16 de Noviembre de 2021
Ficha N° 18 A.13.1.1
CSIRT DE GOBIERNO

Ficha de Control Normativo A.13.1.1

Controles de 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 y según su 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 deben 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, permiten identificar instrumentos, herramientas y desarrollos que conducen a la implementación del control aludido, y con ello a mejorar la postura global de ciberseguridad de la institución.

Todo lo anterior, bajo el marco referencial vigente:

- El 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].
- La norma NCh-ISO/IEC 27001[7].
- La norma NCh-ISO/IEC 27002.
- La norma NCh-ISO/IEC 27010.
- La norma ISA/IEC-62443[8] (estándar global de ciberseguridad para la automatización industrial).
- La Ley N°21.180 sobre Transformación digital del Estado[9].

[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
[8] https://www.isa.org/
[9] https://www.bcn.cl/leychile/navegar?idNorma=1138479

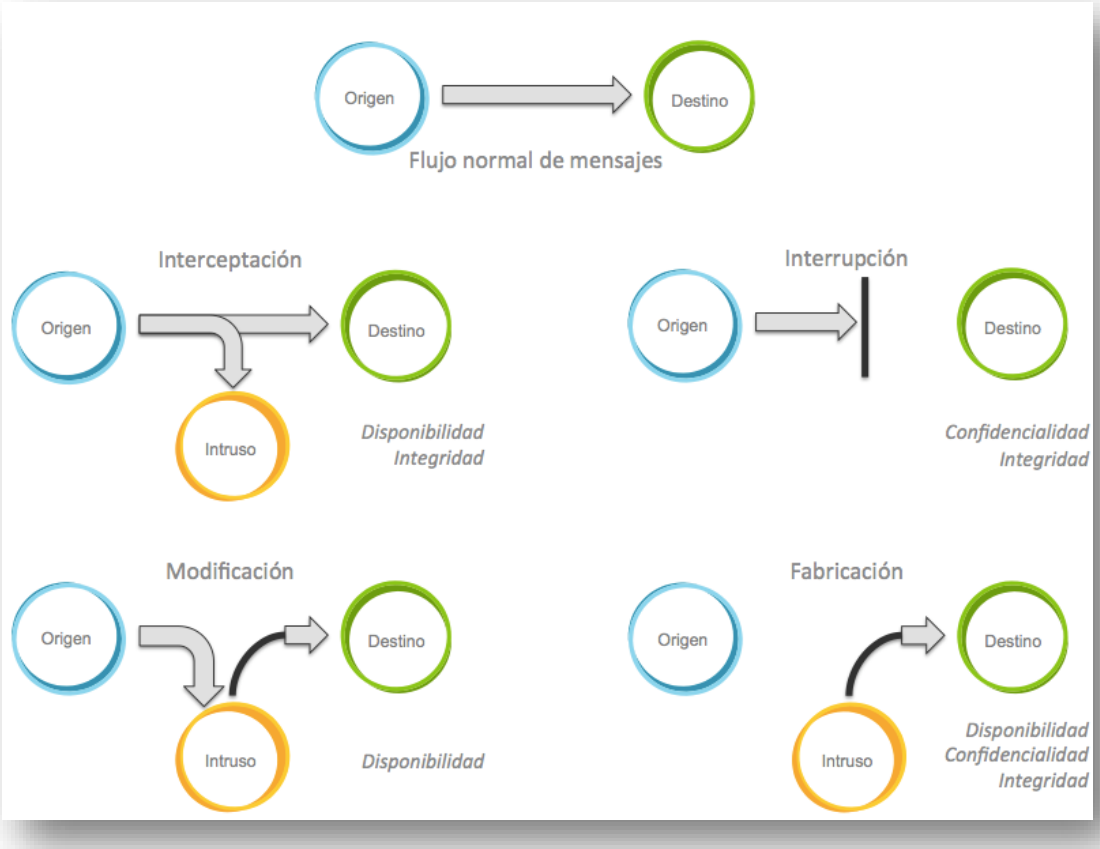
II. La importancia de la red y la ciberseguridad

En general, las normas sobre privacidad y comunicaciones electrónicas tienen por objeto garantizar la privacidad, la confidencialidad y la protección de los datos personales de las comunicaciones electrónicas en amparo de los derechos y libertades fundamentales de las personas físicas y jurídicas.

