10 de Agosto de 2021
Ficha N° 7 A.9.4.3
CSIRT DE GOBIERNO

Ficha de Control Normativo A.9.4.3

Sistema de gestión de contraseñas

I. INTRODUCCIÓN

Este documento, denominado “Ficha de Control Normativo", tiene como objetivo ilustrar sobre los diferentes controles normativos que se estima son prioritarios para todo Sistema de Gestión de Seguridad de la Información. Ciertamente cada control debe ser evaluado y aplicado según su mérito e impacto en los procesos de cada institución según el respectivo proceso de gestión del riesgo.

La experiencia nos ha permitido identificar algunos controles que tienen propiedades basales y que en la práctica se considera que debieran estar presentes en toda institución con grados de implementación “verificado” según la escala de madurez que ha promovido el CAIGG[1].

Nivel	Aspecto	% de cumplimiento	Descripción
1	Inicial	20%	No existe este elemento clave o no está aprobado formalmente y no se ejecuta como parte del Sistema de Prevención
2	Planificado	40%	Se planifica y se aprueba formalmente. Se programa la realización de actividades
3	Ejecutado	60%	Se ejecuta e implementa de acuerdo con lo aprobado y planificado
4	Verificado	80%	Se realiza seguimiento y medición de las acciones asociadas a la ejecución
5	Retroalimentado	100%	Se retroalimenta y se toman medidas para mejorar el desempeño

[1] https://www.auditoriainternadegobierno.gob.cl/wp-content/upLoads/2018/10/DOCUMENTO-TECNICO-N-107-MODELO-DE-MADUREZ.pdf

Por tanto estas directrices si bien no reemplazan el análisis de riesgo institucional, si permiten identificar instrumentos, herramientas y desarrollos que pueden conducir a la implementación del control aludido e ir mejorando la postura global de ciberseguridad institucional.

Todo esto bajo el marco referencial presente relativo al Instructivo Presidencial N°8 / 2018[2], el Decreto Supremo N°83 / 2005[3], el Decreto Supremo N°93 / 2006[4], el Decreto Supremo N°14 de 2014[5], el Decreto Supremo N°1 de 2015[6] y a la Nch-ISO IEC 27001[7].

[2] https://transparenciaactiva.presidencia.cl/instructivos/Instructivo-2018-008.pdf
[3] https://www.bcn.cl/leychile/navegar?idNorma=234598
[4] https://www.bcn.cl/leychile/navegar?idNorma=251713
[5] https://www.bcn.cl/leychile/navegar?idNorma=1059778&idParte=9409404
[6] https://www.bcn.cl/leychile/navegar?idNorma=1078308
[7] https://ecommerce.inn.cl/nch-iso-iec-27001202078002

II. SISTEMA DE GESTIÓN DE CONTRASEÑAS

En el nivel más alto, las organizaciones deberían definir una “política general de seguridad de la información" debidamente aprobada por la dirección y que establezca el enfoque de la organización para administrar sus objetivos de seguridad de la información.

Debajo de la política general debiera estructurarse una política específica que regule y entregue las directrices sobre la organización de la ciberseguridad dentro de la institución.

Todo esto debidamente armonizado con una adecuada política específica de Control de Accesos, que permita a los funcionarios acercarse e internalizar los conceptos para aplicarlos de manera transversal en su quehacer diario.

Esta directiva de control de acceso debe abarcar también las reglas que permitan gestionar un sistema robusto de contraseñas, integrando múltiples estrategias, tecnologías, criterios y buenas prácticas que ayuden a los usuarios a contar con un sistema de credenciales que dificulte al máximo los ataques de fuerza bruta y la adivinación básica basada en parámetros del entorno personal de los usuarios.

La institución, entonces, debe contar con un procedimiento de gestión de contraseñas, tanto para el personal interno de la institución como externos que, por necesidades de negocio, deban acceder a los sistemas institucionales.

Se deben considerar aspectos tales como protocolos de entrega de una contraseña al momento de crear un nuevo usuario, cambio de contraseña ante sospecha de uso por terceros, sistemas de autogestión para desbloqueo, entre otros aspectos.

