PSI-11 Seguridad en el Desarrollo y Procesos de Soporte

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

0. Objeto

El objetivo de este proceso es definir las reglas básicas para desarrollo seguro de software y sistemas. Adicionalmente, incluye la gestión de los datos de prueba.

Este documento se aplica al desarrollo y mantenimiento de todos los servicios, arquitectura, software y sistemas que forman parte del Sistema de Gestión de la Calidad y Seguridad de la Información (SGCSI).

Nota. *Si bien* ***CLÍNICA BEIMAN*** *no desarrolla software, el Responsable de Seguridad que en la actualidad ejerce dicha tarea, es un proveedor externo IT cuyo software de gestión clínica KAIROS24h, es desarrollado directamente por este proveedor e implementa mejoras en el mismo según necesidad de nuestra organización. Este software de gestión es a día de hoy de vital importancia para la gestión global de nuestra actividad.* ***CLÍNICA BEIMAN*** *realiza revisiones y de pruebas de compatibilidad sobre software tras cada mejora implementada en el mismo, pero no sobre los entornos de desarrollo del proveedor/es.*

0.1. Entradas y salidas del proceso

Entradas:

- Necesidades de desarrollar aplicaciones y sistemas propios, así como realizar el mantenimiento de los mismos durante todo su ciclo de vida.

Salidas:

- Garantizar la seguridad de la información de las aplicaciones y sistemas desarrollados.

1. Desarrollo y mantenimiento del sistema y de las operaciones

Además de la evaluación de riesgos realizada según **P.02 Gestión de riesgos**, debe realizar periódicamente la evaluación de los siguientes aspectos:

- Las vulnerabilidades técnicas de los sistemas de IT utilizados en la organización.
- Los riesgos que puede traer una nueva tecnología si se utiliza en la organización.

Responsable: Responsable de Segurida de la Información

2. Principios de ingeniería segura

Se dispone de una política de desarrollo, que si bien no aplica para el desarrollo de nuevos sistemas, si lo hace para el mantenimiento de los sistemas existentes; también establecerá para cada aplicación o sistema los estándares mínimos de seguridad que se deben cumplir (validación de versiones, desarrollo de manuales según normativa, etc.).

Los mismos principios de ingeniería se aplicarán a los desarrollos externalizados y se incluirán en los contratos, como se indica en el proceso **PSI.12 Relación con proveedores**.

Responsable: Responsable de Seguridad de la Información

3. Entorno de desarrollo seguro

CLÍNICA BEIMAN no dispone de entorno de desarrollo seguro, puesto que no desarrolla software o aplicaciones.

Responsable: Responsable de Seguridad de la Información

4. Pruebas y aceptación de sistemas

Cuando se quiera implementar alguna aplicación o herramienta, siempre, deberán probarse en equipos o entornos de prueba, antes de proceder a su instalación en los sistemas utilizados para el tratamiento de la información. En el caso de que el producto a comprar no satisfaga los requisitos de seguridad, deberá considerarse de qué manera afectan los riesgos introducidos y si es posible reducirlos.

Esta prueba deberá documentarse en el registro **RSI-1102 Pruebas de aceptación de sistemas** que contendrá una descripción detallada de cada una de ellas, así como los resultados obtenidos.

Cada matriz de prueba realizada contendrá como mínimo:

- Paso.
- Acción realizada.
- Acción esperada.
- Resultado final.
- CSC: Sistema sobre el que se realiza la prueba.
- Nº de tarea.
- Entorno de pruebas.
- Fecha de prueba.
- Descripción de prueba.

Los datos de prueba son datos sintéticos, sin valor fuera del ámbito de las pruebas del sistema. Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo.

Para proteger los datos de prueba se establecerán normas y procedimientos que contemplen lo siguiente:

- Prohibir el uso de bases de datos operativas. En caso contrario se deben despersonalizar los datos antes de su uso. Aplicar idénticos procedimientos de control de acceso que en la base de producción.
- Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización.

- Eliminar inmediatamente, una vez completadas las pruebas, la información operativa utilizada.

Responsable: Responsable de Seguridad de la Información

5. Pruebas funcionales de seguridad

Nuestros proveedores de software, herramientas o aplicaciones, deberán llevar a cabo pruebas de seguridad de la funcionalidad durante el desarrollo de las mismas con el fin de detectar la existencia de vulnerabilidades que generen riesgos para la seguridad de la información o cualquier tipo de incidencia en su funcionalidad de acuerdo a los requisitos establecidos en **CLÍNICA BEIMAN**. En estas pruebas se tiene en cuenta aspectos como el sistema operativo sobre el que se va a implementar, los elementos de conectividad con otras aplicaciones, funcionalidades de red y si utiliza algún tipo de servicio web.

Todos nuestros proveedores IT cuentan con el correspondiente contrato de prestación de servicio (SLA), en el cual se detallan todas las obligaciones pertinentes y que afectan ente otras cuestiones a los requisitos de seguridad e integridad de la información.

Responsable: Responsable de Seguridad de la Información

6. Formatos y anexos

Descripción	Tiempo de archivo de los registros que genera	Responsable
RSI.1101 Política de desarrollo.	Según proceda	Resp. del Sistema
RSI.1102 Pruebas de aceptación de sistemas	Según proceda	Resp. del Sistema

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