sia icasys

An Indra company

Gestión de Vulnerabilidades

LogICA/Mónica

abril 2026

Tabla de contenido

1 Control de Versiones

Versión	Responsable		Fecha	Modificación
1.0	Autor:	Producto	06/04/26	
	Revisor:	Dirección de producto	06/04/26	

2 Introducción

2.1 Objetivo

Descripción del procedimiento utilizado para gestionar e intentar llevar a su corrección las vulnerabilidades identificadas en los productos software LogICA/Monica.

2.2 Alcance del Proceso

El alcance definido para el presente proceso engloba la totalidad de los desarrollos realizados por el área de producto ICASYS.

3 Roles y Responsabilidades

Los roles y responsabilidades en la realización del procedimiento son:

- **Clientes finales**: Son las organizaciones, áreas, divisiones o grupos, internos o externos, que utilizan o pueden llegar a utilizar los productos. Identifican las necesidades de alto nivel que ellos tienen respecto a dichos productos. Detectan incidencias que se puedan producir en el funcionamiento de los productos que utilizan.
- **Grupo de Soporte:** Equipo encargado de dar soporte de primer nivel a los productos y soluciones implantadas en los clientes finales y de gestionar la resolución de las incidencias que se identifican. Se encargan de registrar y gestionar las incidencias identificadas en los productos software.
- **Responsable del producto:** Encargado de supervisar, asesorar y aceptar el correcto mantenimiento y evolución del o de los productos software de los cuales es responsable.

4 Canal de notificación

Todas las partes interesadas disponen de canales de comunicación de incidencias relacionadas con los productos.

Los clientes con licencia vigente y servicios de soporte y mantenimiento activo disponen de los canales oficiales de comunicación:

- Correo electrónico.
- Teléfono.
- Portal de gestión de incidencias.

5 Procedimiento de Gestión de Vulnerabilidades

En el presente documento se describe el procedimiento y las actividades llevadas a cabo, así como los recursos utilizados, para gestionar e intentar mitigar las vulnerabilidades identificadas que afecten o puedan afectar a los productos software.

5.1 Versiones soportadas

El procedimiento de gestión de vulnerabilidades y los servicios de corrección correspondientes se facilitan únicamente para la versión actual del producto y las anteriores que estuvieran soportadas explícitamente y siempre que el producto se encuentre desplegado en plataformas y sistemas operativos soportados expresamente y esté correctamente configurado según las instrucciones definidas para tal fin.

5.2 Procedimiento de Gestión de Vulnerabilidades

En el procedimiento que se lleva a cabo para la gestión de vulnerabilidades se realizan actividades orientadas a la mitigación de las vulnerabilidades que se identifican en el producto implementado y que se concretan en los siguientes pasos generales:

- Monitorización y control para la identificación de vulnerabilidades,
- Registro y análisis inicial de impacto,
- Clasificación de la vulnerabilidad,
- Informe de análisis de impacto,
- Desarrollo de la corrección,
- Liberación de la corrección,
- Cierre de la incidencia.

5.2.1 Monitorización y control para la identificación de vulnerabilidades

Las vulnerabilidades que afecten a la seguridad del producto software pueden ser incidencias del propio software o defectos identificados en otros componentes que interactúen o que formen parte del entorno operacional de dicho producto software, como puede ser el sistema operativo, el *kernel* de la máquina o cualquier otro elemento con el que el producto funcione.

Las vulnerabilidades pueden ser identificadas por los clientes finales, por el personal de los departamentos involucrados en el proceso de desarrollo y mantenimiento del producto o por terceras entidades que conozcan o utilicen el producto o alguno de los componentes que interactúen o que formen parte del entorno operacional del producto.

Su detección puede producirse al llevar a cabo cualquiera de las fases del ciclo de vida del desarrollo, durante el uso normal del producto o, de forma proactiva, obteniendo información de vulnerabilidades o defectos identificados por terceros.

