# PSI-00 Organización de Seguridad de la Información

| 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 un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización. Así como, evitar el acceso no autorizado a dispositivos ubicados fuera de las instalaciones de la organización.

### 0.1. Entradas y salidas del proceso

Entradas:

- Gestión de la Seguridad de la Información.
- Necesidad de definir responsabilidades en materia de seguridad de la información.
- Necesidad de definir políticas para la protección de los dispositivos móviles y el teletrabajo.

Salidas:

- Control interno.
- Gestión de equipos y dispositivos móviles y teletrabajo.

## 1. Roles y responsabilidad en Seguridad de la Información

**CLÍNICA BEIMAN** ha definido y asignado las responsabilidades relativas a la seguridad de la información, definiendo en cada puesto de trabajo tanto las funciones del personal como las obligaciones, de acuerdo a lo establecido en el P-02 Gestión de recursos, y según las responsabilidades definidas en el Manual del SGCSI.

Como norma general, se realiza una segregación de las tareas de responsabilidad en la gestión de la información y los usuarios tendrán únicamente acceso a la información necesaria para el desarrollo de su actividad, reduciendo el riesgo de manipulaciones no autorizadas.

En organización se ha decidido el desarrollo de la **RSI.0001 Guía de usuario**, en la que se indican las normas y políticas de uso aceptable que los usuarios deben aplicar durante el desarrollo de sus actividades en la organización, a fin de asegurar un tratamiento seguro de la información y reducir riesgos asociados al uso de los sistemas de tratamiento.

**Responsable**: Dirección

## 2. Segregación de Tareas

Las funciones de seguridad de la información se han definido de forma que, en la medida de lo posible, exista segregación de tareas, de modo que se impide que una única persona participe en todo el ciclo de vida de un determinado proceso. Así, por ejemplo, las autorizaciones a los usuarios son asignadas por el Responsable del Sistema o los Responsables de las diferentes áreas, siendo supervisados y aprobados por la Dirección. Del mismo modo, las tareas de administración de los sistemas son realizadas por empresa IT externa cuya relación contractual con **CLÍNICA BEIMAN** ha sido perfectamente definida en el correspondiente SLA-ANS

(Acuerdo Nivel de Servicio) con la correspondiente autorización de Dirección y siendo supervisada esta actividad por personal a tal fin designado por Dirección. Dicho proveedor externo, ejerce las funciones de Responsable de Seguridad a efectos de nuestro SGCSI.

**Responsable**: Dirección/Responsable de Seguridad de la Información

## 3. Contacto con las autoridades y grupos de interés

**CLÍNICA BEIMAN** identifica aquellas autoridades y entidades que están relacionadas con la seguridad de la información y que pueden ser necesarias para una adecuada gestión de la seguridad de la información, en particular, en lo referente a incidentes o eventos de seguridad, ya sea para la resolución de los mismos, para la investigación de delitos derivados de ellos, para la recuperación y continuidad de las operaciones de la organización, nuevas vulnerabilidades de los sistemas, nuevos ataques informáticos, buenas prácticas, novedades en cuanto a seguridad de la información…

- Agencia de Protección de datos o autoridades de control relacionados con la protección de datos personales.
- Fuerzas y cuerpos de seguridad, en especial, las áreas de ciberseguridad.
- Servicios de emergencia, bomberos, etc.
- El INCIBE o el Centro Criptológico Nacional, o los organismos similares de cada país.
- Foros o páginas web de seguridad informática en redes sociales.
- Inscripción a newsletter o servicios de noticias relacionados con seguridad de la información.

**Responsable:** Dirección/Responsable del Sistema

## 4. Dispositivos móviles

Entre los equipos móviles se incluyen todo tipo de ordenadores portátiles, teléfonos móviles, tarjetas/dispositivos de memoria/almacenamiento, y demás equipamiento móvil utilizado para almacenamiento, procesamiento y transferencia de datos.

El equipamiento mencionado puede ser llevado fuera de las instalaciones solamente con autorización, de acuerdo a lo establecido en la política de uso de dispositivos móviles que se incluye en la **RSI.0001 Guía de usuario** y que se basan en las siguientes disposiciones:

- Se debe tener especial cuidado cuando los equipos móviles se encuentran en vehículos (incluyendo automóviles), espacios públicos, habitaciones de hotel, salas de reunión, centros de conferencias y demás áreas no protegidas exteriores a las instalaciones de la organización.
- La persona que usa dispositivos móviles fuera de las instalaciones debe cumplir las siguientes reglas:
  - El equipamiento móvil que contiene información importante, sensible o crítica no debe ser desatendido y, en lo posible, debe quedar resguardado bajo llave o se deben utilizar “cierres/bloqueos” especiales para asegurarlo.

