3 de Agosto de 2021
Ficha N° 6 A.9.1.2
CSIRT DE GOBIERNO

Ficha de Control Normativo A.9.1.2

Accesos a las redes y a los servicios de la red

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. ACCESOS A LAS REDES Y A LOS SERVICIOS DE LA RED

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 a los servicios de red y a las redes mismas, pues estas últimas son la carretera que comunica a todos los usuarios, a todos los servidores y a todos los aplicativos, siendo relevante entonces, garantizar que quienes acceden a esta carreteras están debidamente autenticados.

Se debe formular una política en cuanto al uso de redes y servicios de red. Esta política deberá cubrir, al menos los siguientes aspectos:

a) las redes y los servicios de red a los que se tiene derecho de acceso;

b) procedimientos de autorización para determinar a quién se le permite acceder a qué redes y servicios con redes;

c) controles y procedimientos de administración para proteger el acceso a las conexiones de red y a los servicios de red;

d) los medios que se utilizan para acceder a las redes y a los servicios con redes (es decir, el uso de VPN o red inalámbrica);

e) requisitos de autenticación del usuario para acceder a los distintos servicios de red;

f) monitoreo del uso de servicios de red.

La política sobre el uso de servicios de red debería ser coherente con la política de control de acceso de la organización (ver Nch-ISO/IEC 27002:2013 cláusula 9.1.1).

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

III. RECOMENDACIONES Y MEJORES PRÁCTICAS ASOCIADAS AL CONTROL

El control:

Los usuarios solo deben tener acceso directo a la red y a los servicios de la red para los que han sido autorizados específicamente.

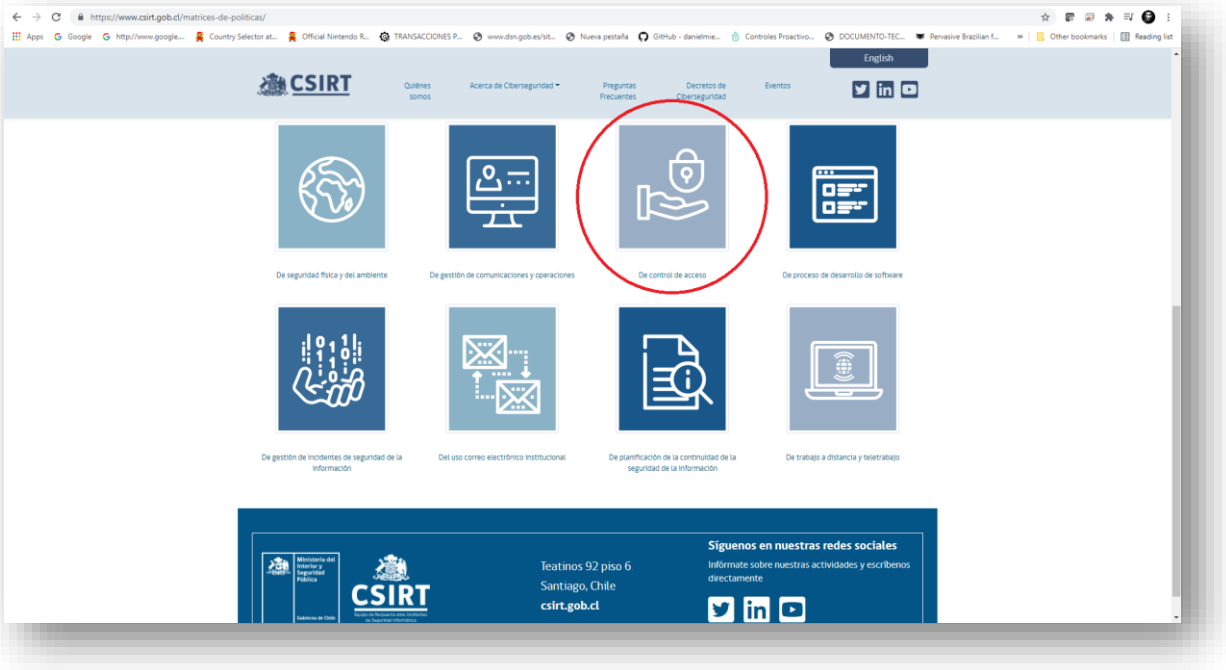
Recomendaciones generales

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), Redes, Servicios de Red 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].



