PSI-07 Seguridad de las Operaciones

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

0. Objeto

El objetivo de este proceso es garantizar el funcionamiento correcto y seguro de las tecnologías de la información y las operaciones de tratamiento en **CLÍNICA BEIMAN**.

0.1. Entradas y salidas del proceso

Entradas:

- Necesidad de controlar y gestionar de forma segura los sistemas de tratamiento de información.
- Necesidad de respaldar la información y realizar copias de seguridad.
- Necesidad de gestionar las vulnerabilidades de los sistemas.

Salidas:

- Definición de políticas de uso aceptable de los sistemas de información.
- Funcionamiento correcto y seguro de las instalaciones de tratamiento de información.
- Definición de procedimientos para la gestión de vulnerabilidades técnicas.
- Procedimientos de copias de seguridad.
- Gestión de la capacidad.
- Auditorías de los sistemas.

1. Gestión de las capacidades

El Responsable de Seguridad será el encargado de alcanzar una comprensión del consumo de recursos debido a la carga de trabajo en los sistemas de información (principalmente equipos servidores).

La gestión de la capacidad de los sistemas se llevará a cabo mediante herramientas específicas de conexión remota a servidores y gestión de tareas correspondientes, consulta de logs y revisión de registros. De este modo se conoce el rendimiento y capacidad de los equipos (incluyendo capacidad de almacenamiento, consumo de memoria RAM, consumo de red, rendimiento…) software PRTG basado en el envío de sonda para monitorización de equipo a través de tecnología WMI

La gestión de la capacidad se realizará con especial dedicación en los equipos servidores, teniendo como cometido el monitorizar en tiempo real el comportamiento de los sistemas principales, así como evaluar, resolver y proyectar las necesidades de los sistemas a fin de evitar que la información pueda dejar de estar disponible en un momento dado.

En cuanto a los equipos de usuarios, los administradores tienen como responsabilidad revisar periódicamente su capacidad, en relación a disco duro, memoria RAM y velocidad del procesador.

Sus criterios, a la hora de determinar las necesidades de incremento de capacidad de alguno de los sistemas deben estar basados en todo momento en datos objetivos, para poder ser aprobados por el Responsable de Seguridad o la dirección.

Las evidencias de las revisiones realizadas sobre la capacidad de los equipos, se registrarán en el formato **RSI.0701 Mantenimiento de equipos**.

Responsable: Responsable de Seguridad de la Información

2. Separación de los recursos de desarrollo, pruebas y operación

En **CLÍNICA BEIMAN** ante la adquisición de nuevo software que deba ser probado, se dispone de un entorno de pruebas (máquinas virtuales) separado del entorno de trabajo o de producción. Igualmente, se dispone de puestos de usuario de prueba. El Responsable de Seguridad se asegura de realizar las pruebas necesarias en estos entornos antes de proceder al despliegue del software en los equipos de trabajo (entorno de producción), y tras verificar que el mismo no introducirá riesgos o provocará pérdidas de integridad sobre los equipos, sistemas u otro software del entorno de producción.

Responsable: Responsable de Seguridad de la Información

3. Protección contra código malicioso

La protección contra código malicioso se basa en la detección del mismo y la reparación del software dañado, complementando con una mayor concienciación y estableciendo controles de acceso a los sistemas. Para el control del código malicioso en los sistemas informáticos, en **CLÍNICA BEIMAN** se consideran las siguientes medidas de seguridad:

- Todos los equipos disponen de antivirus instalado y configurado para actualización automática. Los usuarios utilizan diferentes versiones de Windows como por ejemplo XP pro, 7 pro,8.1, 10home, 10student, 10pro, y 11que se migrará a Windows 10pro bajo dominio de un Windows Server 2022 con un Endpoint de Eset antivirus+antimalware Adicionalmente se utiliza un Firewall cargado en el software de UniFi en la UDM y que forma parte de una de las capas de protección del citado Firewall. El viernes de cada semana se realiza una comprobación de las actualizaciones.
- Durante el mantenimiento de los equipos, se realizará una revisión de la correcta instalación y actualización de los sistemas antivirus, y se valorará la realización de un análisis para detectar software malicioso. Estas revisiones se registrarán en **RSI.0701 Mantenimiento de equipos.**
- El Responsable de Seguridad revisarán periódicamente los registros o logs de los sistemas antivirus para detectar posibles incidencias o tendencias al respecto.
- El software antivirus permitirá el escaneo de los soportes de almacenamiento que se conecten y el correo electrónico de los usuarios El propio antivirus o herramientas adicionales, se utilizarán para controlar el spyware y spam.

- Se definen procedimientos y responsabilidades de gestión para el tratamiento de los sistemas contra el código malicioso, formación en el uso, informe y recuperación de los ataques de código malicioso.
- Preparación de planes de continuidad de negocio para la recuperación de los ataques de código malicioso, donde se incluirán todos los datos y software de copia de seguridad.
- Se implantan procedimientos para la recogida de información con especial interés en ataques por código malicioso (listas de correo, boletines especializados) según **PSI.00 Organización de la seguridad de la información**.
- Se conciencia al personal en relación a buenas prácticas para evitar incidentes derivados de virus.

