27 de Julio de 2021
Ficha N° 5 A.9.1.1
CSIRT DE GOBIERNO

Ficha de Control Normativo A.9.1.1

# Control de Acceso

## 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°1 de 2015[5] y a la Nch-ISO IEC 27001[6].

[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=1078308
[6] https://ecommerce.inn.cl/nch-iso-iec-27001202078002

## II. CONTROL DE ACCESO

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.

Entonces, una organización debería identificar los activos pertinentes en el ciclo de vida de la información y establecer los controles de acceso pertinentes a su importancia, nivel de confidencialidad y nivel de criticidad.

Los propietarios de los activos deberían determinar las reglas de control de la información, los derechos y restricciones de acceso para los roles específicos de los usuarios hacia sus activos, con una cantidad de detalle y rigor en los controles que refleje los riesgos de seguridad de la información asociados.

Los controles de acceso son tanto lógicos como físicos (ver cláusula 11 de Nch-ISO/IEC2 27002:2013 [Seguridad física y ambiental]) y éstos se deberían considerar en conjunto. Los usuarios y los proveedores de servicios deberían contar con una declaración clara sobre los requisitos del negocio que se deberían cumplir con los controles de acceso.

La política debería considerar lo siguiente:

a) los requisitos de seguridad de las aplicaciones comerciales;

b) las políticas para la diseminación y autorización de la información, es decir el principio que se debería conocer y los niveles de seguridad de la información y la clasificación de ésta (ver 8.2 de Nch-ISO/IEC2 27002:2013);

c) coherencia entre los derechos de acceso y las políticas de clasificación de la información de los sistemas y redes;

d) legislación pertinente y cualquier tipo de obligación contractual en cuanto a la limitación de acceso a los datos o servicios (ver 18.1 de Nch-ISO/IEC2 27002:2013);

e) administración de los derechos de acceso en un entorno de red distribuido que reconozca todos los tipos de conexiones disponibles;

f) segregación de los roles de control de acceso, es decir solicitud de acceso, autorización de acceso y administración de acceso;

g) requisitos de autorización formal para las solicitudes de acceso (ver 9.2.1 y 9.2.2 de Nch-ISO/IEC2 27002:2013);

h) requisitos de revisión periódicos para los derechos de acceso (ver 9.2.5 Nch-ISO/IEC2 27002:2013);

i) eliminación de derechos de acceso (ver 9.2.6 de Nch-ISO/IEC2 27002:2013);

j) archivo de los registros de todos los eventos de importancia que involucran el uso y la administración de identidades de usuario e información de autenticación secreta;

k) funciones con acceso privilegiado (ver 9.2.3 de Nch-ISO/IEC2 27002:2013).

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

## III. RECOMENDACIONES Y MEJORES PRÁCTICAS ASOCIADAS AL CONTROL

### El control:

Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos del negocio y de seguridad de la información.

### Recomendaciones generales

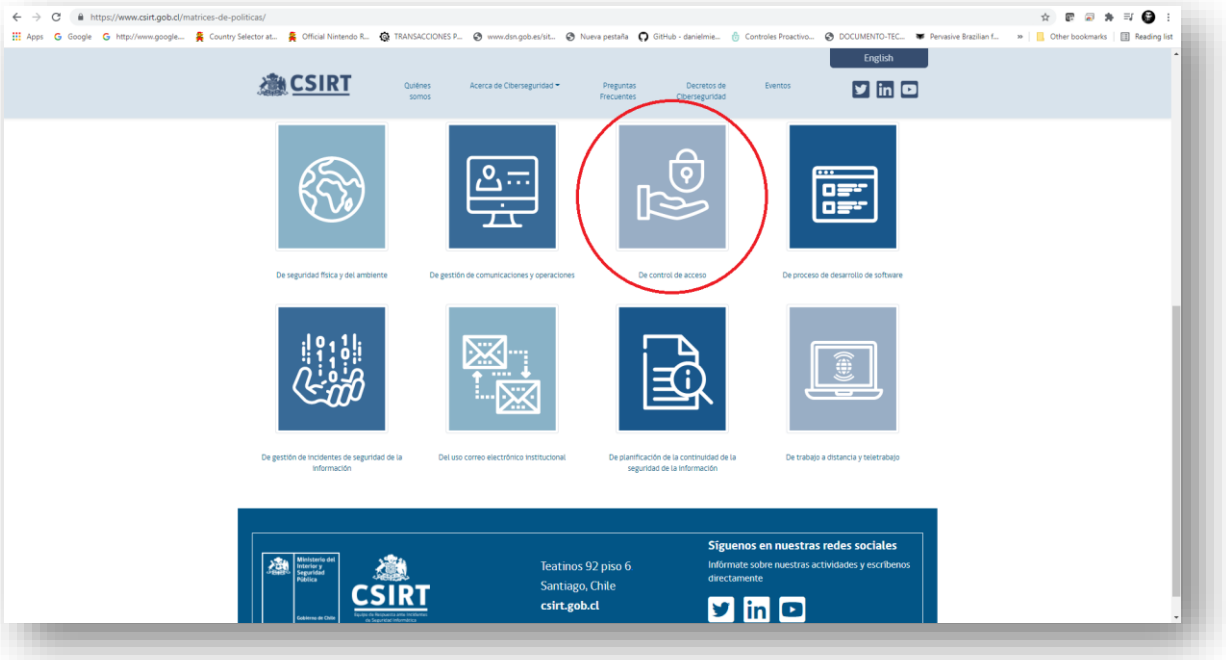
Se recomienda hacer un levantamiento de todos los activos de información institucionales y luego clasificarlos en diversas categorías, por ejemplo: Documentos físicos, Activos Electrónicos (archivos digitales, bases de datos, códigos fuente, entre otros), Plataforma Base (PC, Servidores, Sistema Operativo, Ofimática, Motores de Bases de Datos, Software Antimalware, entre otros), Infraestructura de Soporte al Giro (equipos de comunicaciones, impresoras, Datacenter, Aire Acondicionado, Edificio o Instalaciones, entre otros), y en particular, las personas que integran la institución.