De esta forma, las fuentes de identificación de vulnerabilidades son:

- **Clientes finales**: Los clientes finales como utilizadores del producto podrán identificar errores relacionados con dicho producto, tanto funcionales, de seguridad, documentales, etc.
- **Personal de ICASYS durante el ciclo de vida del producto:** El propio personal de ICASYS involucrado en los procesos del ciclo de vida del software, tanto en el desarrollo, como en la implantación, así como en el mantenimiento y el soporte del producto, podrá identificar defectos de diferente tipo relacionados con el producto.
- **Terceras entidades:** Otras entidades que conozcan o utilicen el producto o alguno de los componentes que interactúen o que formen parte del entorno operacional del mismo podrán identificar errores relacionados con dicho producto o con su entorno operacional, tanto funcionales, de seguridad, documentales, etc.
- **Notificaciones automáticas de vulnerabilidades:** Mecanismos de notificación que informan periódicamente de los problemas, fundamentalmente vulnerabilidades de seguridad, que se van identificando en los diferentes componentes que interactúan o forman parte del entorno operacional del producto.

- **Búsquedas periódicas de vulnerabilidades:** Periódicamente se realiza una búsqueda de vulnerabilidades u otros defectos que pudieran afectar a los diferentes componentes que interactúan o forman parte del entorno operacional del producto.
- **Actualizaciones y pruebas periódicas de componentes:** Periódicamente, en el entorno de pruebas se actualizan los componentes que interactúan o forman parte del entorno operacional del producto, analizándose las correcciones que incorporan y permitiendo validar el comportamiento del producto con los componentes actualizados que teóricamente contendrán menos defectos, agilizando de esta forma su puesta en producción.

La comunicación de las posibles vulnerabilidades la llevará a cabo los clientes finales, las terceras entidades o el personal de ICASYS involucrado en los procesos del ciclo de vida del software a través de la herramienta de gestión de incidencias o contactando con el grupo de Soporte de ICASYS a través de correo electrónico o vía telefónica, será el personal de Soporte de ICASYS el encargado de registrar la incidencia en la herramienta de gestión cuando la comunicación no se haya producido a través de la propia herramienta.

5.2.2 Registro y análisis inicial de impacto

Cuando se detecta o se recibe información sobre una posible vulnerabilidad que afecta al producto implementado, ésta se registra, con objeto de gestionarla, realizar su seguimiento y con fines de auditoría.

El registro de las vulnerabilidades lo supervisa y valida el **Responsable del producto** y se realiza en la herramienta de gestión de incidencias. Se registra como **Incidente de seguridad**, con la subcategoría **Otros**, asociándolo al **Elemento de Configuración** de tipo **Software** correspondiente, para gestionar su mitigación y mantener registro de las versiones del producto en las que se ha identificado, así como de la versión del producto en la que la mitigación es implementada.

Una vez registrada, el **Responsable del producto** encarga, supervisa y valida la realización de un análisis del impacto de la vulnerabilidad, para determinar si la vulnerabilidad potencial notificada realmente es aplicable, verificando si el mal funcionamiento notificado, relacionado con la funcionalidad de seguridad del producto, viola la política de seguridad implícita o explícita de ese producto.

Este análisis inicial de impacto de la vulnerabilidad permite determinar si la vulnerabilidad afecta al producto y en qué medida lo hace, si es necesario implementar medidas mitigadoras en el producto o en su entorno o si no tiene un impacto relevante en el producto.

El análisis permite identificar y descartar aquellas vulnerabilidades potenciales que no son tales, que no suponen ningún problema de seguridad, que no son explotables en el producto o que ya han sido previamente gestionadas, por lo que no requieren que se realice ningún tratamiento adicional para ser mitigadas.

El **Incidente** en el que se encuentra registrada la información de la vulnerabilidad potencial se actualiza con toda la información adicional relevante, para poder consultarla en caso de que sea necesario. El **Responsable del producto** es el encargado de verificar la validez y completitud de la información recogida.

Entre otros datos, se recogen:

- **Asunto**: descripción resumida del incidente.
- **Descripción**: Resumen de la información recibida respecto a la vulnerabilidad.
- **Reportado por:** Fuente de la información.
- **Categorización**: Identificando el servicio de “incidentes de seguridad” y la categoría de “otros”.
- **Clasificación inicial de**: Impacto y Urgencia.
- **Impacto en seguridad**: Para la confidencialidad, integridad y disponibilidad.

- **Elemento de configuración**: La versión o versiones en las que se ha detectado la potencial vulnerabilidad.

