PSI-03 Control de Acceso

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 **CLINICA BEIMAN** para establecer las reglas de acceso para diversos sistemas, equipos, instalaciones e información en base a los requerimientos legales, de negocios y de seguridad.

0.1. Entradas y salidas del proceso

Entradas:

- Necesidad de controlar los accesos a los sistemas de información.
- Necesidad de definir los privilegios y permisos de los usuarios para el desarrollo de sus tareas.
- Necesidades de preservar la información y recursos de información de la empresa.

Salidas:

- Permisos de usuario.
- Sistema de gestión de contraseñas.
- Mecanismos de identificación y autenticación.

1. Políticas y reglas de control de acceso

La totalidad de las reglas especificadas en este proceso serán de obligado cumplimiento, salvo autorización expresa y por escrito del Responsable de Seguridad. El cumplimiento de lo definido en el presente procedimiento debe permitir cumplir con la Política de Control de Accesos desarrollada por **CLÍNICA BEIMAN.**

Todas las tareas relacionadas deben realizarse siempre y en todo momento para controlar el acceso al sistema operativo, a los sistemas empresariales y a las redes que los conectan. No obstante, siempre que sea posible, estas reglas son extendidas a los módulos de administración y gestión de accesos de cualquiera de las aplicaciones o recursos que la organización usa para su operativa diaria.

Responsable: Todo el personal

2. Gestión de identidades

Se deberá asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información (equipos informáticos, aplicaciones, utilidades, soportes de almacenamiento, etc.).

Se identificará a los usuarios de la organización y se registrará indicando nombre de usuario, área, puesto desempeñado…, y también se identificarán de los sistemas a los que dispondrá de acceso, asignación de derechos, permisos, etc. considerando la totalidad de sistemas o recursos disponibles en la empresa. Este acceso será definido por el Responsable de RRHH y comunicado al Responsable de Seguridad quién creará el usuario correspondiente en servicio de directorio Activo, creando una contraseña inicial de un solo uso, quedando sometido a la política de contraseñas del Sistema.

.

SOLO EN CASO DE ESTABLECER DIFERENTES MAPEOS DE RED.

Cabe indicar en este apartado que **CLÍNICA BEIMAN** posee una serie de recursos previamente definidos por el Responsable de Seguridad a los cuales los correspondientes usuarios tendrán acceso una vez dados de alta en el sistema. En concreto existen X mapeos de red con acceso a unos u otros recursos, a saber:

1. **Recursos comunes:** Adobe Reader, , Office 365, Navegadores, WinRar, Software gestión pacientes, etc.
2. **Recursos ÁREA XXXXX:** SEÑALAR software específico para determinados trabajos puntuales para los cuales se adquiere licencia temporal O NO
3. **Recursos ÁREA YYYY**: IDEM

Para el registro de estas asignaciones de acceso a los usuarios se utilizará el formato **RSI.0303 Accesos de usuarios** (mediante el cual se registrarán igualmente las bajas y modificaciones de acceso)

Responsable: Responsable de Seguridad de la Información

3. Responsabilidades de los usuarios

Todo el personal o terceros con acceso a las aplicaciones, sistemas o red de **CLÍNICA BEIMAN**, deberán conocer y cumplir con **RSI.0301 Política de control de accesos** y con **RSI.0302 Política de gestión de contraseñas**, donde se dictan pautas sobre derechos y deberes con respecto al uso adecuado por parte de los usuarios respecto a los permisos y privilegios, así como a las normas de uso seguro de contraseñas.

Responsable: Todo el personal

4. Gestión de Privilegios

El principio básico es que el acceso a todos los sistemas, redes, servicios e información está prohibido salvo que sea expresamente permitido a usuarios individuales por necesidades asociadas al desarrollo de sus funciones, quedando ello reflejado en el **RSI.0303 Accesos de usuarios**.

Al asignar privilegios se tendrán en cuenta los requerimientos de negocio y de seguridad para el acceso (definidos en la evaluación de riesgos), como también la clasificación de la información a la que se accede con esos derechos de acceso, de acuerdo con clasificación de información establecida.

Responsable: Responsable de Seguridad de la Información

4.1. Proceso de solicitud de alta, baja o modificación perfil de usuario

Cualquier tipo de solicitud de acceso (alta, modificación, baja, cambio de perfil, etc.) a los sistemas de información de **CLÍNICA BEIMAN** (puestos de usuario, aplicaciones, intranet, etc.) debe ser gestionada y autorizada por los responsables correspondientes (Responsable de RRHH), siempre en función de las necesidades específicas del puesto de trabajo al que vaya dirigido el acceso.

Ante altas de nuevos trabajadores en la empresa, la solicitud de acceso se remitirá por parte del área de RRHH a los responsables encargados de su aprobación, así como a los Responsables de Sistemas o proveedor externo IT a través de la herramienta de ticketing TRS o vía web, quienes asignarán acceso a los recursos mínimos necesarios y realizarán los correspondientes cambios en el Directorio Activo del sistema operativo, o de las aplicaciones o sistemas de información. Los accesos adicionales según las necesidades de su puesto, serán solicitados por el Responsable de cada área (previa evaluación y autorización), y aprobados por el responsable de RRHH.