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.

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**[7].

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




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

Para ello, debe desarrollar un perfilamiento de usuarios sobre los distintos sistemas y aplicativos, autorizando solo aquellos accesos que su perfil o descriptor de cargo permita.

El perfil de cada usuario debe ser debidamente autorizado por la jefatura del área a la cual pertenece o a la cual presta servicios, en el caso de externos.

En forma adicional, debe generar los procedimientos necesarios ante modificaciones de accesos por cambio de rol y/o eliminación de accesos.

En el caso que exista personal externo a la institución que deba acceder a los sistemas y aplicativos institucionales, se deberán crear cuentas personalizadas para ellos, con algún identificador que permita diferenciarlos de las cuentas de personal interno.

También, deben desarrollarse los procedimientos adecuados para aquellos accesos con cuentas genéricas y/o privilegiadas, los cuales incluyan casos en que se permita el uso de cuentas del tipo "Admin", "Root", "SA", entre otras. Para ello, se deben desarrollar procedimientos específicos para el resguardo de claves de estas cuentas a través de algún otro método.

### Algunas evidencias requeridas para validar cumplimiento

- Documento Política de Control de Acceso.
- Listado de perfiles de usuarios por sistema.
- Evidencia de autorizaciones de perfiles.
- Evidencia de Revisiones de Cuentas de Usuario en Dominio, eliminación de accesos para personal desvinculado, bloqueo de cuentas para casos con licencias prolongadas, revisión de cuentas de personal externo.
- Procedimiento de cuentas privilegiadas, registro de apertura.

### Responsable del Control

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

### Consideraciones específicas

Persiga los siguientes objetivos específicos:

- Identificar los requerimientos de seguridad de cada una de las aplicaciones.
- Identificar toda la información relacionada con las aplicaciones.
- Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de estaciones de trabajo.
- Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.
- Asegurar el cumplimiento de los requisitos normativos, estatutarios, reglamentarios y contractuales, que estén orientados hacia la seguridad de la información en la empresa.
- Establecer los niveles de acceso apropiados a la información de la empresa, brindando y asegurando la confidencialidad, integridad y disponibilidad que requiera cada sistema y usuario.

Establezca responsabilidades:

Todo el personal o terceros que dispongan de acceso a la plataforma tecnológica de la empresa son responsables del cuidado de su información de autenticación y de la información empresarial a la que acceda, cumpliendo con todas las normas de seguridad de la empresa.

Si tiene alguna necesidad específica no dude en contactar al Equipo de Comunicaciones del CSIRT para averiguar si existe materia sobre algún tema específico de ciberseguridad, si existe lo guiarán para que pueda acceder a él y distribuirlo en su institución o bien si existe la disponibilidad de recursos se podría desarrollar y disponibilizar para la comunidad.

Establezca mecanismos de gestión de contraseñas robustos:

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

No se olvide de incluir consideraciones para el Trabajo Remoto:

El trabajo remoto sólo será autorizado por el responsable de la División o centro de responsabilidad de la cual dependa el personal que solicite el permiso o según corresponda a las directivas del Jefe del Servicio. Dicha autorización sólo se otorgará para los servicios y sistemas en que se verifique se dan las condiciones de seguridad de las comunicaciones establecidas por las Políticas Institucionales en la materia, lo que será confirmado por la Unidad TIC y el Encargado de Ciberseguridad.

En resumen mantenga en mente:

Verificar, al menos, los siguientes aspectos para confirmar operatividad de la política de control de acceso y sus respectivos procedimientos:

- ✓ Política de usuarios y grupos
  - Definir los roles de usuarios y de grupos en función del tipo de información al que podrán acceder.
- ✓ Asignación de permisos
  - Asignar los permisos necesarios para que cada usuario o grupo de usuarios solo puedan realizar las acciones oportunas sobre la información a la que tienen acceso.
- ✓ Creación/modificación/borrado de cuentas de usuario con permisos
  - Definir y aplicar un procedimiento para dar de alta/baja o modificar las cuentas de usuario.
- ✓ Cuentas de administración
  - Gestionar las cuentas de administración de sistemas y aplicaciones teniendo en cuenta su criticidad.
- ✓ Mecanismos de autenticación
  - Determinar e implantar las técnicas de autenticación más apropiados para permitir el acceso a la información de la empresa.
- ✓ Registro de eventos
  - Establecer los mecanismos necesarios para registrar todos los eventos relevantes en el manejo de la información de la empresa.
- ✓ Revisión de permisos

- Revisar cada cierto tiempo que los permisos concedidos a los usuarios son los adecuados.

✓ Revocación de permisos y eliminación de cuentas

- Desactivar los permisos de acceso y eliminar las cuentas de usuario una vez finalizada la relación contractual.

Estudie las múltiples opciones y recomendaciones para avanzar en la implementación de este control y 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[8] como en el CSIRT de Gobierno[9] (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.

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

Anexo I: Ejemplo de estructura de Políticas y Procedimientos