SERVICIO LOCAL DE EDUCACIÓN PÚBLICA ANTOFAGASTA

10 POLÍTICAS GENERALES DE CIBERSEGURIDAD

Lo que todas y todos debemos saber y hacer, en aplicación de la Ley N° 21.663

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/OMVP2U-764

¿Qué es la Ciberseguridad?

La ciberseguridad es el conjunto de prácticas, hábitos y medidas que usamos para proteger el equipamiento tecnológico, las redes, los sistemas y la información que manejamos, frente a accesos no autorizados, robos, daños o mal uso. No se trata solo de tecnología: depende, sobre todo, de las decisiones y el cuidado de cada persona en su trabajo diario.

Para el SLEP Antofagasta, esto significa proteger los sistemas de gestión escolar, el correo institucional, el equipamiento tecnológico de los establecimientos y, sobre todo, los datos personales de cerca de 45.000 estudiantes y de todos los funcionarios y funcionarias. Un descuido de ciberseguridad (una contraseña débil, un correo de phishing, un equipo sin protección) puede afectar la continuidad de las clases y la privacidad de las personas.

¿Por qué tenemos estas políticas?

El SLEP Antofagasta administra información de carácter sensible: datos de cerca de 45.000 estudiantes, además de datos de funcionarios, notas, asistencia y remuneraciones. Cuidar esa información es responsabilidad de todas y todos, no solo de la Unidad de Tecnologías de la Información.

La Ley N° 21.663 (Ley Marco de Ciberseguridad) obliga a los servicios públicos a proteger sus sistemas y datos, a contar con una política de ciberseguridad, y a reportar los incidentes graves a la Agencia Nacional de Ciberseguridad (ANCI) dentro de plazos establecidos. Estas 10 políticas traducen esa obligación legal en reglas simples y concretas para el trabajo de todos los días.

Política 1: Compromiso institucional y responsables de la ciberseguridad

La ciberseguridad es una responsabilidad de todo el SLEP Antofagasta, desde la Dirección Ejecutiva hasta cada establecimiento. El Servicio designa formalmente a un Encargado de Ciberseguridad y conforma un Comité de Ciberseguridad, quienes coordinan el cumplimiento de la Ley N° 21.663 y de estas políticas.

Lo que debemos hacer

- Conocer que existe un Encargado de Ciberseguridad y saber cómo contactarlo.
- Cumplir estas políticas en el ejercicio de sus funciones, sin excepción.
- Colaborar con las revisiones, auditorías y capacitaciones que organice el Servicio.
- Las jefaturas deben asegurar que su equipo conozca y aplique estas políticas.

Política 2: Uso responsable de los recursos tecnológicos

El equipamiento tecnológico, las redes, los sistemas y las cuentas institucionales son herramientas de trabajo. Deben usarse de forma responsable, cuidando que no queden expuestos a personas ajenas al Servicio ni se utilicen para fines distintos a las funciones del cargo.

Lo que debemos hacer

- Usar los equipos, redes y sistemas institucionales solo para fines laborales.
- No instalar programas ni conectar dispositivos externos (pendrives, discos) sin autorización de la Unidad de TI.
- Bloquear la pantalla del equipamiento tecnológico al alejarse del puesto de trabajo.
- No compartir el equipamiento tecnológico o la sesión institucional con terceros, incluidos familiares.
- Informar a la Unidad de TI si un equipo se pierde, es robado o presenta fallas sospechosas.

Política 3: Contraseñas seguras y verificación en dos pasos

Una contraseña débil o compartida es una de las formas más comunes en que ocurren los ataques informáticos. Cada persona es responsable de proteger sus propias claves de acceso.

Lo que debemos hacer

- Usar contraseñas largas y difíciles de adivinar, distintas para cada sistema.
- No compartir contraseñas con compañeros de trabajo, jefaturas ni terceros, bajo ninguna circunstancia.
- Activar la verificación en dos pasos (Clave Única u otro segundo factor) en todos los sistemas que lo permitan.
- Cambiar la contraseña de inmediato si se sospecha que alguien más la conoce.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/OMVP2U-764

- No anotar contraseñas en papeles visibles ni guardarlas sin protección en el equipamiento tecnológico o el celular.

