICA BEIMAN** se registrarán conforme a los establecido en el presente documento:

- Los incidentes relacionados con los sistemas de control físicos y de accesos.
- La emisión, entrega y revocación de llaves y/o códigos de seguridad.
- La entrada de cualquier persona fuera del horario habitual de trabajo.
- Los resultados de los mantenimientos y pruebas de sistemas de control y de sus alarmas.

Con carácter **trimestral**, se revisará tanto el sistema de control de accesos a las áreas de acceso restringido como el registro de accesos de personal externo. Si se detecta alguna anomalía en este sentido, se está habilitado para cursar una incidencia de gestión según lo establecido en el proceso de gestión de incidencias.

Responsable: Responsable de Seguridad de la Información

8. Formatos y anexos

Descripción	Tiempo de archivo de los registros que genera	Responsable
KAIROS24h	Actualizado permanentemente	Resp. del Sistema

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