En este contexto, es importante incorporarlas y adecuarlas a los profundos cambios tecnológicos y de modelos de negocio online que permiten comunicaciones interpersonales (entre otros, servicios de voz sobre IP, de mensajería instantánea o de correo electrónico basados en la web), en ocasiones funcionalmente equivalentes a los ya regulados como la telefonía o los mensajes SMS.

¿Qué puede pasar cuando nuestros datos fluyen por la red?: Los datos pueden ser interceptados, interrumpida su transmisión, modificados o fabricados (inyectados falsamente).

En el siguiente diagrama podemos visualizar cada uno de estos casos:



Mecanismos de la Seguridad

Es importante diferenciar entre seguridad del mensaje y seguridad del sistema. Para la seguridad del sistema se establecen protocolos y propiedades que deben ser cumplidos por los sistemas, pero para la seguridad de los mensajes se pueden establecer diferentes mecanismos. Entre los más destacados tenemos la criptografía, técnica que hace uso de una clave y un algoritmo para ocultar un mensaje.

Cifrado Simétrico

El cifrado simétrico es aquel donde sólo es necesario la utilización de una llave para cifrar y descifrar. Las ventajas de este tipo de cifrado son la simplicidad, lo que hace que sea un método sencillo de usar, y la velocidad, ya que utiliza menos recursos informáticos que otros métodos de cifrado. La gran desventaja es la seguridad aplicada a este tipo de cifrado, ya que el envío de la clave debe realizarse por un método seguro, de lo contrario, está ayudando a que cualquier intruso sea capaz de hacerse con la clave de cifrado y descifrado.

Cifrado Asimétrico

El cifrado asimétrico se basa en el empleo de dos llaves, una llave pública para cifrar la información y una llave privada para descifrar la información. La clave pública y privada deben estar vinculadas. Se podría llegar a pensar que a través de la clave pública se puede deducir la clave privada, pero es totalmente incorrecto, ya que usa un algoritmo generado a partir de una contraseña, aspecto que hace imposible su deducción.

Una de las aplicaciones de este tipo de sistemas es la firma de documentos mediante funciones hash, verificando que el emisor es quien dice ser, firmando los documentos con su clave privada y corroborando la identidad con la clave pública. Estas funciones, llamadas funciones resumen, son algoritmos que crean una salida alfanumérica de longitud fija, representando un resumen de la información inicial.

Estas funciones, como se ha comentado, se utilizan para firmas de documentos pero también pueden servir para hacer ilegible una contraseña o para comprobar la correcta transmisión de un archivo. El problema de algunas funciones de este tipo son las colisiones, estas se basan en la entrada de dos diferentes fuentes devolviendo una misma salida para ambas. Para solucionar este error lo que se debe realizar es duplicar la seguridad con dos funciones hash diferentes. Inicialmente se aplica una y, a continuación, al mismo texto inicial le aplicas otra función hash, solucionando así la igualdad de ambas salidas, ya que sólo hay una solución para que de ambas funciones sea igual la salida.

Cifrado híbrido

Al contrario que en el cifrado simétrico, una de las desventajas del cifrado asimétrico es la cantidad de recursos que necesita, por ello se ha creado el método criptográfico híbrido, cuya finalidad es solventar las desventajas de ambos tipos de cifrado y escoger sólo las ventajas de cada método. Las desventajas de ambos métodos son la inseguridad (simétrico) y la velocidad (asimétrico). Este tipo de cifrado es mejor explicarlo por pasos:

1) El receptor genera una clave privada y una clave pública
2) La clave pública se envía al emisor
3) El emisor utiliza un cifrado simétrico con una clave simple para encriptar la información
4) La clave pública es utilizada por el emisor para cifrar la clave simple utilizada en el punto 3
5) El emisor envía la información cifrada de forma simétrica y la clave simple cifrada de forma asimétrica, la cual sólo puede descrifrar el receptor con su clave privada
6) El receptor desencripta la clave simple con su clave privada
7) El receptor desencripta la información con la clave simple generada en el punto 6

Tanto PGP (Pretty Good Privacy) como GnuPG (GNU Privacy Guard) son herramientas de cifrado y, en el caso de GnuPG, también de firmas digitales que usan sistemas de cifrado híbridos.