Política 4: Protección de datos personales y de la información

El SLEP trata datos personales de estudiantes, apoderados y funcionarios, muchos de ellos de niños, niñas y adolescentes. Esta información debe tratarse con especial cuidado y solo debe ser usada para las funciones del cargo.

Lo que debemos hacer

- Acceder únicamente a la información necesaria para cumplir sus funciones (nadie debe revisar datos que no le corresponden).
- No compartir información de estudiantes o funcionarios por canales personales (WhatsApp personal, correo particular, redes sociales).
- No sacar copias ni fotografías de documentos con datos personales fuera de los sistemas autorizados.
- Guardar los documentos con información sensible en las carpetas y sistemas institucionales definidos, no en dispositivos personales.
- Reportar de inmediato si detecta que datos de estudiantes o funcionarios quedaron expuestos por error.

Política 5: Uso seguro del correo institucional y prevención de phishing

El phishing (correos falsos que buscan robar contraseñas o instalar virus) es una de las principales puertas de entrada de los ataques informáticos. Reconocerlo a tiempo depende de cada persona que usa el correo institucional.

Lo que debemos hacer

- Desconfiar de correos que piden con urgencia contraseñas, datos bancarios o clics en enlaces desconocidos.
- Verificar el remitente antes de abrir archivos adjuntos o hacer clic en enlaces.
- No usar el correo institucional para registrarse en páginas o servicios personales.
- Reportar de inmediato a la Unidad de TI cualquier correo sospechoso, sin responderlo ni reenviarlo.
- Participar en los simulacros de phishing que organice el Servicio; son parte del aprendizaje, no una evaluación punitiva.

Política 6: Reporte oportuno de incidentes de ciberseguridad

Un incidente es cualquier evento que pueda afectar la información o los sistemas del SLEP: un equipamiento tecnológico infectado, un acceso indebido, un correo de phishing exitoso, la pérdida de un equipo, o un sistema que deja de funcionar sin explicación. La Ley N° 21.663 exige reportar los incidentes graves a la ANCI dentro de plazos breves, por lo que el aviso interno debe ser inmediato.

Lo que debemos hacer

- Reportar de inmediato cualquier incidente o sospecha al canal definido por el Servicio (Unidad de TI / Encargado de Ciberseguridad).
- No intentar resolver el problema por cuenta propia si excede sus funciones, ni borrar información que pueda ser evidencia.
- Entregar toda la información posible: qué ocurrió, cuándo, y qué sistemas o datos podrían estar afectados.
- Recordar que reportar a tiempo protege al Servicio; no reportar por miedo a un error puede agravar el problema.

Política 7: Cuidado de equipos, redes y establecimientos

La seguridad también es física: un equipo mal resguardado o una red sin protección son puertas de entrada para un incidente. Cada establecimiento y dependencia del SLEP debe cuidar sus equipos y su conexión a internet.

Lo que debemos hacer

- Restringir el acceso a salas de servidores, racks de comunicaciones y equipos de red solo a personal autorizado.
- Mantener actualizado el equipamiento tecnológico y los sistemas (aceptar las actualizaciones que gestiona la Unidad de TI).

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/OMVP2U-764

- Proteger los notebooks y dispositivos móviles institucionales, especialmente al trasladarlos fuera del establecimiento.
- No conectar equipos personales a la red administrativa del Servicio sin autorización.
- Respaldar periódicamente la información relevante, siguiendo las indicaciones de la Unidad de TI.
- Mantener reportes periódicos del historial de navegación de los equipos del Servicio

Política 8: Continuidad del servicio educativo ante un incidente

Si un sistema falla o es afectado por un ataque, el SLEP debe poder seguir funcionando y proteger la continuidad del servicio educativo para los 79 establecimientos. Esto se logra preparando con anticipación cómo actuar.

Lo que debemos hacer

- Conocer los procedimientos alternativos (manuales o de respaldo) definidos para las funciones críticas de su unidad o establecimiento.
- Guardar copias de los documentos esenciales según lo indicado por la Unidad de TI, para poder seguir trabajando si un sistema no está disponible.
- Seguir las instrucciones de la Dirección Ejecutiva y del Comité de Ciberseguridad durante una crisis o incidente mayor.
- Participar en los simulacros de continuidad operacional cuando el Servicio los organice.

