**LEY N°21.796**

**PARTIDA 32**

**GLOSA 04**

**PLANES, POLÍTICAS Y ACCIONES DESTINADAS A FORTALECER LA CIBERSEGURIDAD**
**Y**
**PROCEDIMIENTOS DE RESPALDO**

| Descripción de la Glosa |
| --- |
| El Ministerio de Seguridad Pública informará, a más tardar el 31 de enero de 2026, a la Comisión Especial Mixta de Presupuestos y a las Comisiones de Desafíos del Futuro, Ciencia, Tecnología e Innovación, de Seguridad Pública y de Defensa Nacional del Senado y a las Comisiones de Futuro, Ciencias, Tecnología, Conocimiento e Innovación, de Seguridad Ciudadana y de Defensa Nacional de la Cámara de Diputados, acerca de todos los planes, políticas y acciones destinados a fortalecer la ciberseguridad. Asimismo, se deberá informar el o los protocolos internos de respaldo de información de los computadores.<br><br>Trimestralmente, se deberá informar la ocurrencia de incidentes y ataques informáticos registrados, así como el cumplimiento del o los protocolos de respaldo. |

## 1. Planes, Políticas y acciones destinadas a fortalecer la ciberseguridad

En relación a los planes, políticas y acciones destinados a fortalecer la ciberseguridad en la Subsecretaría de Prevención del Delito, como institución tenemos los siguientes objetivos para el 2026:

1) Publicar mediante Resolución Exenta la actualización de la política de seguridad de la información, alineada con lo exigido para los operadores de importancia vital según la Ley Marco de Ciberseguridad. Esta medida permite establecer un marco formal de control y gobierno, reduciendo riesgos de incumplimiento normativo que pueden derivar en sanciones, observaciones de entes fiscalizadores y costos asociados a la gestión de incidentes.

2) Desarrollar una norma general de protección de datos personales, en consideración a la próxima entrada en vigencia de la Ley de Protección de Datos Personales. Su implementación permitirá prevenir brechas de datos y eventuales responsabilidades legales, evitando costos económicos, reputacionales y operativos asociados a la exposición de información sensible.

3) Implementar un Centro de Operaciones de Seguridad de la Información y Ciberseguridad (SOC), con el objetivo de monitorear continuamente las redes y activos tecnológicos de la institución. Esto permitirá reducir significativamente los tiempos de detección y respuesta ante incidentes, disminuyendo el impacto operativo y los costos asociados a interrupciones de servicio o recuperación ante incidentes de seguridad.

4) Fortalecer el sistema de gestión de seguridad de la información, con el fin de mejorar la identificación, evaluación y tratamiento de riesgos. Esto permitirá una asignación más eficiente de los recursos institucionales, priorizando inversiones en función del nivel de exposición y criticidad de los activos.

5) Actualizar las normas y procedimientos asociados a la Política de Seguridad de la Información, asegurando su coherencia y aplicabilidad. Esto contribuye a estandarizar procesos, reducir errores operativos y evitar reprocesos, generando eficiencias en la gestión institucional.

6) Incorporar dos funcionarios adicionales a la sección de seguridad de la información y ciberseguridad, considerando que actualmente toda la función de la sección recae en el encargado. Esto permitirá distribuir adecuadamente las funciones y mejorar los tiempos de respuesta, evitando costos asociados a la falta de capacidad de respuesta ante incidentes o requerimientos normativos.

7) Realizar capacitaciones periódicas a los funcionarios en materias de protección de datos personales y ciberseguridad, buscando reducir la probabilidad de incidentes asociados a errores humanos, los cuales representan una de las principales causas de brechas de seguridad. Esto permite disminuir incidentes evitables, tales como phishing, pérdida de información o uso indebido de sistemas, contribuyendo además al cumplimiento normativo y a la reducción de riesgos operacionales.

