



POLICIA FEDERAL ARGENTINA

Procedimiento de exclusiones

**Superintendencia FEDERAL DE TECNOLOGÍAS DE
LA INFORMACIÓN Y COMUNICACIONES**



Procedimiento de Exclusiones

EDICIÓN 1
Tipo de Documento: IMPLEMENTACIÓN
Versión: 2.0 / 2025
Página 2 de 5

Tabla de contenido

INTRODUCCIÓN.....	3
ROLES Y RESPONSABILIDADES	3
SOLICITANTE	3
EQUIPO DE SEGURIDAD (SOC)	3
IMPLEMENTACIÓN.....	4
FORMATO ESTANDARIZADO PARA SOLICITUDES Y RESPUESTAS.....	4
SOLICITUD OFICIAL	4
RESPUESTA DEL SOC.....	5
DOCUMENTACIÓN Y SEGUIMIENTO.....	5
REVISIONES Y MODIFICACIONES:.....	5



Procedimiento de Exclusiones

EDICIÓN 1

Tipo de Documento:
IMPLEMENTACIÓN

Versión: 2.0 / 2025

Página 3 de 5

Introducción

Este procedimiento establece los pasos para gestionar solicitudes de exclusión o excepción en herramientas de seguridad como FortiEDR, FortiClient EMS y ESET, asegurando que estas solicitudes se manejen de manera que minimicen los riesgos y mantengan la integridad y la seguridad de los sistemas de la Institución.

Los canales formales de solicitud son mediante la generación de Expediente Electrónico y/o la utilización del Correo Institucional.

Roles y Responsabilidades

Solicitante

- Presentar una solicitud de exclusión justificando la necesidad con la siguiente información:
 - Nombre y cargo del solicitante.
 - Dependencia.
 - Proceso, archivo, IP o URL a excluir.
 - Justificación técnica detallada.
 - Duración estimada de la exclusión (si corresponde).
 - Debe dejar explícitamente que entiende y acepta los riesgos.

Aclaración: las solicitudes incompletas no serán procesadas.

Equipo de Seguridad (SOC)

- Deberá analizar, documentar y emitir una conclusión luego de haber realizado las siguientes acciones:
 - Recepción de la solicitud.
 - Creación de ticket.
 - Evaluación de la solicitud y el riesgo de impacto en la seguridad.
 - Documentar todos los hallazgos realizados en la evaluación técnica.



Procedimiento de Exclusiones

EDICIÓN 1

Tipo de Documento:
IMPLEMENTACIÓN

Versión: 2.0 / 2025

Página 4 de 5

Implementación

- Si el resultado del análisis fuera satisfactorio, el SOC realizará las siguientes acciones:
 - Implementación de la exclusión.
 - Notificar al solicitante
- Si el resultado fuese insatisfactorio debido a los riesgos que podría conllevar dentro de la Institución, las acciones a realizar son las siguientes:
 - Notificar al solicitante.
 - Impacto potencial en la confidencialidad, integridad o disponibilidad de la información o los sistemas.
 - Posibles consecuencias negativas para los procesos críticos de la Dependencia o Institución.
 - Riesgos asociados a la afectación de normativas de cumplimiento o políticas internas.

Formato estandarizado para Solicitudes y Respuestas

Solicitud Oficial

Asunto: Solicitud de exclusión

Por la presente solicito la exclusión del [Proceso / archivo / IP / URL]. La solicitud se fundamenta en [justificación].

- Nombre y cargo del solicitante:
- Dependencia:
- Proceso:
- Archivo:
- IP:
- URL:
- Duración estimada de la exclusión (si corresponde):

Entiendo que la solicitud pueda generar riesgos asociados a la pérdida, filtración o corrupción de la información, daño, perjuicio y desprestigio en contra de la Dependencia y/o Institución. Además, acepto que es mi responsabilidad colaborar con el equipo de seguridad proporcionando toda la información adicional necesaria para mitigar los riesgos identificados y cumplir con las medidas correctivas recomendadas.

Adjunto la información requerida para evaluación.



Procedimiento de Exclusiones

EDICIÓN 1
Tipo de Documento: IMPLEMENTACIÓN
Versión: 2.0 / 2025
Página 5 de 5

Respuesta del SOC

Asunto: RE: Solicitud de exclusión

En respuesta a su solicitud, el equipo del Centro de Operaciones de Seguridad informa que [aprobamos/requerimos ajustes/denegamos] la exclusión solicitada.

Adjunto el informe técnico con detalles.

Documentación y seguimiento

En el marco de este procedimiento, la documentación y el seguimiento desempeñan un papel crítico para garantizar la efectividad y la transparencia en la gestión de las exclusiones implementadas. Cada solicitud aprobada debe ser registrada adecuadamente en nuestro sistema de gestión de tickets. Este registro no solo sirve como evidencia para auditorías, sino que también permite un monitoreo continuo del impacto que estas exclusiones puedan tener en los sistemas de seguridad de la institución.

Además, el seguimiento es esencial para evaluar si las condiciones bajo las cuales se aprobó la exclusión siguen siendo válidas. Por ello, se debe realizar revisiones periódicas, según la criticidad de la exclusión. Este análisis permitirá identificar si la exclusión sigue siendo necesaria o si debe ser ajustada o eliminada.

Por último, es fundamental que todo el proceso esté alineado con las mejores prácticas de seguridad. Esto no solo protegerá los activos críticos de la institución, sino que también fortalecerá nuestra posición frente a posibles auditorías y revisiones externas.

Recordemos que la documentación adecuada no solo respalda nuestras decisiones, sino que también nos permite mantener un entorno seguro y eficiente, promoviendo la confianza y la responsabilidad en nuestras operaciones.

Revisiones y Modificaciones:

➤ 14/01/25