Respecto de la conformación de la contraseña se deben establecer políticas que consideren la creación de contraseñas robustas, según se indica:

- No debe contener parte del nombre del usuario o parte de su fecha de nacimiento o parte de los números de su Cedula Nacional de Identidad.

- Debe tener un largo mínimo de ocho caracteres alfanuméricos, con letras mayúsculas y con letras minúsculas, y con caracteres especiales.

- Se debe establecer una política de caducidad de las contraseñas. Los procedimientos de creación de nuevas contraseñas no deben permitir el uso de contraseñas históricas.

Deben establecerse procedimientos de almacenamiento seguro de las contraseñas, que considere algoritmos de encriptación.

En relación al sistema de control de acceso que tenga la Institución, debe forzar al cambio de contraseña, ante bloqueos de la cuenta por intentos reiterados de acceso.

También se deben considerar los protocolos para las claves las cuentas de administración de plataforma, sean estos para servidores, bases de datos, equipos de comunicaciones, equipos de seguridad, etc.

Se debe establecer protocolos respecto a las claves de acceso para cuentas genéricas o de sistemas legacy.

Ver anexo I con un ejemplo de estructura de políticas y procedimientos.

III. RECOMENDACIONES Y MEJORES PRÁCTICAS ASOCIADAS AL CONTROL

El control:

Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.

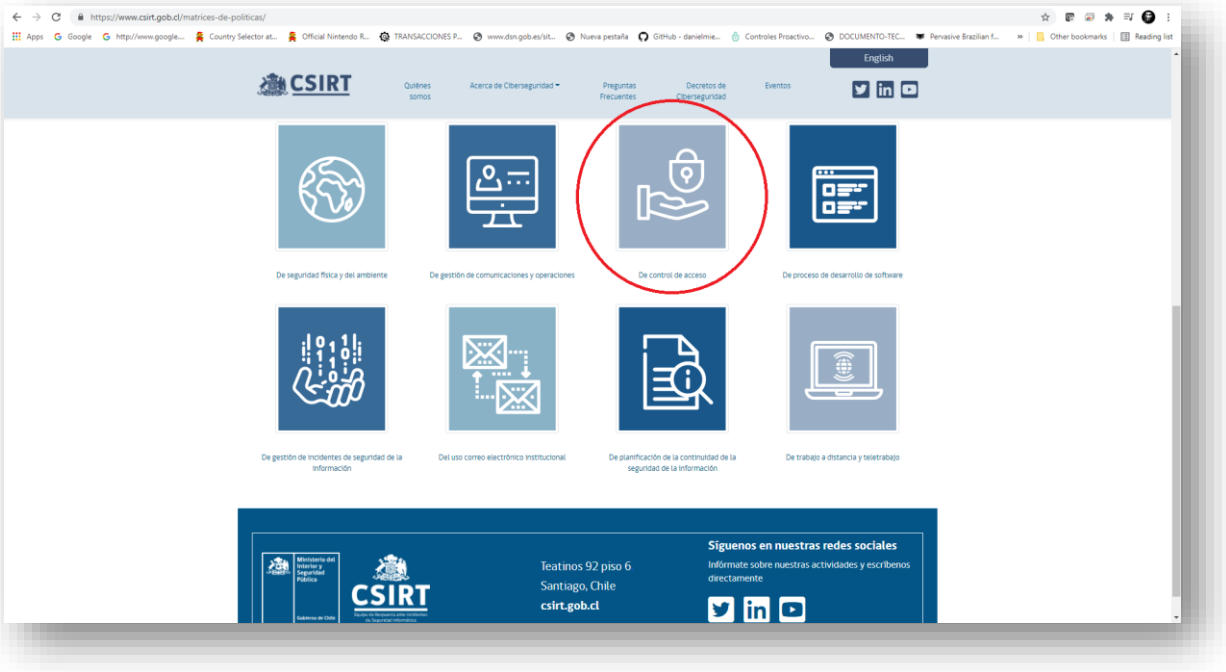
Recomendaciones generales

Se recomienda hacer un levantamiento de todos los activos de información institucionales y luego clasificarlos en diversas categorías; en este caso, contar con un levantamiento de todos los sistemas que requieren autenticación o verificación de identidad de los usuarios los acceden es tan importante como la autenticación entre sistemas automatizados y contraseñas de otros sistemas como los equipos de comunicaciones, las contraseñas de sistemas (SecretID), las contraseñas de acceso a bases de datos, entre otros.

