PSI-08 Gestión de Cambios

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

0. Objeto

El objetivo de este proceso es el de asegurar que todos los cambios realizados en **CLÍNICA BEIMAN** son valorados, aprobados, implementados y revisados de una manera controlada.

0.1. Entradas y salidas del proceso

Entradas:

- Necesidad de gestionar los cambios que afecten al negocio, instalaciones y sistemas de información.

Salidas:

- Peticiones y autorizaciones de cambios.
- Registros de cambios.

1. Petición y registro del cambio

En CLÍNICA BEIMAN todos los recursos asignados se encuentran diferenciados por mapeos de red. Aun así, no todos los usuarios definidos en cada mapeo, disponen de todos los recursos definidos para el mismo. Cada recurso ha de ser autorizado por el correspondiente Responsable de Área y/o Responsable de Recursos Humanos.

Para tener acceso a determinados recursos (pej. teletrabajo) deberá ser únicamente el Responsable de Área quien solicite este recurso al Responsable de Recursos Humanos quién autorizará este cambio para proceder a su gestión.

Los trabajadores de **CLÍNICA BEIMAN** poseen la herramienta de gestión de tickets GLPI para la gestión de estas solicitudes. Cada solicitud debe indicar:

- Área desde la que se solicita.
- Identificación del solicitante: nombre e email.
- Asunto de la solicitud.
- Mensaje: explicación de la solicitud, motivos, necesidad etc.
- Datos adjuntos: si fueran necesarios para una mejor comprensión de la petición.

Una vez enviada, la solicitud se completa de forma automática o por el Responsable de Seguridad con la siguiente información:

- ID de seguimiento.
- Número de ticket.
- Propietario o responsable del cambio.
- Estado.
- Fechas de creación, actualización y vencimiento.
- Tiempo dedicado.
- Número de respuestas e histórico de mensajes intercambiados. (configurar según GLPI)

Responsable: Todos los usuarios

2. Clasificación de los cambios

CLÍNICA BEIMAN identifica los siguientes tipos de cambios:

- Cambios **"estándar"** o **"pre-aprobados":** todos los cambios recurrentes, conocidos, y de escaso impacto en los procesos de negocio, instalaciones de tratamiento de la información y los sistemas.
- Cambios **menores:** todos aquellos que no sean estándar, pero que sean de bajo impacto, en los procesos de negocio, instalaciones de tratamiento de la información y los sistemas.
- Cambios **mayores:** son aquellos que suponen un alto impacto en la organización, en los procesos de negocio, instalaciones de tratamiento de la información y los sistemas.

El Responsable de Seguridad es el encargado de clasificar el cambio una vez recibida la solicitud.

Responsable: Responsable de Seguridad de la Información

3. Cambios "estándar" o "preaprobados"

Entre ellos se encuentran:

- Actualizaciones de sistema operativo y de aplicaciones.
- Gestión de altas, modificaciones y bajas de usuario solicitadas por RRHH o Responsables de área.
- Instalación de herramientas de software autorizadas solicitadas por los Responsables de área.
- Mantenimiento de hardware y software.
- Actualizaciones de la documentación y/o procedimientos.

Responsable: Responsable de Seguridad de la Información

4. Cambios menores

Entre ellos se encuentran:

- Ampliación o asignación de nuevos equipos, periféricos o elementos de telefonía.
- Cambios de versión.
- Traslado de puesto.
- Habilitar nuevo punto de red.

Responsable: Responsable de Seguridad de la Información

5. Cambios mayores

Entre estos cambios se encuentran:

- Ampliación o cambios de envergadura de la infraestructura tecnológica.
- Cambios en la configuración de activos importantes.
- Cambios en un servicio o en los componentes de un servicio.

Responsable: Responsable de Seguridad de la Información

6. Restricciones paquetes de software

No se realizan modificaciones ni cambios en los paquetes de software de terceros.

Se prohíbe el uso y/o copia de cualquier paquete de software, por parte de los usuarios, del cual no se disponga de su respectiva licencia que lo autorice.

La instalación de paquetes de software “OPEN” debe ser autorizada por el Responsable de Seguridad que asegurará que se cumplen los requisitos de herramientas de software utilizados por **CLÍNICA BEIMAN**.

