Gestión de Vulnerabilidades

Mónica / LogICA

Procedimiento operativo

indramind.com

IndraMind

Control de versiones

Versión	Responsable	Fecha	Descripción
1.0	Equipo Quality & Product Enablement	06/04/2026	Versión inicial

Índice

1 Introducción

1.1 Objetivo

El presente procedimiento tiene por objeto describir el proceso establecido para **gestionar, analizar y, cuando proceda, corregir o mitigar** las vulnerabilidades identificadas en los productos software **LogICA/MONICA**.

1.2 Alcance del Proceso

El alcance del presente proceso comprende **la totalidad de los desarrollos realizados por el área de producto ICASYS**, incluyendo las actividades necesarias para la identificación, análisis, seguimiento, mitigación y cierre de vulnerabilidades que puedan afectar a dichos productos.

2 Roles y Responsabilidades

Los roles y responsabilidades asociados a la ejecución del procedimiento son los siguientes:

- **Clientes finales**: organizaciones, áreas, divisiones o grupos, internos o externos, que utilizan o pueden llegar a utilizar los productos. Identifican necesidades de alto nivel y comunican las incidencias o vulnerabilidades que puedan detectarse durante el uso de los productos.
- **Grupo de Soporte**: equipo responsable de prestar soporte de primer nivel a los productos y soluciones implantadas, así como de **registrar, canalizar y realizar el seguimiento** de las incidencias identificadas.
- **Responsable del producto**: persona encargada de **supervisar, validar y aceptar** las actividades relacionadas con el mantenimiento, evolución, análisis de impacto, mitigación y cierre de vulnerabilidades del producto software bajo su responsabilidad.

3 Canal de notificación

Todas las partes interesadas disponen de **canales definidos de comunicación** para notificar incidencias o posibles vulnerabilidades relacionadas con los productos.

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

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

4 Procedimiento de Gestión de Vulnerabilidades

En el presente documento se describe el procedimiento, las actividades y los recursos utilizados para **gestionar, mitigar o corregir** las vulnerabilidades identificadas que afecten o puedan afectar a los productos software.

4.1 Versiones soportadas

El procedimiento de gestión de vulnerabilidades y los servicios de corrección asociados se facilitan únicamente para **la versión actual del producto** y para aquellas versiones anteriores que se encuentren **explícitamente soportadas**. Asimismo, será necesario que el producto esté desplegado sobre

plataformas y sistemas operativos soportados y que se encuentre configurado conforme a las instrucciones definidas.

4.2 Procedimiento de Gestión de Vulnerabilidades

El procedimiento de gestión de vulnerabilidades contempla un conjunto de actividades orientadas a la **identificación, evaluación, priorización, mitigación, liberación y cierre** de las vulnerabilidades detectadas en el producto implementado. De forma general, el proceso se articula en las siguientes fases:

- **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**.

4.2.1 Monitorización y control para la identificación de vulnerabilidades

Las vulnerabilidades que afecten a la seguridad del producto software pueden tener su origen en incidencias del propio software o en defectos identificados en componentes que interactúen con él o formen parte de su entorno operacional, tales como el sistema operativo, el *kernel* de la máquina u otros elementos necesarios para su funcionamiento.

Las vulnerabilidades podrán ser identificadas por **clientes finales**, por personal de los departamentos involucrados en el ciclo de vida del producto o por **terceras entidades** que conozcan, utilicen o analicen el producto o alguno de los componentes de su entorno operacional.

La detección puede producirse durante cualquiera de las fases del ciclo de vida del desarrollo, durante el uso ordinario del producto o de forma proactiva, mediante la consulta de información publicada por terceros sobre vulnerabilidades o defectos conocidos.

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

- **Clientes finales**: los clientes finales, como usuarios del producto, podrán identificar defectos relacionados con el mismo, ya sean **funcionales, de seguridad o documentales**.
- **Personal de ICASYS durante el ciclo de vida del producto**: el personal de ICASYS involucrado en los procesos de **desarrollo, implantación, mantenimiento y soporte** podrá identificar defectos de diferente naturaleza relacionados con el producto.
- **Terceras entidades**: otras entidades que conozcan, utilicen o analicen el producto, o alguno de los componentes de su entorno operacional, podrán identificar defectos **funcionales, de seguridad o documentales**.
- **Notificaciones automáticas de vulnerabilidades**: mecanismos de notificación que informan periódicamente sobre problemas o **vulnerabilidades de seguridad** identificadas en los componentes que interactúan con el producto o forman parte de su entorno operacional.
- **Búsquedas periódicas de vulnerabilidades**: de forma periódica se realizan búsquedas orientadas a identificar vulnerabilidades u otros defectos que puedan afectar a los componentes que interactúan con el producto o forman parte de su entorno operacional.
- **Actualizaciones y pruebas periódicas de componentes**: en el entorno de pruebas se actualizan periódicamente los componentes del entorno operacional, analizando las correcciones incorporadas y validando el comportamiento del producto antes de su eventual puesta en producción.

