ACUERDO GENERAL NÚMERO TREINTA

En la Ciudad de San Juan, Provincia del mismo nombre, República Argentina, a los catorce días del mes de abril de dos mil veinticinco, reunida la Señora Presidenta de la Corte de Justicia DRA. ADRIANA VERÓNICA GARCÍA NIETO y los Señores Ministros, DR. DANIEL OLIVARES YAPUR, DR. JUAN JOSÉ VICTORIA, DR. GUILLERMO DE SANCTIS y DR. MARCELO JORGE LIMA, con la asistencia del Señor Fiscal de Cámara, subrogante de Fiscalía General, DR. DANIEL GALVANI, DIJERON:----------

--- Que, mediante Expediente N° 155743 caratulado "DIRECCION DE INFORMÁTICA S/ Peticiona (ref. evaluación protocolo de respuesta ante incidentes de alto impacto)" el Sr. Subdirector de Informática, Sr. Raúl César Rodríguez, solicita la aprobación e implementación del "Protocolo de Respuesta ante Incidentes de Alto Impacto".----------

--- Que, el referido Protocolo se ha elaborado siguiendo las mejores prácticas, con el objetivo de establecer lineamientos claros para la detección, contención, erradicación, recuperación y reporte de incidentes de seguridad que puedan comprometer la operación y reputación del Poder Judicial de San Juan.----------

--- Que, el referido Protocolo establece roles, responsabilidades y procedimientos críticos para la gestión de incidentes que afectan la

confidencialidad, integridad y disponibilidad de la información, siendo coherente con las reglamentaciones establecidas por los Acuerdos Generales N° 126 del año 2022 y N° 22 del año 2023.----------

--- Que, consecuentemente, resulta procedente su aprobación, destacando que para su implementación y cumplimiento no son necesarios recursos adicionales para la Dirección de Informática.----------

--- Que, por todo ello, en uso de las facultades que le confiere el artículo 207 de la Constitución de la Provincia y la Ley Orgánica de Tribunales, Ley N° 2352-O, **ACORDARON**:----------

1.- Aprobar el Protocolo de Respuesta ante Incidentes de Alto Impacto que, en Anexo, integra el presente.----------

2.- Disponer la obligatoriedad del cumplimiento del "Protocolo de Respuesta ante Incidentes de Alto Impacto" por parte de la totalidad del personal del Poder Judicial, considerando cualquier conducta contraria u omisiva de las reglas allí establecidas como falta disciplinaria, pasible de sanción.----------

3.- Disponer se dé amplia difusión del mismo en todo el ámbito del Poder Judicial y se publique por un día en el Boletín Oficial de la provincia.----------

--- Dispuestas las comunicaciones del caso, termina el acuerdo, que se firma por ante mí.-

Dr. Daniel Gustavo Olivarda Yaqui
MINISTRO

Dr. Juan José E. Victoria
MINISTRO

Dr. Marcelo Jorge Lima
MINISTRO

Dra. Adriana Verónica García Nieto
PRESIDENTA

Dr. Guillermo Horacio De Sanctis
MINISTRO

Dr. DANIEL GALVANI
FISCAL GENERAL
SUBROGANTE

Dr. Javier Vera Frassinelli
SECRETARIO ADMINISTRATIVO
CORTE DE JUSTICIA

CORTE DE JUSTICIA
SAN JUAN

ANEXO ACUERDO GENERAL N° 30/2025

Protocolo de Respuesta ante Incidentes de Alto Impacto

Poder Judicial de San Juan

Tabla de contenidos

Objetivo

Establecer lineamientos claros, roles, responsabilidades, procedimientos y controles para detectar, contener, erradicar, recuperar y reportar incidentes de seguridad de alto impacto que puedan comprometer la operación y la reputación del Poder Judicial de San Juan, garantizando en todo momento la confidencialidad, integridad y disponibilidad de la información.

1. Alcance

Este protocolo aplica a todos los sistemas, infraestructura, datos, procesos y personal del Poder Judicial de San Juan involucrados en la gestión, almacenamiento y transmisión de información.