Debe de quedar información documentada de los diferentes privilegios y derechos asignados a los usuarios (acceso a equipos informáticos, acceso a aplicaciones, acceso a soportes y dispositivos móviles, etc.) para lo cual se utilizará el formato **RSI.0303 Accesos de usuarios**.

Las solicitudes de alta de usuario o permisos (o de bajas y modificaciones de los mismos), deberán realizarse a través de la herramienta de Ticketing GLPI/vía web o a través de algún medio que permita conservar su registro y su trazabilidad. La información mínima que deberá contener este mail será:

- Nombre y apellidos usuario.
- Departamento/área destino.
- Recursos adicionales opcionales
- Nombre de coordinador asignado o responsable del usuario.

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

4.2. Provisión de acceso de usuario

Cada usuario estará identificado de manera inequívoca con una cuenta de acceso. Esta cuenta es personal e intransferible con el fin de permitir que el sistema de acceso mantenga la trazabilidad, y se permita únicamente el acceso a usuarios controlados y autorizados. Por tanto, no están permitidas cuentas genéricas o compartidas, a no ser que éstas estén formalmente autorizadas y sujetas a controles compensatorios.

El sistema de autenticación principal se lleva a cabo mediante la combinación de usuario y contraseña.

Responsable: Responsable de Seguridad de la Información

4.3. Gestión de la información secreta de autenticación

En **CLÍNICA BEIMAN**, se ha definido una Política de Contraseñas Seguras con la idea de garantizar un uso seguro de las mismas, y que debe ser conocida por todos los usuarios con

acceso a los sistemas de información. Se debe asegurar una distribución segura de las contraseñas a los usuarios.

Inicialmente a los usuarios se les facilitarán unas credenciales de acceso que deben ser modificadas en el primer inicio de sesión definiendo el usuario una contraseña que sólo el conozca, y que se ajuste a lo definido en la Política de Contraseñas.

En **CLÍNICA BEIMAN** cuentan con el software de almacenamiento y seguridad de las contraseñas **KEEPASS**, que permite que las mismas permanezcan cifradas, de manera que únicamente el Responsable de Seguridad y por un tiempo limitado, tiene acceso a las mismas.

Responsable: Responsable de Seguridad de la Información

5. Supervisión: Revisión, retirada y reasignación

Los propietarios de los sistemas y e instalaciones que requieren derechos de acceso deben revisar si los permisos concedidos se mantienen de acuerdo a los requerimientos de negocios y de seguridad.

Las revisiones se deben realizar de manera periódica a la totalidad de usuarios que tengan acceso a los sistemas, redes e información. Estas revisiones son documentadas y, en caso de detectar anomalías, deben de gestionarse según el proceso gestión de incidencias de seguridad.

Las tareas realizadas con estas revisiones son relativas a:

- Revisión de los derechos de acceso de los usuarios semestralmente y después de cualquier cambio.
- Revisar semestralmente las autorizaciones de derechos de acceso con privilegios especiales.
- Asegurar semestralmente que no se han obtenido privilegios no autorizados.

Cuando se produce un cambio o finalización de empleo se debe informar a la persona que autorizó los privilegios del empleado para que proceda a suprimir o modificar inmediatamente los permisos de acceso inicialmente designados.

Nota. Cuando se modifican las relaciones contractuales con entidades externas que tienen acceso a sistemas, servicios e instalaciones, o cuando finaliza el contrato, el propietario del contrato debe informar inmediatamente a las personas que autorizaron los privilegios de dichas entidades externas.

Las modificaciones y supresiones de accesos de los usuarios, deberán de quedar registradas en **RSI.0303 Accesos de usuarios**.

Responsable: Responsable de Seguridad de la Información

6. Procedimientos seguros de inicio de sesión

El acceso a los recursos de una división concreta dentro de **CLÍNICA BEIMAN** (puestos de usuario, sistemas operativos, aplicaciones, etc.) se encuentra protegido mediante la necesidad de uso de usuario y una contraseña de acceso segura. Los sistemas se encuentran configurados para que, inicialmente, no se muestre información referente a esta información de acceso, debiendo el usuario de completarla para cada inicio (en especial, los sistemas de acceso no muestran la contraseña introducida por los usuarios)

El sistema operativo de los equipos, conserva información sobre los accesos realizados (con éxito o fallidos).

El sistema de gestión de contraseñas y control de usuarios se encuentra configurado para que exista un número máximo de intentos de acceso, tras el cual la sesión se bloquea.

Responsable: Responsable de Seguridad de la Información

7. Sistema de gestión de contraseñas

Se ha definido una política de contraseñas seguras que garantiza un uso adecuado de las mismas. A cada usuario se le asigna una contraseña inicial de modo que se asegure que no puede ser conocida por nadie más. Esta contraseña inicial debe cambiarse en el primer inicio de sesión, eligiendo el usuario una nueva contraseña que se ajuste a la política de contraseñas definida.