Responsable: Responsable de Seguridad de la Información

7. Aprobación de cambios

Según la clasificación del cambio efectuada, se actuará de la siguiente forma:

- En el caso de los cambios pre-aprobados, no es necesaria la aprobación explícita, puesto que se encuentran pre-aprobados por defecto.
- En el caso de los cambios menores, deben ser autorizados por el Responsable de Seguridad, que debe evaluar su justificación para el negocio y las potenciales consecuencias negativas sobre la seguridad.
- En el caso de los cambios mayores, el Responsable del Sistema junto con el Responsable de Seguridad deberá informar sobre los costes del cambio a Dirección, quién será el responsable de autorizar o no el cambio.

Las modificaciones a los paquetes de software o sistemas adquiridos a terceros, que surjan producto de su explotación y tengan relación con la seguridad de la información, deben ser aprobados por el Responsable de Seguridad.

Responsable: Responsable de Seguridad de la Información

8. Análisis del impacto

Una vez que la solicitud se admite a trámite, es necesario llevar a cabo una evaluación del impacto para determinar si el cambio tendrá un impacto importante o no sobre el servicio o la propia organización. Analizándose los siguientes aspectos:

- Impacto general sobre el servicio/producto/negocio/recursos de información.
- Activos afectados.
- Impacto en la seguridad de la información en términos de confidencialidad, integridad y disponibilidad.
- Identificación de nuevos riesgos que pueden introducirse o de cambios sobre los riesgos identificado actualmente.
- Recursos necesarios.
- Plazos.
- Coste.

En caso de cambios cuyas consecuencias pueden resultar relevantes, se valorará la necesidad de realizar un análisis de riesgos según lo dispuesto en **P.02 Gestión de riesgos**.

Responsable: Responsable de Seguridad de la Información

9. Prioridad del cambio

La prioridad del cambio será determinada en función del impacto del mismo sobre la organización, de los beneficios de este para los servicios o para la seguridad de la información, y de los recursos necesarios para afrontar dicho cambio, pudiéndose priorizar de acuerdo a los 3 grupos siguientes:

- Prioridad Baja: Cambio relativamente común, sin impacto ni beneficios relevantes en la seguridad de la información y en la prestación de servicios. Tampoco existe urgencia en realizar el cambio.
- Prioridad Media: es un cambio detectado para mejorar en funcionamiento del sistema y que puede favorecer la seguridad de la información y la prestación de servicios.
- Prioridad Alta: el cambio debe ser implementado relativamente rápido pues es necesario para asegurar la seguridad de la información o para la prestación eficaz de los servicios.

- Prioridad Crítica: El impacto en el sistema de seguridad de la información es alto y/o el tiempo en el que se debe implementar el cambio es bajo, por lo que requiere acción inmediata.

La prioridad será identificada en la apertura del ticket de cambio por el solicitante pudiendo ser modificada por el Responsable de Seguridad.

Responsable: Responsable de Seguridad de la Información

10. Identificación del equipo implementador del cambio

Una vez autorizado el cambio, clasificado y priorizado, se asignará el responsable o equipo que lo vaya a desarrollar quien tendrá que planificar el mismo, quedando constancia en el software GLPI**.**

Responsable: Responsable de Seguridad de la Información

11. Planificación del cambio

El Responsable de Seguridad, deberá de identificar en **GLPI,** la fecha probable de realización, y las tareas a desarrollar.

Utilizando la información cubierta hasta el momento, se describirán las acciones más importantes para que el cambio pueda llevarlo a cabo, realizando consultas con el interesado si fuera necesario.

Responsable: Responsable de Seguridad de la Información

12. Realización del cambio

El Responsable de Seguridad será el encargado de llevar a cabo el cambio, siguiendo la planificación establecida. Se realizarán las pruebas necesarias para comprobar si el cambio tiene el resultado esperado.

Responsable: Responsable de Seguridad de la Información

13. Verificación, revisión técnica y cierre del cambio

El Responsable de Seguridad verificará que los cambios se han implementado de acuerdo a lo planificado, y que este se ha implementado de modo eficaz y sin consecuencias negativas para los sistemas de información.

Se debe probar y verificar la estabilidad del sistema: el sistema no debe ser puesto en producción antes de haber realizado pruebas exhaustivas.

En el proceso de análisis y adquisición de paquetes de software a terceros, deben considerarse aspectos y atributos de seguridad de la información, y el impacto en la seguridad frente eventuales cambios o modificaciones para su implantación.

Se cierra el cambio cuando se haya completado todo el ciclo de manera satisfactoria.

Responsable: Responsable de Seguridad de la Información

14. Formatos y anexos

Descripción	Tiempo de archivo de los registros que genera	Responsable
Software GLPI para gestión de tickets, cambios, incidencias...	3 años	Resp. del Sistema

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