# ATENCIÓN A INCIDENTES DE SEGURIDAD INFORMÁTICA

# CONTROL DE EMISIÓN

| Elaboró | Revisó | Aprobó |
|---|---|---|
| I.S.C. Mario Valdez Velázquez | Mtra. Gabriela Gutiérrez García | Dr. Juan Humberto Sossa Azuela |
| Firma: | Firma: | Firma: |

# CONTROL DE CAMBIOS

| Número de versión | Fecha de actualización | Descripción del cambio |
|---|---|---|
| 01 | 23-Jul-25 | Elaboración de primera vez |

## I. PROPÓSITO DEL PROCEDIMIENTO

Gestionar los incidentes de seguridad informática, clasificándolos como internos o externos dependiendo el origen de estos.

## II. ALCANCE

La seguridad informática del Instituto Politécnico Nacional en términos técnicos es dirigida por la Dirección de Cómputo y Comunicaciones a través del Departamento de seguridad informática, administrando de forma centralizada la seguridad perimetral del Instituto y el endpoint antimalware. Por lo anterior, en el Centro de Investigación en Computación se atenderán los incidentes de seguridad informática locales excluyendo aquellos que el Departamento de Seguridad Informática y el Grupo Estratégico de Seguridad de la Información (GESI) del Instituto han solicitado les sean turnados.

## III. DOCUMENTOS DE REFERENCIA Y NORMAS DE OPERACIÓN

Manual de Organización del Centro de Investigación en Computación. - 4 de julio de 2025.

Norma ISO 9001:2015 - Sistema de Gestión de la Calidad- Requisitos NMX-CC-9001-IMNC-2015.

Norma ISO 9000:2015 - Fundamentos y vocabulario NMX-CC-9000-IMNC-2008.

Norma ISO/IEC 27001:2022 – Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de la Seguridad de la Información.

ISO/IEC 27002:2022 Seguridad de la Información, Ciberseguridad y Protección de la Privacidad – Controles de Seguridad de la Información.

ISO/IEC 27005:2022 Tecnología de la Información – Técnicas de Seguridad – Gestión del riesgo en la Seguridad de la Información.

DOF: 06/09/2021. ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.

Objetivos alineados a la Política General de SI. https://www.ipn.mx/assets/files/cenac/docs/normatividad/objetivos-alineados.pdf

POLÍTICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN. (29/10/2021). https://www.ipn.mx/assets/files/cenac/docs/normatividad/politica-seguridad.pdf

## IV. POLÍTICAS DE OPERACIÓN

1. Todo incidente de seguridad de la información deberá ser registrado y canalizado.
2. Siempre se asignará un especialista en el tema y podrá solicitar una escalación más antes de turnarlo al Departamento de Seguridad Informática.
3. La prioridad de la información del Centro de Investigación en Computación estará sobre las solicitudes que realice el Departamento de Seguridad Informática.
4. Semestralmente se entregará un informe mediante Tarjeta Informativa.
5. El Subdirector de Desarrollo Tecnológico será el especialista en Seguridad Informática.

| ACTIVIDAD | RESPONSABLE | REGISTROS |
|---|---|---|
| 1. Recibe el reporte de un posible incidente de seguridad informática a través de los canales establecidos (correo electrónico, Mesa de Servicios, sistema de tickets, etc.). | SDT | |
| 2. Realiza un análisis preliminar para identificar la naturaleza del evento, su alcance y posibles implicaciones en la infraestructura tecnológica. | SDT | |
| 3. Se determina si el evento corresponde a un incidente de seguridad informática. Si: 4 , No: 6 | SDT | |
| 4. Se analiza si el incidente debe ser escalado al Departamento de Seguridad Informática (DSI) por su complejidad o criticidad. Si: 5 , No: 6 | SDT | |
| 5. Turna al Departamento de Seguridad Informática mediante la Mesa de Servicios del Centro Nacional de Cálculo, incluyendo toda la información recopilada hasta el momento. | DSTO | |
| 6. Realiza las primeras acciones técnicas para contener o mitigar el impacto del incidente, como aislamiento de sistemas, bloqueo de accesos, restauración de servicios, entre otros. | SDT | |
| 7. Determina si el impacto del incidente amerita un nuevo escalamiento al Departamento de Seguridad Informática. Si: 5 , No: 8 | SDT | |
| 8. Identifica si el servicio afectado corresponde a un componente tecnológico administrado por la Subdirección de Desarrollo Tecnológico. Si: 10 , No: 9 | SDT | |
| 9. Turna a la Subdirección correspondiente o a la Coordinación de Enlace y Gestión Técnica para su atención. | SDT | |
| 10. Asigna un especialista técnico del área correspondiente para atender el incidente. | SDT | |
| 11. Verifica si el especialista asignado logró resolver el incidente. Si: 14 , No: 12 | SDT | |
| 12. Escala a otro especialista con mayor experiencia o conocimiento específico del sistema afectado. | SDT | |

| ACTIVIDAD | RESPONSABLE | REGISTROS |
|---|---|---|
| 13. Verifica si el segundo especialista logró resolver el incidente.Si: 14 , No: 5 | SDT | |
| 14. Elabora un informe técnico que debe incluir entre otras cosas: Descripción del incidente, acciones realizadas, evidencias (capturas, registros, logs), recomendaciones. | | |
| 15. Envía informe por correo electrónico a la Subdirección de Desarrollo Tecnológico y, si aplica, a otras áreas involucradas. | | |
| **FIN DE PROCEDIMIENTO** | | |