- Cuando se utiliza equipamiento móvil en lugares públicos, el usuario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.
- Cuando se utiliza equipamiento móvil en lugares públicos, el usuario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.
- Las actualizaciones de parches y demás configuraciones del sistema son realizadas de forma automática. Las actualizaciones de SO llegarán a los usuarios de Windows a través de Windows Update, lanzándose la actualización desde el Servidor de Dominio, para tener controladas las distintas actualizaciones del sistema. En el caso de dispositivos sustituidos por modernización o préstamo para reparación del mismo, las configuraciones del sistema de cada dispositivo son realizadas por el proveedor IT previamente a la entrega del dispositivo y en cuanto a las actualizaciones serán verificadas que poseen la que se precise desde soporte del proveedor IT.
- Se dispone de una solución tecnológica antia-malware, anti-virus y anti-spyware en cada uno de los equipos, supervisados por una consola desde el Servidor de Dominio. Aún se está valorando la solución tecnológica a utilizar. El router principal de acceso a la clínica, dispondrá de software de gestión de red, integrando cortafuegos, VPN, DPI: inspección profunda de paquetes, IPS / IDS - Sistema de prevención de intrusiones
- Las conexiones externas a **CLINICA BEIMAN**, se realizará siempre con equipos de la propia clínica, para asegurar el control del mismo, y se realizará usando una VPN que implementará el router. Sólo determinados usuarios tendrán permiso para estas conexiones externas. Para la excepción de los datos que se almacenen directamente en el equipo, será el propio usuario el que realice sus copias de seguridad sobre su carpeta vinculada en el servidor (Carpeta con su propio nombre de usuario a la que tendrá acceso. 2Gb).
- La conexión a redes de comunicación y el intercambio de datos debe reflejar la sensibilidad de los datos y se realiza a través de recursos de red establecidos por la empresa y queda diferenciada por carpetas de unidades organizacionales a las cuales se tiene acceso por usuario y definición de privilegios de acceso.
- La información que se encuentra en ordenadores portátiles se encuentra cifrada. Estos usuarios trabajaran en únicamente para determinados archivos sensibles/confidenciales/de carácter sanitario que son almacenados en una carpeta previamente definida en el servidor y mediante conexión VPN. Se cifra por completo el disco duro, para evitar la fuga de información en caso de pérdida o robo del equipo.
- **En el caso que el equipamiento móvil sea desatendido**, se deben aplicar las reglas para equipamiento de usuario desatendido, de acuerdo a la política de uso aceptable.

El Responsable del Sistema junto con el Responsable de Seguridad de la Información y RRHH son los responsables de la capacitación y concienciación de las personas que utilizan equipamiento de computación móvil fuera de las instalaciones de la organización.

La autorización respecto al uso de los dispositivos móviles deberá de quedar formalmente documentada y aprobada a través del registro **RSI.0401 Registro de acceso de usuarios** incluido en la ficha de proceso de **PSI.04 Control de acceso**.

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

## 5. Dispositivos BYOD (bring your own device)

**CLÍNICA BEIMAN no permite el uso de dispositivos BYOD en sus instalaciones.**

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

## 6. Teletrabajo

Sólo el personal autorizado podrá realizar su trabajo fuera de la organización. El teletrabajo incluye el uso de teléfonos móviles corporativos fuera de las instalaciones de la organización.

El teletrabajo debe ser autorizado por el/la Responsable de RRHH, que comunicará vía email al Responsable de Seguridad (proveedor IT) de la necesidad para realizar la correspondiente habilitación, que quedará documentada en el registro **RSI.0401 Accesos de usuarios** incluido en la ficha de proceso de PSI.04 Control de acceso.

El/la Responsable del Seguridad es el encargado de preparar planes y procedimientos si se considera necesario para garantizar lo siguiente:

- Protección de dispositivos móviles, de acuerdo a lo indicado en la sección anterior.
- Evitar el acceso no autorizado especialmente cuando se realiza teletrabajo.
- Configuración adecuada de la red local utilizada para conectarse a internet. (Configuración del cliente de VPN)
- Protección de los derechos de propiedad intelectual de la organización, tanto por el software como por otros contenidos que puedan estar protegidos por derechos de propiedad intelectual.
- Proceso de devolución de datos y equipamiento en caso de finalización del empleo.
- Nivel mínimo de configuración de la instalación donde se realizarán las actividades de teletrabajo.
- Tipos de actividades permitidas y prohibidas.

**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.0001 Guía de usuario. | 3 años | Resp. del Sistema |
| RSI.0002 Declaración de aplicabilidad. | 3 años | Resp. del Sistema |

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