2. Definición de Incidente de Alto Impacto

Se considera incidente de alto impacto cualquier evento que afecte significativamente las dimensiones C-I-A (Confidencialidad, Integridad y Disponibilidad) de los sistemas y datos del Poder Judicial de San Juan. Ejemplos incluyen:

- Confidencialidad: Exfiltración de datos sensibles (información personal protegida, expedientes judiciales, información clasificada), accesos no autorizados o violaciones de privacidad.
- Integridad: Alteración no autorizada de registros judiciales, modificación maliciosa de software, manipulación de evidencias digitales.
- Disponibilidad: Ataques de denegación de servicio a sistemas críticos, fallas en la infraestructura tecnológica que impiden el acceso a servicios esenciales.

3. Referencia al Marco NIST

Este protocolo se basa en el Ciclo de Vida de Respuesta a Incidentes del NIST SP 800-61 Rev. 2, el cual incluye las siguientes fases:

1. Preparación
2. Detección y Análisis
3. Contención, Erradicación y Recuperación

4. Lecciones Aprendidas (Post-Incidente)

Durante cada fase, se considerará el impacto sobre la confidencialidad, integridad y disponibilidad (C-I-A).

4. Roles y Responsabilidades

- *Mesa de Ayuda:* actúa como el primer punto de contacto para la identificación y escalamiento de incidentes de seguridad. Su función principal es garantizar que cualquier actividad anómala o sospechosa sea registrada, categorizada y derivada al equipo responsable, asegurando una respuesta rápida y coordinada. Incluye tanto el Departamento de Soporte a Usuarios (Responsable: Virginia Caballero) como el Departamento de Seguridad Informática (Responsable: Marisú Pages).
- *Comité de Seguridad del Poder Judicial*: Coordina y lidera la respuesta. Notifica a las autoridades internas (Secretaría Administrativa, Corte de Justicia) y, si corresponde, a organismos reguladores o policiales.
- *Dirección de Informática*: Proporciona recursos técnicos, información sobre infraestructura, accesos y herramientas de monitoreo. Participa en la investigación y remediación técnica del incidente.
- *UFI Delitos Informáticos y Estafas*: Toma acción luego de identificado el incidente, investigando responsables y posibles acciones legales.
- *Dirección de Comunicación Institucional*: Gestiona la comunicación oficial al personal interno, magistrados, funcionarios y, si es necesario, a la ciudadanía, a través de voceros autorizados.
- *Oficial de Seguridad de la Información* (CISO): Valida y lidera las estrategias y acciones de remediación. Asegura el cumplimiento de las políticas de seguridad y propone mejoras tras el incidente.

5. Preparación (Antes del Incidente)

Es responsabilidad del Comité de Seguridad (*planeamiento*) y de la Dirección de Informática (*ejecución*):

- Políticas y Procedimientos: Mantener y revisar periódicamente políticas de seguridad, planes de continuidad del negocio y recuperación ante desastres.
- Capacitación: Asegurar la capacitación al personal sobre amenazas, uso seguro de sistemas y manejo de información sensible.

- Herramientas y Monitoreo: implementar, operar y mantener soluciones de IDS/IPS, antivirus, SIEM, sistemas de respaldo y otras soluciones para detectar y mitigar amenazas de acuerdo con la matriz de riesgos.
- Pruebas y Ejercicios: Realizar simulaciones de incidentes, ejercicios de respuesta y pruebas de restauración desde backups.

6. Detección y Análisis (Durante el Incidente)

1. En caso de tratarse de un posible Ransomware (imposibilidad de acceder a archivos, archivos con extensiones raras, mensaje que informa que los archivos han sido cifrados, fondo de pantalla que cambia con mensajes extraños, etc), antes de reportar el incidente el usuario debe hacer lo siguiente:
    a. Desconectar cable de red.
    b. Apagar el equipo hasta nuevo aviso.
    c. Si sus compañeros/compañeras tienen un problema similar deben proceder de la misma manera.
    d. Notificar el incidente a la Mesa de Ayuda.
2. Notificación del Incidente: El personal del Poder Judicial que detecte actividad sospechosa debe reportarla de inmediato a la Mesa de Ayuda al +54 264 432-4550 opción 4, de Lunes a Viernes de 7 a 20 hs. Fuera de ese horario, contactar a los teléfonos de escalamiento.
3. Mitigación inicial: Luego de la evaluación inicial y habiendo identificado la presencia de ransomware, el personal de la Mesa de Ayuda o quién haya recibido el reporte, deberá agotar la siguiente lista de contactos para acción inmediata:
    a. Personal de Infraestructura disponible en horario de normal de trabajo:
        i. Tadeo Derkacz, +54 9 264 521-1718
        ii. Fernando Almazán, +54 9 343 475-9718
    b. Marcelo Podestá, +54 (9 264) 457-6330
    c. Raúl Rodríguez, +54 (9 264) 626-7070
    d. Leandro Esteban Castro Aneas, +54 (9 264) 514-8977
4. Análisis inicial: el Área de Ciberseguridad evalúa el tipo de amenaza, alcance, impacto potencial sobre C-I-A.
5. Recolección de evidencias: Preservar registros (logs), capturas de tráfico, imágenes de sistemas comprometidos, manteniendo la cadena de custodia.
6. Comunicar al Comité de Seguridad todos los detalles de lo sucedido.