La institución entonces debe desarrollar una Política de Control de Acceso, contemplando los aspectos de accesos a las redes y a los servicios de la red, 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.

La institución debe mantener un control sobre aquellos dispositivos que se conecten a la red, para ello, se recomienda:

- Contar con un mapa de red y documentar los componentes de red.
- Gestionar los dispositivos electrónicos personales.
- Contar con protocolos y dispositivos que controlen el acceso a la red.
- Contar con Gestión de Logs.
- Contar con un inventario de dispositivos de red, tales como: impresoras, escáner, entre otros, que permitan acceder a recursos dentro de la red.

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

Algunas evidencias requeridas para validar cumplimiento

- Listado de dispositivos permitidos y no permitidos dentro de la red.
- Protocolo política de uso de dispositivos electrónicos personales que se autorizan a conectar a la red de la institución.
- Protocolo o política de logs.

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 control de acceso a la red institucional:

La [Unidad TIC] controlará el acceso a los servicios de red tanto internos como externos con el propósito de garantizar la seguridad de los usuarios y mantener la estabilidad de los servicios, para lo cual se restringen los puertos de acceso por defecto, salvo casos particulares y debidamente justificados.

Las reglas de acceso a la red a través de los puertos estarán basadas en la premisa general de que "todo está restringido, salvo lo que esté expresamente permitido".

Desarrolle e implemente procedimientos para la utilización de los servicios de red:

La [Unidad TIC] establecerá procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

- Control el acceso a los servicios de red tanto internos como externos.
- Control de acceso a los equipos de red en forma local y/o remota.
- Identificación de las redes y servicios de red a los cuales se permite el acceso.

Establezca autenticación de usuarios para conexiones externas:

La [Unidad TIC] proveerá servicios de conexión remota a la plataforma empresarial basados en la tecnología y plataforma de red privada virtual: servicio VPN (por sus siglas en inglés), con lo cual el tráfico de datos entre usuario remoto y red institucional se encontrará debidamente encriptada.

Dependiendo del perfil del usuario y de si la clasificación de la información a transferir a través de la VPN es confidencial o interna, relacionada con la infraestructura crítica o de terceras partes ya sean públicas o privas, o relativas a la seguridad nacional, la autenticación deberá contar, progresivamente, con el nivel más alto de robustez, incorporando múltiples factores: "algo que el usuario sabe", "algo que el usuario tiene" y "algo que el usuario es", es decir, utilizar un segundo o triple factor de autenticación:

- Algo que sabemos, por ejemplo, una contraseña o un código PIN.
- Algo que poseemos, por ejemplo, una tarjeta de coordenadas o un token RSA.
- Algo que somos (autenticación biométrica), como la forma de la mano o la huella dactilar.

Establezca identificación de equipos en la red:

La [Unidad TIC] controlará e identificará los equipos conectados a la red institucional, mediante el uso de controladores de dominio, asignación manual de IP y portal cautivo para la conexión WIFI.

Establezca seguridad y Protección de los equipos de comunicaciones:

El acceso a la administración directa de los equipos de comunicaciones debe ser debidamente protegida para lo cual se configura acceso lógico con sistema de autentificación y debe estar ubicado en lugar físico resguardado de accesos de personal no autorizado.

Por lo cual, al realizar algún soporte o mantenimiento a los equipos de red, sólo personal autorizado por la [Unidad TIC] puede acceder a estos equipos.

Establezca separación de redes:

Para la gestión de la red, se aplicará segmentación de redes apoyada con dispositivos de seguridad denominados Cortafuegos o "Firewalls", para controlar el acceso entre los segmentos.

Los criterios para implementar son:

- Ubicación geográfica
- Funcionalidad
- Ubicación espacial
- Organizacional
- Tipos de conexión
- Otros.