En relación al **procedimiento de respaldo de equipos**, tanto los correos como los elementos de onedrive se respaldan automáticamente en nuestra plataforma de Microsoft y están disponibles por un periodo de 5 años desde la fecha de desactivación de la cuenta.

## 2. Ocurrencia de incidentes y ataques informáticos registrados, así como el cumplimiento del o los protocolos de respaldo.

En lo que respecta a incidentes, se registra únicamente un evento de carácter menor ocurrido el día 13 de febrero de 2026. Este correspondió a la detección de un software no deseado de tipo AdWare (clasificado como Spyware, asociado a la visualización de publicidad sin consentimiento del usuario) en un equipo ubicado en la recepción del piso 9, en dependencias de Teatinos 220. El equipo fue aislado de la red, analizado y restaurado durante la misma jornada, dándose el incidente por subsanado. No se evidenció propagación a otros equipos ni pérdida de información.

Se adjunta correo de alerta remitido a la ANCI, junto con la respuesta entregada por dicho organismo.

**Maria Teresa Lizana Leiva**

**De:** portal@notificaciones.anci.gob.cl
**Enviado el:** viernes, 13 de febrero de 2026 10:47
**Para:** Felipe Molins Gonzalez
**Asunto:** [Reporte REP-GHTVUCQ] Envío de reporte exitoso



Estimado(a) usuario(a),

El portal de la Agencia Nacional de Ciberseguridad recibió correctamente el siguiente reporte:

**Datos de la Institución afectada**

| | |
|---|---|
| **Razón social:** | Subsecretaría de Prevención del Delito |
| **Nombre de fantasía:** | SPD |
| **Email:** | spd-ciberseguridad@minsegpublica.gob.cl |
| **Teléfono:** | 225502676 |

**Datos del usuario que ingresó el reporte**

| | |
|---|---|
| **Nombre:** | Felipe Tomás Molins González |
| **Rut:** | 18.341.209-4 |
| **Email:** | fmolins@minsegpublica.gob.cl |
| **Teléfono:** | 225502676 |
| **Cargo:** | Encargado de Seguridad de la Información y Ciberseguridad |

**Reporte del incidente**

| | |
|---|---|
| **Etapa del reporte:** | Alerta temprana |
| **Identificador del reporte:** | REP-GHTVUCQ |
| **Fecha de toma de conocimiento del incidente:** | 13 de febrero de 2026 a las 09:15 |
| **Fecha estimada de inicio:** | 12 de febrero de 2026 a las 18:53 |
| **Necesita apoyo del CSIRT:** | No |
| **Recursos potencialmente afectados:** | • Equipos de Usuario Final |
| **Taxonomía:** | • Ejecución no autorizada de código |

**Descripción:** Se recibe correo de la SSP sobre alerta de IPS por tráfico sospechoso desde equipo institucional hacia sitios identificados como Spyware CnC. Se analiza el equipo y se aisla de la red de forma inmediata. En el análisis se