Sobre este listado, se deben realizar los análisis respectivos de riesgos y tomar las medidas adecuadas de protección, dentro de las que están el Control de Acceso. Por tanto se debe desarrollar y aplicar una política específica de Control de Acceso y un procedimiento que cubra los aspectos operativos de un Sistema de Gestión de Contraseñas.

En el caso de que la institución cuente con activos de información que deben ser accedidos por terceros (personas, equipamiento en arriendo, bases de datos de terceros, etc.), deberá considerar este aspecto en el diseño de la política de control de acceso e incluirlo en la aplicación de ésta así como los respectivos procedimientos operativos que ayudan a su operativización.

El CSIRT ha preparado algunas políticas que pueden servir de punto de partida para aquellas instituciones que aún no tengan dichos documentos armados y aprobados por sus autoridades. Revíselas en el siguiente enlace[8].



La institución entonces debe desarrollar una Política de Control de Acceso, contemplando los aspectos de Gestión de Contraseñas, para todos los usuarios de los sistemas informáticos de la institución bajo el concepto de "necesidad de saber". Puede usar como base la propuesta de política elaborada por el CSIRT.

Un sistema de administración de contraseñas debería:

a) forzar el uso de IDs de usuario y contraseñas individuales para mantener la responsabilidad;

b) permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para permitir los errores de entrada;

c) imponer la selección de contraseñas de calidad;

d) obligar a los usuarios a cambiar sus contraseñas al primer inicio de sesión;

[8] https://www.csirt.gob.cl/matrices-de-politicas/

e) imponer cambios regulares de contraseñas según sea necesario;

f) mantener un registro de las contraseñas utilizadas anteriormente y evitar su nuevo uso;

g) no mostrar contraseñas en la pantalla mientras se ingresan;

h) almacenar archivos de contraseñas de manera separada de los datos del sistema de aplicación;

i) almacenar y transmitir contraseñas en forma protegida.

Algunas evidencias requeridas para validar cumplimiento

- Documento Política de Control de Acceso.
- Evidencias de revisiones periódicas a las cuentas de los sistemas
- Evidencias de revisiones de logs de las cuentas que más se bloquean en el mes.
- Procedimiento de cuentas privilegiadas, registro de apertura de ensobrado.

Responsable del Control

Encargado de TI, en conjunto con el Encargado de Ciberseguridad y/o Seguridad de la Información.

Consideraciones específicas

Registro de inicio seguro

El acceso a los sistemas operativos estará protegido, mediante un inicio seguro de sesión, permitiendo el acceso al usuario autorizado exclusivamente, contemplando las siguientes condiciones:

- No mostrar información del sistema, hasta que el proceso de inicio se haya completado.
- No suministrar mensajes de ayuda, durante el proceso de autenticación.
- Validar los datos de acceso, una vez se han entregado todos los datos de entrada.
- Limitar el número de intentos fallidos de conexión, auditando los intentos no exitosos posteriormente.
- No mostrar las contraseñas digitadas.

- No transmitir la contraseña en texto claro, es decir se transmite siempre encriptada y verificando que los protocolos de encriptado estén vigentes y no declarados como obsoletos o débiles.
- Se protegen los registros de los accesos a las estaciones de trabajo, permitiéndose el acceso exclusivamente para casos de auditorías e investigaciones instruidas por el Jefe de Servicio.

