PROREP

IMPULSANDO UNA INDUSTRIA CIRCULAR

Protocolo de Ciberseguridad y Manejo de Información de ProREP

Enero 2026

PROREP

ÍNDICE

PROREP

ÍNDICE

Ciberseguridad y Manejo de Información de ProREP

1. Antecedentes

Con el fin de asegurar el cumplimiento de la normativa vigente en materia de ciberseguridad por parte de la Corporación ProREP para la Gestión de Residuos ("**ProREP**"), así como la adopción de buenas prácticas internacionales, se efectuó una revisión de los principales estándares legales y técnicos aplicables a la gestión y almacenamiento de información en Chile.

Luego de ello, se explicitan los estándares utilizados actualmente por ProREP para dar cumplimiento a los estándares y buenas prácticas identificados.

1. Marco normativo nacional

En Chile, la ciberseguridad se encuentra regulada por diversas normas que establecen obligaciones de prevención, control y gestión de riesgos, las cuales no imponen un estándar técnico ni una certificación determinada. Entre las principales normas que se refieren a la materia objeto de análisis, se destacan:

- Ley N°21.663 – Ley Marco de Ciberseguridad: establece principios y deberes para prevenir, reportar y resolver incidentes de ciberseguridad, crea la Agencia Nacional de Ciberseguridad y define estándares técnicos obligatorios para sectores críticos.

- Ley N°21.459 – Ley de Delitos Informáticos: moderniza el marco legal sobre ciberdelitos y firma electrónica, alineando la normativa chilena con el Convenio de Budapest.

- Ley N°21.719 – Ley de Protección y Tratamiento de Datos Personales: crea la Agencia de Protección de Datos Personales y establece la obligación de implementar medidas adecuadas para garantizar la confidencialidad, integridad y disponibilidad de los datos, incluyendo evaluación de riesgos y la notificación de incidentes de seguridad.

2. Estándares Internacionales

Las normas de la serie ISO/IEC 27000 establecen buenas prácticas para la gestión de la seguridad de la información, abarcando desde la definición de políticas y controles hasta la

gestión de incidentes y riesgos. Si bien su adopción no es obligatoria, estas normas persiguen objetivos análogos a la legislación referida. De hecho, muchas de ellas han sido adoptadas como Normas Chilenas por el Instituto Nacional de Normalización (INN) y forman parte del marco normativo referido en la Política Nacional de Ciberseguridad[1].

Entre las más relevantes se encuentran:

- NCh ISO/IEC 27001:2023: Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de Gestión de la seguridad de la información – Requisitos.

- NCh ISO/IEC 27017: NCh-ISO IEC 27017:2016: Tecnología informática - Técnicas de seguridad - Código de práctica para los controles de seguridad de la información basado en ISO/IEC 27002 para los servicios en la nube.

- NCh ISO/IEC 27018: Tecnología de la información - Técnicas de seguridad - Código de prácticas para la protección de la información de identificación personal (PII) en nubes públicas que desempeñen el rol de procesadores de PII.

3. Servicios digitales utilizados por ProREP

Habiéndose revisado el marco normativo chileno vigente y los estándares internacionales aplicables, se ha estimado que los servicios digitales utilizados por ProREP para el almacenamiento de su documentación interna y la plataforma de recopilación de información sus socios, se encuentran alineadas con las exigencias legales chilenas y con las mejores prácticas internacionales en materia de seguridad de la información.

En específico, todos los correos electrónicos son enviados a través de una cuenta de Google mail empresa, mientras que los archivos y documentos de trabajo de ProREP son almacenados en la plataforma Google Drive, ambos servicios que forman parte del ecosistema Google Workspace, el cual cuenta con múltiples certificaciones internacionales de seguridad, incluyendo la ISO/IEC 27001, ISO/IEC 27017 y ISO/IEC 27018, entre otras[2].

Por otro lado, la plataforma de recopilación de información de Socios, gestionada por un proveedor especializado, utiliza los estándares empleados en Amazon Web Services (“**AWS**”), que cumple con los estándares ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018,

[1] https://anci.gob.cl/documents/4430/Política_Nacional_de_Ciberseguridad_2023-2028.pdf

[2] https://business.safety.google/intl/es/compliance/

SOC 1, SOC 2 y SOC 3, entre otros, garantizando la protección, disponibilidad y continuidad operativa de la información alojada[3].

Conforme a esta información, las certificaciones con las que cuentan los servicios de Google y AWS, dan cuenta de la implementación de medidas técnicas y organizativas robustas, el uso de mecanismos avanzados de cifrado y detección de amenazas, y la existencia de protocolos continuos de gestión y respuesta ante incidentes, por lo que se considera que la gestión y almacenamiento de información de ProREP se ajusta a las exigencias normativas y a las buenas prácticas internacionales en materia de seguridad de la información.

Por otra parte, se hace presente que los datos contenidos en la plataforma de la Corporación se encuentran protegidos mediante un mecanismo de autenticación basado en **JSON Web Tokens (JWT)**, generados a partir de credenciales de usuario y contraseña. En relación al manejo de seguridad de la información en tránsito, la transmisión de datos entre el cliente y el servidor está protegida mediante **protocolo HTTPS**, asegurando una comunicación cifrada de extremo a extremo.