| | |
|---|---|
| | detecta comportamiento inusual por aplicaciones de tipo AdWare, tomándose las medidas correspondientes para la eliminación del mencionado malware. |
| **Potenciales repercusiones:** | No hay |
| **Repercusiones transfronterizas:** | No |
| **Causas principales:** | Durante la revisión del equipo se detectó en el historial de navegación acceso a sitios con alta presencia de publicidad y redireccionamientos exter, Las que podrían contener anuncios maliciosos o enlaces que al ser abiertos ejecutan descargas automáticas o instalan extensiones no deseadas. Es probable que, a partir de una interacción del usuario con alguno de estos elementos, un clic en un banner o ventana emergente, se haya ejecutado contenido no autorizado en el equipo, lo que explicaría los intentos de comunicación detectados hacia infraestructura clasificada como SpywareCnC, los cuales fueron bloqueados por el firewall institucional. |
| **Medidas de mitigación:** | El equipo fue aislado preventivamente de la red institucional una vez detectada la actividad sospechosa, con el fin de evitar cualquier posible comunicación adicional con infraestructura externa o propagación a otros sistemas. Posteriormente, se procedió a la restauración completa del equipo mediante la reinstalación de imagen de windows, lo que asegura la eliminación de cualquier componente potencialmente no autorizado y restablece las configuraciones y controles de seguridad definidos por la institución. |
| **IoC detectados:** | ○ **constructpreachystopper.com**<br>○ Tipo: Dirección web<br>○ Fuente o ubicación: Firewall perimetral FortiGate – Evento SpywareCnC (infected-domain)<br>○ Descripción: Dominio detectado en comunicación saliente desde endpoint institucional (Host SPD-057118), clasificado por el motor de seguridad como SpywareCnC. Se observaron múltiples intentos de conexión HTTPS bloqueados perimetralmente. El patrón es consistente con infraestructura asociada a PUP/adware. No se confirmó exfiltracion de datos al momento del analisus<br><br>○ **139.45.197.248**<br>○ Tipo: Dirección IP (versión 4) |

- Fuente o ubicación: Firewall perimetral FortiGate – Evento SpywareCnC (infected-ip)
- Descripción: Dirección IP externa identificada como destino de múltiples intentos de conexión desde endpoint institucional comprometido. Clasificada por el IPS como infraestructura SpywareCnC. Se registraron 59 eventos bloqueados vía HTTPS (443). Indicio de posible beaconing automático desde proceso local no autorizado o extensión de navegador

- **T1071.001**
- Tipo: Código de tácticas, técnicas o procedimientos MITRE ATT&CK
- Fuente o ubicación: Análisis interno – Comunicación C2 vía protocolo web
- Descripción: Comunicación con infraestructura de comando y control utilizando protocolo HTTPS. Tráfico saliente detectado y bloqueado por firewall institucional.

Este reporte no ha sido compartido con otras entidades reguladoras, por lo que debes hacerlo en caso de existir dicha obligación.

Ante cualquier consulta, puedes contactarnos a través del chat del reporte disponible en el Portal ANCI, haciendo click en el botón "Chat del reporte".

## Maria Teresa Lizana Leiva

**De:** Benjamín Iturra Piñones <biturra@anci.gob.cl>
**Enviado el:** viernes, 13 de febrero de 2026 11:07
**Para:** Felipe Molins Gonzalez
**CC:** SPD Ciberseguridad; Kevin Anguita Rojel; ANCI Ayuda; César López Hormazábal; Manuel Varela Mancilla
**Asunto:** Reporte REP-GHTVUCQ



Muy buenos días estimado Felipe,
Junto con saludarte y confirmar que recibimos el reporte indicado en el asunto quería informarte que por el momento, y entendiendo los antecedentes entregados en la alerta temprana, consideramos que el reporte corresponde a un evento de ciberseguridad que aún debe ser investigado por parte del equipo TI / Ciberseguridad institucional para ser declarado como un incidente de efecto significativo.
Nos parece muy bien las acciones de contención preventiva que tomaron con el equipo, pero antes de reportar deben confirmar que se cumplió con alguna de las condiciones indicadas el artículo 3° del reglamento de reportes de incidentes (https://www.bcn.cl/leychile/navegar?idNorma=1211466).
Por nuestra parte vamos a cerrar el reporte, liberándolos de la obligación de cumplir con los plazos y protocolos de segundo reporte y reporte final, sin embargo en caso de que con la investigación que están realizando confirmen alguna de las condiciones indicadas previamente, deben realizar un nuevo reporte, o en su defecto nos pueden solicitar que reabramos el reporte en comento.
Muchas gracias y esperamos que tengas feliz día.

Atte.,


**Benjamín Iturra Piñones**
Jefe de Departamento de
Respuesta a Incidentes
**Gobierno de Chile**
biturra@anci.gob.cl
anci.gob.cl