Gestión de contraseñas

La asignación de contraseñas se deberá controlar a través de un proceso formal de gestión a cargo de la [Unidad TIC]. Las recomendaciones mínimas para proteger las contraseñas y evitar que sean conocidas por otros, de modo de minimizar los riesgos de accesos no autorizados son:

- No escribirlas en papeles de fácil acceso, agenda, ni en archivos sin cifrar.
- No habilitar la opción "recordar clave en este equipo", que ofrecen los programas.
- No enviarla por correo electrónico.
- Mantener las contraseñas confidenciales en todo momento.
- No compartir las contraseñas con otros usuarios. Hay que recordar que las credenciales de usuario/contraseña pueden considerarse como una firma electrónica según la Ley N° 19.799.
- Cambiar su contraseña si piensa que alguien más la conoce.
- Seleccionar contraseñas que no sean fáciles de adivinar.
- El sistema de validación para el ingreso a la red (controlador de dominio o sistema equivalente) solicitará cambiar sus contraseñas cada 90 días.
- No utilizar la opción de almacenar contraseñas en Internet.

- No utilizar contraseña con números telefónicos, nombre de familia etc.
- No utilizar contraseña con variables (Por ejemplo: soporte1, soporte2, soporte3).

Uso de software del sistema

Todo software que se utilice en la institución debe cumplir con los licenciamientos correspondientes del proveedor y contratos de mantención de al menos las actualizaciones de solución de problemas de seguridad. Los equipos computacionales contemplan una instalación de software estándar descrito en la normativa "Utilización de equipos personales" e "Instalación legal de software" publicadas en la [Intranet o sitio web interno de la empresa]. En estas, se establece una política a nivel de controlador de dominio o sistema equivalente para la gestión centralizada de autenticación e identidad, que no permite la instalación de software y cambios de configuración del sistema, salvo que se trate de personal autorizado de la Unidad TIC.

Ningún usuario final, deberá tener privilegios de usuario administrador en ningún equipo o dispositivo.

Tiempo de inactividad de la sesión

Después de cinco (5) minutos de inactividad del sistema, se considerará tiempo muerto y se bloqueará la sesión automáticamente, sin cerrar las aplicaciones que se encuentren abiertas.

Los usuarios deberán bloquear sus sesiones, cuando abandonen temporalmente su puesto de trabajo (Tecla Windows + L) y apagar los equipos al finalizar la jornada laboral o cuando se ausenten por más de dos (2) horas.

Téngase presente que si se están desarrollando trabajos remotos que requieran el acceso al equipo, éste podrá quedar encendido pero debidamente bloqueado su acceso.

Control de acceso a la información

El control de acceso a la información a través de una aplicación se realizará a través de roles que administren los privilegios de los usuarios dentro del sistema de información.

El control de acceso a información física o digital se realizará teniendo en cuenta los niveles de clasificación y el manejo de intercambio de información.

Todo acceso a información confidencial debe estar registrado y auditado.

Alistamiento de sistemas sensibles

La Unidad TIC identificará según los niveles de clasificación de información, o por definición legal, o a requerimiento de otra unidad debidamente fundado, cuáles son los sistemas sensibles y que deben gestionarse desde ambientes tecnológicos aislados e independientes, con requerimientos de seguridad de la información robustos y resilientes, propios del tratamiento de infraestructura crítica o equipamiento de misión crítica.

Al aislar estos sistemas, se preverá que el intercambio de la información con otras fuentes de datos sea seguro, ya que no se permitirá duplicar información en otros sistemas, siguiendo las directrices de fuentes únicas de datos.

Estudie las múltiples opciones y recomendaciones para avanzar en la implementación de este control y así obtener resultados específicos y concretos que puedan mostrarse al Comité de Seguridad de la Información (o equivalentes). Procure buscar apoyo tanto en el entorno de Gobierno Digital[9] como en el CSIRT de Gobierno[10] (Ministerio del Interior y Seguridad Pública) si siente que está detenido en algún punto de la implementación de este control.

En caso de cualquier inquietud o sugerencia no dude en contactarnos en soc-csirt@interior.gob.cl.

[9] https://digital.gob.cl/
[10] https://www.csirt.gob.cl/

Anexo I: Ejemplo de estructura de Políticas y Procedimientos