5.2.3 Clasificación de la vulnerabilidad

Si el análisis del impacto de la vulnerabilidad realizado confirma la existencia y la relevancia de ésta y se determina que puede ser explotada en el producto, se aborda su mitigación o corrección, elaborando un informe del correspondiente análisis de impacto de la vulnerabilidad y estableciendo un plan de acciones correctivas.

Con la información del análisis de impacto disponible, el **Responsable del producto** clasifica la vulnerabilidad, según su impacto (1-2-3) y urgencia (Baja-Media-Alta-Critica).

La clasificación asignada a la vulnerabilidad determinará la prioridad o urgencia (Baja-Media-Alta-Critica) con la que se abordará la elaboración del correspondiente informe de análisis del impacto de la vulnerabilidad, así como su mitigación o corrección.

En el caso en el que, tras el análisis de impacto de la vulnerabilidad potencial, se descarte la mitigación o corrección de la misma pasa a un estado final.

5.2.4 Informe de análisis de impacto

En caso de que se confirme que la vulnerabilidad es explotable y afecta a la seguridad del producto, el **Responsable del producto** gestiona y supervisa la elaboración de un informe de análisis de impacto de la vulnerabilidad.

En dicho informe se tendrá en cuenta, de manera especial, el hecho de que el producto en el que se identifica la vulnerabilidad disponga de certificación de seguridad. En este caso, se tiene que considerar la posibilidad de que la certificación del producto se vea afectada y que haya que abordar acciones correctivas especiales orientadas al mantenimiento o recuperación de dicha certificación.

El informe de análisis de impacto de la vulnerabilidad contendrá, al menos, la siguiente información:

- Detalles de la vulnerabilidad: Incluyendo, por ejemplo, una descripción técnica, las condiciones de explotación, el impacto sobre el producto, la capacidad de que sea explotada, etc.
- Análisis de la causa raíz: Incluyendo el análisis técnico de la causa de la vulnerabilidad, la relación de productos y versiones afectadas, el impacto técnico, etc.
- Plan de acciones correctivas: Incluyendo las medidas de mitigación de la vulnerabilidad que se pudieran tomar, las medidas correctivas previstas, las fechas estimadas de disponibilidad de la mitigación y/o de la solución definitiva, el método de distribución de la solución, la posible validación o reevaluación del producto certificado, etc.
- Cronograma de aplicación del parche o actualización: Incluyendo la planificación de las actividades a llevar a cabo para paliar, mitigar y/o dar solución definitiva a la vulnerabilidad.
- Definición de la comunicación a los stakeholders: Incluyendo los mecanismos y medios previstos para la comunicación de la vulnerabilidad a las diferentes partes involucradas que pudieran verse afectadas por la vulnerabilidad.

El informe de análisis del impacto de la vulnerabilidad y la documentación asociada pertinente se almacenan en el repositorio de gestión de requisitos, relacionándolos con el incidente de la herramienta de gestión de incidentes, en el que se registra la información principal de la vulnerabilidad. El caso en el que se documente el detalle para la explotación de la vulnerabilidad, será considerado información sensible de difusión limitada.

Si el producto en el que se identifica la vulnerabilidad dispone de alguna certificación de seguridad y ésta se ve afectada, se llevarán a cabo las acciones correctivas especiales necesarias orientadas al mantenimiento o recuperación de dicha certificación. Esto podría requerir, por ejemplo:

- Informar sin demora de la vulnerabilidad al organismo certificador correspondiente.
- Facilitar al organismo certificador toda o parte de la información recopilada en el informe de análisis de impacto de la vulnerabilidad.
- Consensuar con el organismo certificador el plan de acciones correctivas a llevar a cabo.
- Permitir el organismo certificador que realice el seguimiento y verificación del cumplimiento del plan de acciones correctivas.
- Llevar a cabo las tareas de evaluación y certificación necesarias para conseguir mantener o recuperar la certificación del producto.

5.2.5 Desarrollo de la corrección

El **Responsable del producto** se encarga de planificar y gestionar la realización del plan de acciones correctivas propuesto, para asumir el riesgo, paliar, mitigar y/o resolver la vulnerabilidad identificada en el producto.

Se abordan las acciones correctivas planificadas sobre el producto y/o sobre los elementos del entorno que provocan la vulnerabilidad, para asumir el riesgo, paliar, mitigar y/o resolver dicha vulnerabilidad.