La comunicación de posibles vulnerabilidades será realizada por los clientes finales, terceras entidades o personal de ICASYS involucrado en el ciclo de vida del software mediante la herramienta de gestión de incidencias o contactando con el **Grupo de Soporte de Minsait ICASYS** por correo electrónico o vía telefónica. Cuando la comunicación no se haya producido a través de la herramienta, será el personal de Soporte de ICASYS quien registre la incidencia correspondiente.

4.2.2 Registro y análisis inicial de impacto

Cuando se detecte o se reciba información sobre una posible vulnerabilidad que afecte al producto implementado, dicha vulnerabilidad deberá registrarse con el fin de **garantizar su gestión, seguimiento y trazabilidad** a efectos operativos y de auditoría.

El registro de las vulnerabilidades será supervisado y validado por el **Responsable del producto** y se realizará en la herramienta de gestión de incidencias. La vulnerabilidad se registrará como **Incidente de seguridad**, con la subcategoría **Otros**, asociándola al **Elemento de Configuración** de tipo **Software** correspondiente, con el fin de gestionar su mitigación y mantener la trazabilidad de las versiones afectadas y de la versión en la que se implemente la mitigación.

Una vez registrada la vulnerabilidad, el **Responsable del producto** encargará, supervisará y validará la realización de un **análisis inicial de impacto**, con el objetivo de determinar si la vulnerabilidad potencial notificada resulta aplicable al producto y si el comportamiento identificado vulnera la política de seguridad implícita o explícita del mismo.

Este análisis inicial permite determinar si la vulnerabilidad afecta al producto, en qué medida lo hace y si resulta necesario aplicar **medidas mitigadoras o correctivas** sobre el producto o sobre su entorno operacional.

El análisis también permite identificar y descartar vulnerabilidades potenciales que no constituyan un problema real de seguridad, que no sean explotables en el producto o que ya hayan sido gestionadas previamente, en cuyo caso no será necesario aplicar tratamiento adicional.

El **Incidente** en el que se registre la información de la vulnerabilidad potencial deberá actualizarse con toda la información adicional relevante. El **Responsable del producto** verificará la validez, completitud y coherencia de la información incorporada.

Entre otros datos, se recogen:

- **Asunto**: descripción resumida del incidente.
- **Descripción**: resumen de la información recibida relativa a la vulnerabilidad.
- **Reportado por**: fuente que comunica o identifica la información.
- **Categorización**: identificación del servicio **Incidentes de seguridad** y de la categoría **Otros**.
- **Clasificación inicial**: valoración preliminar de **impacto** y **urgencia**.
- **Impacto en seguridad**: valoración preliminar sobre **confidencialidad, integridad y disponibilidad**.
- **Elemento de configuración**: versión o versiones en las que se ha detectado la potencial vulnerabilidad.

4.2.3 Clasificación de la vulnerabilidad

Si el análisis de impacto confirma la existencia, aplicabilidad y relevancia de la vulnerabilidad, y se determina que puede ser explotada en el producto, se iniciará su **mitigación o corrección**, elaborando el correspondiente informe de análisis de impacto y definiendo un plan de acciones correctivas.

Con la información del análisis de impacto disponible, el **Responsable del producto** clasificará la vulnerabilidad atendiendo a su **impacto** (1, 2 o 3) y a su **urgencia** (Baja, Media, Alta o Crítica).

La clasificación asignada determinará la prioridad con la que se abordará la elaboración del informe de análisis de impacto, así como la planificación y ejecución de las acciones de mitigación o corrección.

Cuando, tras el análisis inicial, se descarte la necesidad de mitigación o corrección, el incidente pasará a un **estado final**, dejando constancia del motivo correspondiente.

4.2.4 Informe de análisis de impacto

Cuando se confirme que la vulnerabilidad es explotable y afecta a la seguridad del producto, el **Responsable del producto** gestionará y supervisará la elaboración de un **informe de análisis de impacto de la vulnerabilidad**.

En dicho informe deberá considerarse de forma específica si el producto afectado dispone de **certificación de seguridad**. En tal caso, se evaluará si la certificación puede verse afectada y si resulta necesario ejecutar acciones correctivas especiales orientadas a su mantenimiento o recuperación.