Responsable: Responsable de Seguridad de la Información

4. Registro y supervisión de eventos de seguridad

En **CLÍNICA BEIMAN** se revisan los registros de los sistemas a fin de evaluar los posibles eventos de seguridad y detectar incidencias o posibles tendencias sobre las que sea preciso actuar.

El Responsable de Seguridad revisará los registros de los sistemas operativos (visor de eventos) y los registros de las aplicaciones utilizadas en la organización. Adicionalmente la organización dispone de herramientas de monitorización de la red mediante herramientas integradas en sistema Unifi del Dream Machine Pro.

Adicionalmente se revisarán los registros de otros recursos como el firewall, los accesos VPN u otros dispositivos de red.

Con carácter general, se revisan la información de registros de:

- Registros e información sobre intentos fallidos o exitosos de acceso.
- Actividades realizadas de los usuarios y uso de privilegios.
- Acceso a objetos.
- Sucesos del sistema.
- Instalaciones o cambios de configuración de los sistemas.

Los sistemas están configurados para conservar estos registros de manera automatizada.

Se conservan igualmente los registros de las actividades realizadas por los administradores, las cuales serán revisadas por el Responsable de Seguridad.

A los mecanismos de monitorización sólo tienen acceso el personal perteneciente al proveedor de IT que disponen de cuentas individuales con permisos suficientes para poder conceder y alterar los accesos al sistema y recursos, pero no para alterar los registros log que estos mecanismos generan. Adicionalmente, se realizan copias de seguridad de esta información.

Responsable: Responsable de Seguridad de la Información

5. Sincronización de relojes

Se han definido las políticas y directivas necesarias para que los equipos informáticos sincronicen sus relojes con el servidor de la organización, a fin de, entre otros aspectos, asegurar la integridad y la eficacia de los eventos y registros de los sistemas. Adicionalmente, los equipos servidores se encuentran sincronizados con sistemas externos de sincronización horaria a fin de disponer una trazabilidad con una hora oficial. A este efecto se utiliza el servidor NTP interno que conecta con la hora estándar.

Responsable: Responsable de Seguridad de la Información

6. Control de software en explotación

Antes de introducir un equipo en un entorno de producción deben considerarse las siguientes medidas de seguridad:

- Formateo de los medios de almacenamiento de información, especialmente en equipos reutilizados.
- Deshabilitar las cuentas por defecto (por ejemplo, Administrador en sistemas Windows) siempre que sea posible. Cuando las cuentas no puedan ser deshabilitadas deberán establecerse contraseñas robustas para estas cuentas.
- En el caso de elementos de red (routers, switches, firewall) deben modificarse:
    - Contraseñas de las cuentas de acceso a los paneles de administración.
    - Cuando aplique las contraseñas de acceso a la conectividad inalámbrica.
    - Comunidad por defecto (public/guest) siempre que el protocolo SNMP esté habilitado.
- Se configurarán usuarios con permisos limitados, de manera que la instalación de software o la modificación de la configuración del sistema solo pueda ser realizada por administradores informáticos y no por los propios usuarios.
- Se instalarán y/o configurarán solo las aplicaciones que el usuario necesite para acceder a la información a la que se le ha concedido el acceso, de acuerdo a **PSI.03 Control de acceso**.
- Todos los puestos de usuario y servidores (independientemente del sistema operativo) disponen de sistema antivirus que se actualiza de manera automática desde la consola de Eset.
- Se configurarán todos los equipos para que se bloqueen tras un periodo de inactividad. Será necesario autenticarse nuevamente ante el sistema para poder desbloquear el equipo.
- En los servidores de dominio debe configurarse un cierre de las sesiones tras periodo de inactividad.

- Se asegurará que se define la correcta configuración de los equipos informáticos, de modo que se asegure una configuración de seguridad en consonancia con los requisitos de seguridad.
- Para garantizar un correcto funcionamiento de la infraestructura y ayudar a reducir el número de incidentes, se realizarán tareas de mantenimiento preventivo con carácter periódico, que se desarrollarán según lo definido en **PSI.06 Seguridad de los equipos**, dejando evidencia en el registro **RSI.0601 Mantenimiento preventivo.**

Mediante la definición de permisos y privilegios se impedirá modificar la configuración de seguridad de los equipos. Las nuevas instalaciones de software o los cambios en la configuración de los equipos, deberán de ser supervisadas y autorizadas por los responsables, y deberán de ajustarse a lo definido en **PSI.08. Gestión de Cambios**.

Responsable: Responsable de Seguridad de la Información

7. Gestión de vulnerabilidades y auditoría de los sistemas

Ante la aparición de nuevos parches o actualizaciones de seguridad se estudiará la conveniencia de instalarlos, considerando el efecto que estos podrían tener en el resto del sistema. En ocasiones puede ser conveniente retrasar la instalación para evaluar los riesgos asociados según la experiencia de otros usuarios.