Establezca control de conexión de las redes

La [Unidad TIC] controlará y limitará el acceso de los equipos, para los siguientes servicios:

- Conexiones Wifi será WPA2/AES/CMMP o superior.
- Mensajería instantánea.
- Telefonía IP a través de internet.
- Videoconferencia o Teleconferencias través de la intranet institucional e internet.
- Correo electrónico comercial no autorizado que sea identificado como tal.
- Descarga de archivos de sitio peer to peer (P2P).
- Conexiones a sitios de streaming o multimedia no autorizado.
- Servicios de escritorio remoto a través de internet.
- Cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeño de esta.
- El acceso a los sitios o páginas Web que contengan materiales amenazadores, pornográficos, racistas, xenofóbico, sexistas, negación, minimización grave, aprobación o justificación de

genocidios o delitos contra la humanidad o cualquier otro que degrade la calidad del ser humano, salvo aquellas requeridas por la naturaleza de las funciones institucionales del usuario.

Establezca un control del acceso a internet

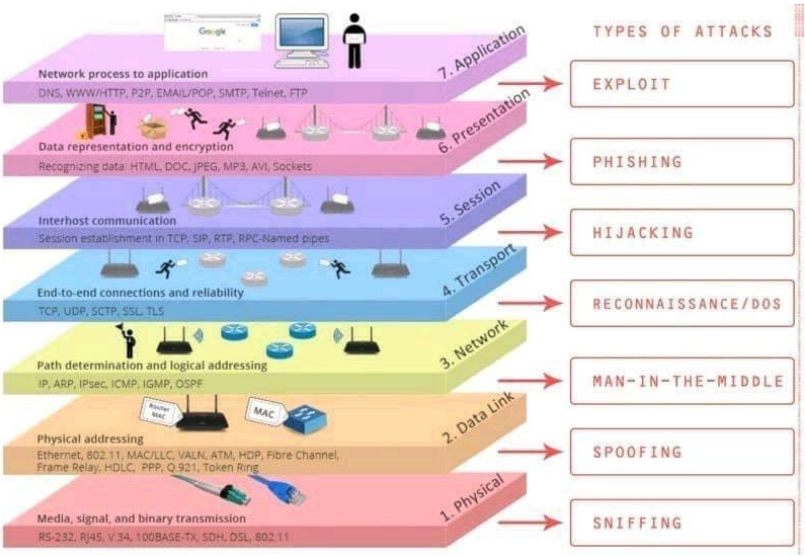
La [Unidad TIC] proveerá este servicio a través de sus ISPs (Proveedor de Servicio de Internet), el que será el único servicio de internet autorizado.

La instalación de cualquier dispositivo, no autorizado por la [Unidad TIC], que permita acceder a internet a un equipo de la empresa será considerada una infracción grave a la seguridad de la información.

No olvide establecer acciones de control de redes para el entorno de computación móvil y trabajo remoto.

CONCLUSIÓN

Este control de acceso a las redes como ya se explicó viene a reforzar la seguridad de acceso a las carreteras de los datos en las instituciones. Estas carreteras permiten el intercambio de datos institucionales y a acceder las aplicaciones corporativas o específicas de cada área de trabajo.



Si no se controla el acceso a estas carreteras de datos (redes de comunicaciones y sus servicios) es posible que terceras partes puedan conectarse a la red y capturar datos sensibles tanto corporativos como personales, levantar falsos servicios para robar datos o credenciales internas y así con el acceso a la carretera abierto y las llaves adecuadas en poder del ciberdelincuentes se pueden llegar a los activos más protegidos de la institución.

Es importante que seamos conscientes de la importancia de cuidar y controlar estos accesos, tanto lógicos como físicos. Si, físicos, pues hay que mirar por donde pasan nuestros cables de comunicaciones y si están bien resguardados, al igual que las puertas de acceso a la red que están distribuidas por la institución, desactivando aquellas que no están oficialmente en uso.

Entonces controle el acceso de entrada y salida de sus redes y sus servicios y desactive todas aquellas puertas de servicios tanto físicas como lógicas que no este utilizando.

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[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