Política 9: Relación segura con proveedores y terceros

El SLEP trabaja con empresas y personas externas que prestan servicios tecnológicos (soporte informático, plataformas educativas, sistemas administrativos). Estos terceros también deben cumplir reglas de ciberseguridad, porque un descuido de un proveedor puede afectar al Servicio.

Lo que debemos hacer

- Contratar servicios tecnológicos solo a través de los canales y contratos formales del Servicio.
- Exigir que los contratos con proveedores tecnológicos incluyan cláusulas de ciberseguridad y protección de datos (responsabilidad de la Unidad Jurídica y de TI).
- No entregar accesos a sistemas institucionales a proveedores sin autorización ni supervisión de la Unidad de TI.
- Reportar de inmediato si un proveedor solicita información o accesos que parezcan indebidos.

Política 10: Capacitación, revisión y mejora continua

La ciberseguridad no se resuelve una sola vez: las amenazas cambian, la normativa se actualiza y las personas cambian de funciones. Por eso el SLEP capacita periódicamente a su comunidad funcionaria y revisa estas políticas de forma regular.

Lo que debemos hacer

- Participar en las capacitaciones de ciberseguridad que organice el Servicio, según su rol.
- Aplicar en el trabajo diario lo aprendido en las capacitaciones y comunicados internos.
- Proponer mejoras o dudas sobre estas políticas a través de su jefatura o del Encargado de Ciberseguridad.
- Saber que estas políticas se revisarán al menos una vez al año, o antes si cambia la normativa de la ANCI.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/OMVP2U-764

¿Qué pasa si no se cumplen estas políticas?

El incumplimiento de estas políticas puede exponer al SLEP y a la comunidad educativa a riesgos serios (pérdida o filtración de datos de estudiantes, interrupción de clases, sanciones de la ANCI). Según la gravedad, el incumplimiento puede derivar en medidas administrativas internas, conforme a la normativa que rige al personal del Servicio, además de las responsabilidades legales que correspondan a cada persona.

El objetivo de estas políticas no es sancionar, sino prevenir. Ante una duda o un error, lo correcto es siempre avisar de inmediato: reportar a tiempo evita que un problema pequeño se transforme en uno grande.

Aprobación

Este documento fue elaborado por el Encargado de Ciberseguridad y aprobado por la Comisión de Ciberseguridad (REX N°285 de 27 de noviembre de 2025, modificada por la REX N°339 de 08 de septiembre de 2026) y la Dirección Ejecutiva (s) del SLEP Antofagasta antes de su difusión oficial a toda la comunidad funcionaria.

Firmado por:
Pablo Ignacio Oyarzún Olivares
Coordinador de Infraestructura y Mantenimiento
Fecha: 11-09-2026 16:45 CLT
Servicio Local de Educación Pública de Antofagasta

Firmado por:
Bastián Francisco Padilla González
Profesional Ti
Fecha: 11-09-2026 16:47 CLT
Servicio Local de Educación Pública de Antofagasta

Firmado por:
Betzabet Cozbi Parra Parra
Director Ejecutivo (s)
Fecha: 11-09-2026 16:54 CLT
Servicio Local de Educación Pública de Antofagasta

Firmado por:
Marcelo Andrés Jorquera Bustos
Coordinador de Mantenimiento de Infraestructura Educacional
Fecha: 12-09-2026 17:05 CLT
Servicio Local de Educación Pública de Antofagasta

Firmado por:
Naiomi Natalia Saiz Aguirre
Profesional Jurídico
Fecha: 16-09-2026 09:15 CLT
Servicio Local de Educación Pública de Antofagasta

Firmado por:
Sergio Antonio Guerra Espinoza
Técnico En Subvenciones
Fecha: 16-09-2026 11:13 CLT
Servicio Local de Educación Pública de Antofagasta

Firmado por:
Claudio Alberto Lillo Triviño
Directivo Jefe Unidad Técnico Pedagógica (s)
Fecha: 17-09-2026 09:56 CLT
Servicio Local de Educación Pública de Antofagasta

Firmado por:
Catalina Leonor Conejeros Muñoz
Coordinadora Gdp
Fecha: 21-09-2026 09:09 CLT
Servicio Local de Educación Pública de Antofagasta

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/OMVP2U-764