PSI-10 Requisitos de Seguridad

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

0. Objeto

El objetivo del presente documento es definir la sistemática establecida por **CLÍNICA BEIMAN** para identificar y controlar los requisitos de seguridad que deben de tenerse en cuenta en los sistemas de información que se adquieran en la organización.

0.1. Entradas y salidas del proceso

Entradas:

- Necesidad de garantizar la seguridad de la información en los sistemas nuevos y existentes, aplicaciones, redes públicas y en las transacciones en línea.
- Necesidad de controlar los servicios web y la información publicada.
- Necesidad de controlar los servicios de transacciones en línea.

Salidas:

- Identificación y registro de requisitos de seguridad.
- Medidas de control para los servicios a través de redes públicas.
- Medidas de control para las transacciones en línea.

1. Análisis de requisitos y especificaciones de seguridad de la información

Al adquirir nuevos sistemas de información (hardware, software o servicios), o cambiar los vigentes, se deben identificar aquellos requisitos de seguridad que deben de cumplir estos nuevos sistemas. Estos requisitos se documentarán en el registro **RSI.1001 Requisitos de seguridad.**

Entre estos requerimientos se considerarán aspectos como:

- Cómo evitar el acceso no autorizado.
- Requerimientos para respaldo de la información.
- Controles para acceso remoto.
- Transferencia segura de datos y mecanismos de control para enviar y/o recibir.
- Mecanismos para verificar la integridad de los datos.
- Cómo se reportan los errores.

Las nuevas adquisiciones o las actualizaciones de los sistemas de información, requerirá la revisión y posible identificación, análisis y evaluación de riesgos.

Además, las nuevas adquisiciones o las actualizaciones de los sistemas de información, deberán de ajustarse, en la medida que sea necesario, con lo definido en la **PSI.08 Gestión de cambios** en cuanto al proceso de autorización, seguimiento, clasificación, priorización, etc.

Antes de la puesta en marcha de un nuevo sistema, el Responsable de Seguridad, en colaboración con el Responsable del Sistema, deben asegurar que se cumplen los requisitos de seguridad, valorando como mínimo:

- El comportamiento y los requisitos de seguridad de los sistemas.
- Las mejoras detectadas tras la revisión de los sistemas de información.
- El impacto que podría tener su implantación sobre los que ya están en uso.

- Su facilidad de uso.
- La formación necesaria para el manejo de estos nuevos sistemas.
- La posibilidad de actualización, corrección de errores y exactitud de los datos de salida.

Responsable: Responsable de Segurida de la Información

2. Requerimiento de seguridad relacionados con redes públicas

En **CLÍNICA BEIMAN** no se disponen de servicios web a los clientes a través de redes públicas: tienda online, contratación online, etc.

Para la gestión global de nuestros pacientes, se utiliza el software KAIROS24h. Las medidas de seguridad implementadas son las de control de usuario y contraseña (alta de usuario), con la correspondiente personalización de acceso a contenedores en función del perfil del puesto.

El sistema permite la citación online de los pacientes, mediante el acceso a un portal público identificado con usuario y contraseña. También para la confirmación de la asistencia a citas, el paciente accede a una página web donde podrá confirmar o cancelar la asistencia. Para acceder a esta web, el paciente recibirá previamente un mensaje SMS a su teléfono personal.

También dispone de una bot de Whatsapp, donde los pacientes pueden consultar, cancelar y coger cita a través del programa de mensajería Whatsapp.

Asi mismo, disponemos de un bot telefónico, con el que los pacientes también pueden consultar, cancelar y coger cita, mediante llamada telefónica, de forma automática, sin intervención de operador humano.

Todos estos servicios, están integrados en Kairos24h, configurando las agendas que se quiera con la cita online.

Para la realización de videoconferencias y reuniones con clientes o entre personal de la empresa se usa Zoom con cifrado punto por punto en las diferentes sesiones organizadas.

En cuanto a transacciones con la administración pública, **CLÍNICA BEIMAN** dispone de certificado digital emitido por la FNMT para su uso en las distintas plataformas de la Administración.

Sobre estos servicios, el Responsable del Sistema, en colaboración con los responsables de área necesarios, se asegurarán de que se aplican las medidas de seguridad necesarias para:

- Garantizar el control de acceso para la publicación o modificación de estos servicios.
- Garantizar la confidencialidad de la información publicada.
- Garantizar la autenticación de las partes implicadas en los sistemas.
- Formalizar la relación contractual de estos servicios a través de los documentos o mecanismos necesarios.
- Asegurar la confidencialidad e integridad de la información intercambiada.
- Uso de conexión segura o canales cifrados (https).

Las medidas de seguridad existentes en los servicios por redes públicas se identificarán y evaluarán a través del proceso de análisis de riesgos. Ante la adquisición de nuevos servicios o modificación de los existentes, se identificarán los requisitos de seguridad a través del registro **RSI.1001 Requisitos de seguridad.**

Responsable: Responsable de Seguridad de la Información

3. Requerimientos de seguridad relacionados con transacciones en línea

CLÍNICA BEIMAN dispone de los siguientes servicios realizados a través de redes públicas:

- Compra online.
- Pago nóminas banco.
- Pasarela de pago
- Chipcard Tyrea
- SII

Sobre estos servicios, el Responsable de Seguridad, en colaboración con los responsables de área necesarios, se asegurarán de que se aplican las medidas de seguridad necesarias para**:**

- Asegurar la autenticación de los usuarios.
- Asegurar la integridad y confidencialidad de las transacciones.
- Evitar el direccionamiento erróneo.
- Evitar la transmisión de datos incompletos.
- Evitar la modificación no autorizada de mensajes.
- Evitar la duplicación no autorizada de mensajes.

Para ellos se aplican las siguientes medidas:

- Sistemas de identificación y autenticación.
- Uso de certificados digitales.
- Encriptado de información.
- Uso de canales de comunicación y protocolos seguros.

Las medidas de seguridad existentes en los servicios con transacciones en línea se identificarán y evaluarán a través del proceso de gestión de riesgos. Ante la adquisición de nuevos servicios o modificación de los existentes, se identificarán los requisitos de seguridad en **RSI.1001 Requisitos de seguridad.**

Responsable: Responsable de Seguridad de la Información

4. Requisitos de seguridad en servicios externos

Para la identificación y control de los requisitos de seguridad en servicios contratados externamente, se seguirá lo definido en la **PSI.12 Relación con proveedores**, y sus registros asociados.

Responsable: Responsable de Seguridad de la Información

5. Verificación de los requisitos de seguridad

Tras la puesta en marcha de los nuevos sistemas o las modificaciones sobre los existentes, el Responsable de Seguridad verificará que los mismos cumplen con los requisitos de seguridad identificados.

Periódicamente el Responsable de Seguridad verificará que los servicios a través de redes públicas así como los servicios de transacciones en línea cumplen con los requisitos de seguridad identificados.

Estos procesos de verificación, quedarán registrados a través del documento **RSI.1002 Verificación de Requisitos de seguridad.**

Responsable: Responsable de Seguridad de la Información

6. Formatos y anexos

Descripción	Tiempo de archivo de los registros que genera	Responsable
RSI.1001 Requisitos de seguridad.	Según proceda	Resp. del Sistema
RSI.1002 Verificación de Requisitos de seguridad.	Según proceda	Resp. del Sistema

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