7. Contención, Erradicación y Recuperación Detección y Análisis (Durante el Incidente)

Son responsabilidades de la Dirección de Informática:

1. Contener: Aislar sistemas afectados para evitar propagación o mayor daño. En el datacenter, se han dejado rotulados los equipos de comunicación críticos que deben ser apagados ante un evento de ransomware con la siguiente imagen:

2. Erradicar: Eliminar malware, deshabilitar cuentas maliciosas, aplicar parches, reforzar la seguridad.
3. Recuperar: Restaurar sistemas desde copias seguras, verificar integridad de datos y asegurar la disponibilidad completa de los servicios críticos.

8. Lecciones Aprendidas (Post-Incidente)

Son responsabilidades del Comité de Seguridad:

1. Informe Final: Documentar causa raíz, alcance, impacto, costos y recomendaciones de mejora.
2. Revisión y Ajustes: Actualizar procedimientos, políticas y controles de seguridad.
3. Notificación y Cumplimiento: Reportar a las autoridades competentes según normativas aplicables.

9. Consideraciones de la Triada de Seguridad (C-I-A)

Son responsabilidades de la Dirección de Informática:

- Confidencialidad: Verificar y reforzar medidas para proteger datos sensibles.
- Integridad: Validar la autenticidad y exactitud de la información restaurada.
- Disponibilidad: Garantizar que los sistemas críticos estén nuevamente operativos.

10. Coordinación con Entidades Externas

Son responsabilidades del Comité de Seguridad:

- Mantener una lista actualizada de contactos externos (CERT.ar, fuerzas policiales, proveedores de TI).
- Cooperar con autoridades en casos que requieran investigación criminal o peritajes forenses.
- Colaborar con otras jurisdicciones que requieran de recursos en caso de ser necesario.

Anexo: Datos de Contacto Importantes

Internos

La siguiente lista de contactos sirve a los efectos del escalamiento:

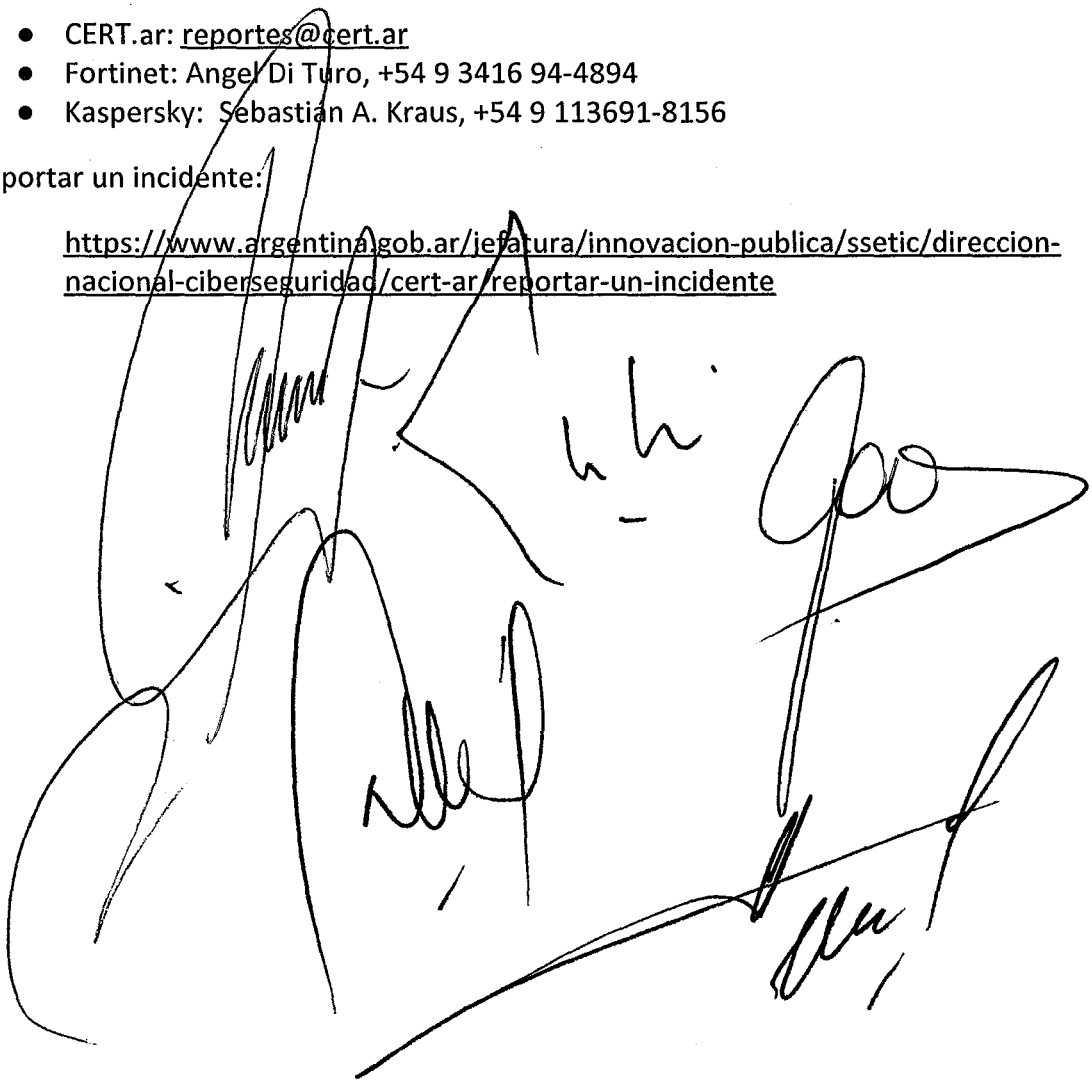
- CISO: Leandro Esteban Castro Aneas, lcastro@jussanjuan.gov.ar, +54 (9 264) 514-8977
- Analista de Ciberseguridad: Pablo Marquez, pmarquez@jussanjuan.gov.ar, +54 (9 264) 484-8616
- Jefe de Infraestructura: Marcelo Podestá, marcelopodesta@jussanjuan.gov.ar, +54 (9 264) 457-6330
- Subdirector de Informática: Raúl Rodríguez, raulrodriguez@jussanjuan.gov.ar, +54 (9 264) 626-7070
- Director de Informática: Miguel Ángel Godoy, miguelgodoy@jussanjuan.gov.ar, +54 (9 264) 460-4392

Externos

- CERT.ar: reportes@cert.ar
- Fortinet: Angel Di Turo, +54 9 3416 94-4894
- Kaspersky: Sebastián A. Kraus, +54 9 113691-8156

Reportar un incidente:

https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar/reportar-un-incidente



Anexo - Rol y Responsabilidades de la Mesa de Ayuda

La Mesa de Ayuda actúa como el primer punto de contacto para la identificación y escalamiento de incidentes de seguridad.

Su función principal es garantizar que cualquier actividad anómala o sospechosa sea registrada, categorizada y derivada al equipo responsable, asegurando una respuesta rápida y coordinada.

Dentro de la Mesa de Ayuda se incluye tanto al Departamento de Soporte a Usuarios (Responsable: Virginia Caballero) como al Departamento de Seguridad Informática (Responsable: Marisú Pages).

1. Recepción y Registro de Incidentes:

- Registrar detalladamente los incidentes reportados por usuarios, sistemas de monitoreo o personal técnico.
- Recabar información clave sobre el incidente, como quién lo reporta, fecha y hora del evento, descripción inicial, y sistemas o servicios afectados.