Responsable: Responsable de Seguridad de la Información

7.1. Definición de criterios

Los criterios a aplicar para la gestión de contraseñas son los siguientes:

- Longitud mínima 13 caracteres, utilizando tres de los siguientes bloques: Mayúsculas, Minúsculas y Números
- Vigencia máxima de la contraseña: 90 días
- Vigencia mínima: 1 día
- Bloqueo tras cinco intentos fallidos durante 5 minutos
- Cada vez que se cambie la contraseña esta debe ser distinta por lo menos de las últimas 13 anteriores.

Las cuentas de nueva creación se bloquearán permanentemente tras inactividad inicial.

La sintaxis de las contraseñas será la definida en la política de contraseñas establecida en **CLÍNICA BEIMAN.**

Todas las contraseñas de sistema (cuentas de administrador, cuentas de administración de aplicaciones, interacciones críticas, etc.) deberán cambiarse con una periodicidad de al menos una vez cada tres meses. El sistema forzará al cambio de contraseña cuando proceda. El sistema recordará al usuario que debe cambiar la contraseña 15 días antes de que caduque.

Todas las contraseñas de usuario (cuentas de correo, cuentas de servicios web, etc.) deberán cambiarse en un plazo marcado según aplicación e indicado en la política de contraseñas. Si se sospecha que una contraseña haya sido revelada, se cambiará inmediatamente, por el administrador.

NOTA. *Las cuentas de usuario que tengan privilegios de sistema, deberán tener contraseñas distintas a otras cuentas mantenidas por dicho usuario en los servicios y recursos.*

En la medida de lo posible, las contraseñas serán generadas automáticamente con las características recomendadas en esta política y se les comunicará a los usuarios su contraseña siempre en estado "expirado" para obligar al usuario a cambiarlo en el primer uso que hagan de la cuenta o servicio.

Responsable: Responsable de Seguridad de la Información

7.2. Auditoría

Para poder detectar posibles amenazas, los procedimientos de auditoría deberán permitir la correcta identificación del usuario que acceda al sistema de información, así como la ubicación, la fecha y la hora en la que ocurrió el acceso, si el sistema ha concedido o denegado el acceso y, si procede, la transacción realizada.

Esta información deberá ser almacenada en ficheros específicos (log de usuarios) para consultar online, por un periodo de tiempo mínimo de 6 meses.

Para ello, deberá activarse en el sistema de información del equipo controlador, el registro de sucesos o incidencias que permita conocer los accesos al sistema o cambios de privilegios de la siguiente forma:

- Auditar el uso de privilegios: correctos y erróneos.
- Auditar la administración de cuentas: correctos y erróneos.
- Auditar sucesos de inicio de sesión: erróneos.
- Auditar sucesos de inicio de sesión de cuenta: correctos y erróneos.
- Auditar el cambio de directivas: correcto.

NOTA. *Para los equipos que tienen su propia base de datos de configuración, al mismo efecto, deberán retener la información de registro de accesos oportuno durante al menos 2 meses.*

Responsable: Responsable de Seguridad de la Información

8. Uso de utilidades con privilegios de sistema

Para prevenir que las aplicaciones efectúen cambios en áreas clave del sistema operativo sin autorización, se configurará el sistema operativo del servidor de tal forma que se restrinja de manera predeterminada los permisos de parte de ellas, todo equipo que sea puesto en funcionamiento, tanto en ambientes productivos como no productivos, deberá contar con las medidas de seguridad mínimas requeridas.

Controles mínimos de Seguridad requeridos:

- Configuración de perfiles y privilegios de grupo.
- Eliminación de servicios no utilizados.
- Configuración de banners de acceso.
- Eliminación de servicios y protocolos no seguros.
- Estandarización de nombre de host.
- Alta de monitores de seguridad.
- Aplicación de hardening estándar.
- Ejecución de análisis de vulnerabilidades.
- Remediación de vulnerabilidades identificadas.
- Eliminación de cuentas y contraseñas de fábrica.

Responsable: Responsable de Seguridad de la Información

9. Control de acceso al código fuente de los programas

Se deberá tener en cuenta si los programas informáticos en su licencia permiten que el código fuente esté disponible para que cualquiera pueda estudiarlo, modificarlo o reutilizarlo. Cuando se cumple este aspecto se dice que el programa es de código abierto y son, en general, software libre, en contraposición al software privado en el que el usuario tiene limitaciones para usarlo, modificarlo o redistribuirlo.

CLINICA BEIMAN no dispone de equipo de desarrollo propio, por lo que no existirá ningún código fuente de programa que gestione la propia clínica.

Responsable: Responsable de Seguridad de la Información

10. Formatos y anexos

Descripción	Tiempo de archivo de los registros que genera	Responsable
RSI.0301 Política de control de accesos	3 años	Resp. del Sistema
RSI.0302 Política de gestión de contraseñas	3 años	Resp. del Sistema
RSI.0303 Acceso de usuarios	3 años	Resp. del Sistema

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