A su vez, todos los recursos de la solución, tanto en el **front-end** (la parte visible con la que interactúan los usuarios), como en el **back-end**, (la lógica interna de la aplicación), están resguardados bajo este modelo de autenticación y autorización. El control de acceso a los distintos módulos y funcionalidades se determina en función de los **roles del sistema** y los **tipos de usuario** definidos, los que se encuentran organizados en base a un criterio de "mínimos accesos indispensables para el desempeño de la función".

En virtud de lo anterior, los trabajadores de ProREP cuentan con distintos perfiles y, por lo tanto, accesos, dependiendo de las tareas que realizan para la Corporación.

Desde el punto de vista de los usuarios de la Plataforma externos al personal de ProREP, también cuentan con accesos compartimentados y restringidos, según perfil, a saber: Productor, Consumidor Industrial, Reciclador o Gestor.

En ese sentido, la implementación del control de acceso se ha desarrollado para garantizar que la información esté disponible únicamente para los perfiles autorizados, asegurando así la integridad y confidencialidad de los datos.

[3] https://aws.amazon.com/es/compliance/programs/

4. Gestión y uso de contraseñas

Las contraseñas de la Corporación deberán propender hacia un esquema de autenticación multifactor (MFA), el que deberá estar habilitado para acceder al correo electrónico, sistemas administrativos, VPN, y todo servicio que permita acceso a información crítica.

Asimismo, y en la medida en que la Corporación disponga de dicho servicio, se podrá utilizar un sistema de administración de contraseñas validado, especialmente, para el acceso al correo electrónico de ProREP, de los Sistemas de Gestión documental que se utilicen y de la plataforma de declaración actualmente administrada por Pleyasoft, o la que lo suceda o reemplace.

La extensión y calidad de la contraseña deberá resguardar reglas de composición específicas, por ejemplo, exigiendo la utilización de un número mínimo de caracteres, y de mayúsculas, números y caracteres especiales.

A su vez, las contraseñas deberán ser modificadas ante cualquier evidencia o indicio de compromiso de la seguridad de las mismas. No se solicitarán expiraciones o modificaciones forzosas frecuentes, toda vez que dichos cambios pudieran generar brechas de seguridad.

No se permitirá el uso de contraseñas conocidas, filtradas, triviales o de uso común. La lista de contraseñas prohibidas (lista negra) deberá ser actualizada anualmente.

5.1. **Requisitos técnicos mínimos**

Longitud mínima: 15 caracteres para cuentas que usan solo contraseña; mínimo 8 cuando la contraseña es un factor dentro de MFA.

Longitud máxima: permitir al menos 64 caracteres (soportar frases largas o contraseñas complejas generadas por gestores de contraseñas).

Composición: no imponer reglas rígidas (no exigir combinaciones específicas de clases de caracteres) que conduzcan a patrones previsibles; permitir todos los caracteres imprimibles y espacios.

Comprobaciones: bloquear contraseñas encontradas en listas de contraseñas comprometidas (p. ej. Have I Been Pwned) y patrones obvios (“password”, “123456”,

nombres de la organización). Mostrar un medidor de fuerza y ayudar al usuario a elegir.

Almacenamiento: almacenar solo hashes con sal usando algoritmos resistentes a GPU (Argon2, bcrypt o scrypt) y parámetros actualizados; nunca guardar contraseñas en texto plano.

Bloqueo ante intentos fallidos: aplicar limitación de intentos o control de velocidad (rate limiting), desafío MFA tras intentos sospechosos y políticas de bloqueo proporcional.

5.2. **Gestión de cuentas privilegiadas y de servicio**

Cuentas administrativas: exigir factores adicionales (hardware security keys/passkeys) y sesiones con tiempo de vida corto; uso obligatorio de MFA fuerte y autenticación por clave pública cuando sea posible.

5.3. **Política de expiración y rotación**

Caducidad general: no exigir cambios periódicos (p. ej. cada 90 días) de forma automática. Forzar cambio solo cuando exista sospecha o evidencia de compromiso (detección de brecha, credenciales en listas negras, acceso sospechoso).

Excepciones: definir rotación forzada para cuentas privilegiadas o con acceso a sistemas críticos (ej. cada 180 días o según riesgo) y cuando el secreto sea almacenado fuera del vault seguro.

5.3. **Recuperación y restablecimiento de contraseñas**

No usar preguntas de seguridad débiles ni pistas que puedan facilitar el ataque. Proceso de restablecimiento: verificación segura (MFA, correo institucional controlado, verificación por mesa de ayuda con procedimiento de identidad) y registro completo del evento. Evitar reemitir la misma contraseña anterior.

5.4. **Monitorización y detección**

Se deberán monitorear intentos de autenticación (spraying, credential stuffing) y alertar ante anomalías. Integrar logs con SIEM y playbooks de respuesta. Aplicar detección de inicios desde nuevos dispositivos/ubicaciones sospechosas y exigir reautenticación/MFA adicional.

5. Modificación y difusión del Protocolo

Este Protocolo forma parte de la normativa interna de ProREP y debe observarse en armonía con las demás reglas que rigen el funcionamiento de la Corporación. Adicionalmente, se someterá a revisiones y actualizaciones con la frecuencia que corresponda.

La aprobación del documento y sus posteriores modificaciones corresponde al Directorio, debiendo posteriormente difundirse a todas las personas sujetas al Protocolo por los medios de comunicación habituales.

6. Entrada en vigencia del Protocolo

Este Protocolo tendrá vigencia desde el momento de su publicación en el sitio web de la Corporación.

PROREP

Impulsando una Industria Circular