2. Evaluación Inicial:

- Realizar un análisis preliminar para determinar si el incidente debe clasificarse como un evento de alto impacto. Dentro de los eventos de alto impacto podemos mencionar los siguientes:

1. Ataque de Ransomware

- Cifrado de archivos críticos, interrumpiendo operaciones.
- Exigencia de pago para recuperar datos.
- Posible filtración de información sensible.

2. Filtración de Datos Sensibles

- Robo de información confidencial (datos personales, judiciales o estratégicos).
- Publicación o venta de datos en la dark web.
- Posibles sanciones legales y daño reputacional.

3. Compromiso de Cuentas Privilegiadas

◈ Un atacante obtiene acceso a credenciales de administradores.
◈ Modificación de configuraciones críticas o eliminación de registros.
◈ Escalada de privilegios y movimientos laterales en la red.

4. Caída Total de Infraestructura Crítica

◈ Fallos en servidores clave, bases de datos o servicios en la nube.
◈ Interrupción de servicios esenciales para la organización: Mev, Cloud, Zonda, Validador, etc.
◈ Costos elevados de recuperación y pérdida de productividad.

5. Ataque de Ingeniería Social (Phishing/Whaling)

◈ Empleados engañados para entregar credenciales o ejecutar malware.
◈ Suplantación de identidad de directivos para realizar transferencias fraudulentas.
◈ Puerta de entrada para ataques más graves (ransomware, espionaje, etc.).

- Verificar si el incidente tiene relación con problemas previamente reportados.

3. Notificación y Escalamiento:

- Informar a la Dirección de Informática y/o CISO según los protocolos establecidos.
- Escalar de inmediato los incidentes clasificados como de alto impacto al nivel correspondiente, de acuerdo a lo especificado en esta tabla:

Incidente	Orden para Reportar	Forma de reportar
Ataque de Ransomware	1. Informar al Área de Ciberseguridad. 2. Informar a Personal de Infraestructura. 3. Informar a	Llamado telefónico asegurándose que alguien conteste el llamado y tome el caso.

	Dirección.	
Filtración de Datos Sensibles	1. Informar al Área de Ciberseguridad. 2. Informar a Personal de Infraestructura. 3. Informar a Dirección.	Llamado telefónico asegurándose que alguien conteste el llamado y tome el caso.
Compromiso de Cuentas Privilegiadas	1. Informar al Área de Ciberseguridad. 2. Informar a Personal de Infraestructura. 3. Informar a Dirección.	Llamado telefónico asegurándose que alguien conteste el llamado y tome el caso.
Caída de la Infraestructura Crítica	1. Informar al área de Infraestructura. 2. Informar al Área de Ciberseguridad. 3. Informar a Dirección.	Llamado telefónico asegurándose que alguien conteste el llamado y tome el caso.
Ataque de Ingeniería Social	1. Informar al Área de Ciberseguridad. 2. Informar a Personal de Infraestructura. 3. Informar a Dirección.	Llamado telefónico asegurándose que alguien conteste el llamado y tome el caso.

4. Comunicación con los Usuarios:

- Actuar como punto de contacto para los usuarios finales afectados, informándoles sobre el estado del incidente.
- Ofrecer instrucciones básicas sobre cómo proceder, cómo desconectar dispositivos sospechosos.

5. Seguimiento:

- Monitorear el progreso de los incidentes reportados y mantener actualizado el estado en los sistemas de gestión.
- Asegurarse de que las áreas responsables tomen las acciones necesarias dentro de los tiempos definidos.

6. Documentación:

- Asegurar que toda la información relacionada con el incidente esté registrada en el sistema de gestión.
- Proveer un reporte inicial que se usará para generar el informe del incidente a entregar al Comité de Seguridad para el análisis posterior.

7. Apoyo durante la Recuperación:

- Facilitar la coordinación con usuarios afectados para la validación de los sistemas restaurados.
- Ofrecer soporte a los usuarios en el restablecimiento de operaciones normales.

Dr. Guillermo Horacio De Sanctis
MINISTRO

Dr. Marcelo Jorge Lima
MINISTRO

Dra. Adriana Verónica García Nieto
PRESIDENTA

Dr. Daniel Gustavo Olivares Yapur
MINISTRO

Dr. Juan José E. Victoria
MINISTRO

CORTE DE JUSTICIA
SAN JUAN

Dr. DANIEL GALVANI
FISCAL GENERAL
SUBROGANTE