La urgencia con la que se llevan a cabo estas acciones correctivas planificadas dependerá, tanto de la clasificación y priorización de la vulnerabilidad, como de la solución que se haya decidido dar a la misma, asumiendo el riesgo, paliándola, mitigándola o corrigiéndola.

5.2.6 Liberación de la corrección

La comunicación de la vulnerabilidad y de la mitigación y/o corrección de la misma a los stakeholders o partes involucradas se realiza siguiendo los mecanismos y medios que se hubieran previsto para dicha comunicación.

Igualmente, siguiendo el método de distribución de la solución que se hubiera establecido en el plan de acciones correctivas, la mitigación y/o corrección aplicada al producto y/o a los elementos del entorno se libera para que, si aplica, los clientes finales actualicen sus entornos adecuadamente.

En el caso de que el producto disponga de alguna certificación de seguridad que se haya visto comprometida, se abordan los mecanismos para la divulgación de la información de la vulnerabilidad que se hubieran establecido y acordado. Igualmente, se llevan a cabo las tareas de evaluación y certificación necesarias para conseguir mantener o recuperar la certificación del producto.

Si, durante la gestión de la vulnerabilidad, se identifica que ésta podría haberse evitado modificando de alguna forma el proceso de desarrollo, se tomarán las medidas oportunas para actualizar el ciclo de vida de la seguridad del producto de forma que se mitigue la reaparición de alguna otra vulnerabilidad del mismo tipo que pueda surgir.

5.2.7 Cierre de la incidencia

Una vez gestionada la vulnerabilidad, se marcará como estado “Resuelto” en la herramienta de gestión de incidentes, indicando el Código de solución:

- En el caso de que la vulnerabilidad se identifique como solucionada: ***“Falla corregida”*** indicando el resumen de la solución.
- En el caso de que la vulnerabilidad se identifique como rechazada: ***“Otro”*** indicando el motivo del rechazo.

En ambos casos la solución se recoge en el campo de su descripción, pudiendo indicarse como información complementaria:

- Corregido / Solucionado
- No se corregirá
- Inválido
- Duplicado
- No se puede reproducir
- Sin respuesta

Si se considera necesario, en el campo de bitácora y/o notas de la solución se puede incluir algunos comentarios adicionales y relacionados con la gestión de la vulnerabilidad.

6 Anexo I: Informe de análisis de impacto de vulnerabilidad

Tabla de ayuda para completar el informe de análisis de impacto de una vulnerabilidad detectada, Vulnerability Impact Analysis Report.

Sección	Punto / Campo	Valor (a rellenar)	Evidencia / Referencia
Información general	Producto	LogICA / Mónica	
	Responsable del producto		
	Grupo de soporte		
	Fecha de detección		
	Estado del incidente	Abierto / En mitigación / Cerrado	
Registro del incidente	Registro en ICASYS		
	Elemento de configuración		
	Versiones afectadas		
Identificación de la vulnerabilidad	Fuente de identificación	cliente, soporte, personal ICASYS, terceros, notificación automática, etc.	
	Descripción resumida		
Análisis inicial de impacto	Evaluación preliminar		
	Impacto preliminar (C/I/D)		
Análisis de impacto EUCC (VIA)	Referencia EUCC		
	Certificado EUCC		
	Nivel de garantía		
	TOE (Objeto de evaluación)		
	Impacto sobre funciones de seguridad		
Clasificación de la vulnerabilidad	Impacto	1 / 2 / 3	
	Urgencia	Baja / Media / Alta / Crítica	
	Prioridad resultante		
Informe técnico del impacto	Causa raíz		
	Condiciones de explotación (precondiciones, acceso, privilegios, etc.)		
Plan de acciones correctivas	Medidas de mitigación/corrección		
	Cronograma		

Sección	Punto / Campo	Valor (a rellenar)	Evidencia / Referencia
Comunicación	Comunicación a stakeholders		
	Notificación a organismo/autoridad		
Validación	Liberación de la corrección		
	Verificación/validación		
Cierre de la incidencia	Código de solución	Falla corregida / Otro	
	Resumen de la solución / motivo de rechazo		
Aprobaciones	Aprobación: Responsable del producto		
	Fecha de aprobación		

An Indra company

Producto de ciberseguridad

Av. Bruselas, 35, 28100, Alcobendas
(Madrid) - Spain
T +34 914 80 50 00