En CLÍNICA BEIMAN las actualizaciones automáticas de Windows se encuentran deshabilitadas. Con las fechas de emisión mensual de los parches de Windows, las actualizaciones se instalan en las plantillas virtuales de la máquina de referencia para luego reflejarlas en los puestos de usuario.

La instalación de software queda terminantemente prohibida en CLÍNICA BEIMAN. Únicamente los perfiles de administrador (personal Dpto. IT) tienen esta opción.

El responsable del sistema supervisará la correcta realización y eficacia de estas actualizaciones.

El responsable de seguridad recibe notificaciones periódicas mediante correo electrónico de los respectivos fabricantes acerca de las vulnerabilidades que afecten al software o hardware utilizado en la empresa.

Por otra parte, el responsable de Seguridad se mantendrá informado de las vulnerabilidades que puedan afectar a los sistemas de información, a través de las entidades especializadas en la materia (INCIBE, AGPD…) según lo definido en **PSI.00 Organización de la seguridad de la información.**

Durante las actividades de mantenimiento de los equipos, se revisará que los sistemas operativos y otros softwares de los equipos se encuentran correctamente configurados, dejando evidencias en los registros **RSI.0603 Mantenimiento preventivo de ciberseguridad**, **RSI.0602 Mantenimiento preventivo de sistemas** y **RSI.0601 Mantenimiento de equipos.**

Adicionalmente se valorará la necesidad de realizar de manera periódica auditorías de vulnerabilidades mediante software específico, así como de tests de intrusión o hacking ético según las necesidades.

Responsable: Responsable de Seguridad de la Información

8. Copias de seguridad

En CLÍNICA BEIMAN se realizan copias de seguridad periódicas de la información centralizada en discos HDD externos, y en nube. Se realizan copias completas de carácter diario del controlador de dominio, las cuales están programadas de una forma progrseiva. Cada hora se realizará una copia incremental de los datos del servidor de datos, se realizará una copia quincenal completa y una mensual completa. También se realizará una copia semanal del proxmox (servidor de virtualización). Y referente a las máquinas virtuales instaladas se realizará una copia semanal. Sobre el Sistema Kairos se realiza una copia de la máquina virtual y datos diariamente y la BBDD cada 5 minutos. Para la realización de copias de seguridad se utiliza un software específico (Duplicati) el cual dispone de un registro de las copias realizadas que debe ser revisado periódicamente por el Responsable de Seguridad (en caso de que no se disponga de software que conserve registro, la realización de las copias se evidenciará en el registro asociado Adicionalmente el software de copias envía notificaciones por correo electrónico al Responsable de Seguridad de la correcta realización de las copias.

Es responsabilidad de cada usuario guardar todos los datos fruto de su actividad (comercial, técnica o administrativa) en el servidor, con el fin de que queden registrados en las copias de seguridad.

Cuando por motivos de administración o cambio de sistema se tenga que formatear o reinstalar un puesto de trabajo, se hará una copia previa de los datos contenidos en el mismo en un disco duro auxiliar. Esta tarea será llevada a cabo por el Responsable de Seguridad.

Responsable: Responsable de Seguridad de la Información

9. Restauración de copias de seguridad

La restauración parcial o completa de las copias de seguridad debe ser previamente autorizada por el Responsable de Seguridad, indicando la incidencia que motiva la misma. El proceso de recuperación de datos, será realizado por personal del departamento IT debidamente autorizado. La información de la restauración de la copia quedará registrada en el registro **RSI.0701 Restauraciones de seguridad**.

El proceso de restauración por pérdidas de información u otras incidencias deberá de generar el correspondiente registro de incidencias.

Responsable: Responsable de Seguridad de la Información

10. Pruebas de restauración de copias de seguridad

Con periodicidad **semestral** se realizarán pruebas de restauración que contemplen diferentes escenarios y sistemas para asegurarse de la correcta ejecución de las copias de seguridad. La recuperación de datos se realizará en una ubicación secundaria y no sobre los ficheros originales, o se renombrarán previamente los ficheros originales si se restaura sobre la misma ubicación. Este procedimiento será realizado por personal técnico autorizado, tomando la copia de respaldo más

reciente disponible (o aquella que sea adecuada). La información de la prueba de restauración de la copia quedará registrada en el registro **RSI.0701 Restauraciones de seguridad**.

Responsable: Responsable de Seguridad de la Información

11. Formatos y anexos

Descripción	Tiempo de archivo de los registros que genera	Responsable
RSI.0601 Mantenimiento de equipos.	3 años	Resp. del Sistema
RSI.0602 Mantenimiento preventivo de sistemas	3 años	Resp. del Sistema
RSI.0603 Mantenimiento preventivo de ciberseguridad	3 años	Resp. del Sistema
RSI.0701 Restauraciones de seguridad.	3 años	Resp. del Sistema

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