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

- **Detalles de la vulnerabilidad**: descripción técnica, condiciones de explotación, impacto sobre el producto y capacidad de explotación, entre otros aspectos relevantes.
- **Análisis de la causa raíz**: análisis técnico de la causa de la vulnerabilidad, relación de productos y versiones afectadas e impacto técnico asociado.
- **Plan de acciones correctivas**: medidas de mitigación o corrección previstas, fechas estimadas de disponibilidad, método de distribución y, cuando proceda, validación o reevaluación del producto certificado.
- **Cronograma de aplicación del parche o actualización**: planificación de las actividades necesarias para paliar, mitigar o resolver definitivamente la vulnerabilidad.
- **Comunicación a los stakeholders**: mecanismos y medios previstos para comunicar la vulnerabilidad a las partes involucradas que pudieran verse afectadas.

El informe de análisis de impacto y la documentación asociada se almacenarán en el repositorio de gestión de requisitos, quedando relacionados con el incidente registrado en la herramienta de gestión de incidencias. Cuando se documente información relativa a la explotación de la vulnerabilidad, dicha información se considerará **sensible y de difusión limitada**.

Si el producto afectado dispone de una certificación de seguridad y ésta pudiera verse comprometida, se ejecutarán las **acciones correctivas especiales** necesarias para mantener o recuperar dicha certificación. Estas acciones podrán incluir, entre otras:

- **Informar sin demora** de la vulnerabilidad al organismo certificador correspondiente.
- **Facilitar al organismo certificador** la información necesaria del informe de análisis de impacto de la vulnerabilidad.
- **Consensuar con el organismo certificador** el plan de acciones correctivas que deba ejecutarse.
- **Permitir el seguimiento y verificación** por parte del organismo certificador del cumplimiento del plan de acciones correctivas.
- **Ejecutar las tareas de evaluación y certificación** necesarias para mantener o recuperar la certificación del producto.

4.2.5 Desarrollo de la corrección

El **Responsable del producto** será el encargado de planificar y gestionar la ejecución del **plan de acciones correctivas**, orientado a asumir, paliar, mitigar o resolver la vulnerabilidad identificada.

Las acciones correctivas se aplicarán sobre el producto y/o sobre los elementos del entorno que originen o condicionen la vulnerabilidad, con el objetivo de reducir el riesgo asociado o proporcionar una solución definitiva.

La urgencia de ejecución dependerá de la **clasificación y priorización de la vulnerabilidad**, así como de la estrategia adoptada: aceptación del riesgo, mitigación temporal, corrección parcial o solución definitiva.

4.2.6 Liberación de la corrección

La comunicación de la vulnerabilidad y de su mitigación o corrección a los stakeholders o partes involucradas se realizará conforme a los **mecanismos y medios definidos** en el plan de comunicación correspondiente.

Asimismo, siguiendo el método de distribución establecido en el plan de acciones correctivas, la mitigación o corrección aplicada al producto y/o a los elementos del entorno será liberada para que, cuando proceda, los clientes finales actualicen sus entornos de forma adecuada.

Cuando el producto disponga de una certificación de seguridad que pudiera haberse visto comprometida, se aplicarán los mecanismos de divulgación acordados y se realizarán las tareas de evaluación y certificación necesarias para mantener o recuperar dicha certificación.

Si durante la gestión de la vulnerabilidad se identifica que ésta podría haberse evitado mediante cambios en el proceso de desarrollo, se adoptarán las medidas oportunas para actualizar el ciclo de vida de seguridad del producto y reducir la probabilidad de reaparición de vulnerabilidades similares.

4.2.7 Cierre de la incidencia

Una vez gestionada la vulnerabilidad, el incidente se marcará con estado **"Resuelto"** en la herramienta de gestión de incidencias, indicando el código de solución correspondiente:

- Cuando la vulnerabilidad se identifique como solucionada, se utilizará el código ***"Fallo corregido"***, indicando el resumen de la solución aplicada.
- Cuando la vulnerabilidad se identifique como rechazada, se utilizará el código ***"Otro"***, indicando el motivo del rechazo.

En ambos casos, la solución deberá recogerse en el campo de descripción correspondiente, pudiendo incorporarse como información complementaria alguno de los siguientes estados:

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

Cuando se considere necesario, podrán incluirse comentarios adicionales en el campo de bitácora y/o notas de la solución, siempre que estén directamente relacionados con la gestión de la vulnerabilidad.

5 Anexo I: Informe de análisis de impacto de vulnerabilidad

El presente anexo proporciona una tabla de apoyo para cumplimentar el **informe de análisis de impacto de una vulnerabilidad** detectada, denominado *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		
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		

PROTECTING TO EMPOWER

Avda. de Bruselas, 35
28108 Alcobendas
Madrid, Spain
T +34 91 480 50 00

indramind.com

IndraMind