Cifrado homomórfico

Este cifrado se usa entre otros casos para la seguridad de los sistemas cloud. Debido a que la seguridad siempre ha sido un freno para este tipo de sistemas, el cifrado homomórfico es una técnica que nos da la posibilidad de procesar sobre datos cifrados y devolver dicho resultado cifrado de la misma manera. La base de este método es el poder realizar operaciones sobre texto cifrado, pero éstas deben ser sencillas tales como sumas, multiplicaciones, etc., garantizando así la confidencialidad de los mensajes o datos.

Basándonos en el glosario de términos que disponibiliza INCIBE[10] se pueden entender los términos más utilizados en este contexto:

Activo de información

Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

[10] https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

Actualización de seguridad

Modificaciones que se aplican, de forma automática o manual, en el software de los sistemas operativos o aplicaciones instalado en los dispositivos electrónicos, con el objetivo de corregir fallos de seguridad, errores de funcionamiento o bien para dotar a los dispositivos de nuevas funcionabilidades, así como incorporar mejoras de rendimiento.

Sinónimo: Parches de seguridad.

Acuerdo de licencia

Es una cesión de derechos entre un titular de derechos de propiedad intelectual (licenciante) y otra persona que recibe la autorización de utilizar dichos derechos (licenciatario) a cambio de un pago convenido de antemano (tasa o regalía) o de unas condiciones determinadas. Existen distintos tipos de acuerdos de licencias que pueden clasificarse en las siguientes categorías:

- acuerdos de licencia tecnológica
- acuerdos de licencia y acuerdos de franquicia sobre marcas
- acuerdos de licencia sobre derecho de autor

Amenaza

Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

Brecha de seguridad

Violaciones de la seguridad que ocasionan la destrucción, pérdida o alteración accidental o deliberada de datos personales cuando están siendo transmitidos, están almacenados o son objeto de otros tratamientos. Las brechas de seguridad también afectan a la comunicación o acceso no autorizados a dichos datos.

Ciberataque

Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema.

Ciberdelincuente

Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información, deterioro de software o hardware, fraude y extorsión. Casi siempre están orientados a la obtención de fines económicos.

Dirección IP

Las direcciones IP (del acrónimo inglés IP para Internet Protocol) son un número único e irrepetible con el cual se identifica a todo sistema conectado a una red. Podríamos compararlo con una matrícula en un coche. Así, una dirección IP (o simplemente IP) en su versión v4 es un conjunto de cuatro números del 0 al 255 separados por puntos. Por ejemplo: 192.168.121.40. En su versión v6, las direcciones IP son mucho más complejas, siendo hasta 4 veces más largas, más seguras y permitiendo un gran número de sistemas conectados a Internet. Un ejemplo es el siguiente: 2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b. Las direcciones IP pueden ser «públicas», si son accesibles directamente desde cualquier sistema conectado a Internet o «privadas», si son internas a una red LAN y solo accesibles desde los equipos conectados a esa red privada.

Dirección MAC

Una dirección MAC, también conocida como dirección física, es un valor de 48 bits único e irrepetible que identifica todo dispositivo conectado a una red. Cada dispositivo tiene su propia dirección MAC determinada que es única a nivel mundial ya que es escrita directamente, en forma binaria, en el hardware del interfaz de red en el momento de su fabricación. El acrónimo MAC hace referencia a Media Access Control que traducido al español significa Control de Acceso al Medio.

Sinónimo: dirección física, dirección hardware

Firmware

Tipo de software que permite proporcionar un control a bajo nivel de un dispositivo o componente electrónico, siendo capaz de proveer un entorno de operación para las funciones más complejas del componente o comportándose como sistema operativo interno en armonía con otros dispositivos o componentes.

Fuga de datos

La fuga de datos o de información es la pérdida de la confidencialidad de la información privada de una persona o empresa. Información que no debería ser conocida más que por un grupo de personas, en el ámbito de una organización o actividad, y que termina siendo visible o accesible para otros.

Integridad

La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales. La integridad, la disponibilidad y la confidencialidad constituyen las dimensiones claves en la seguridad de la información, ya que de un lado, se pretende evitar los accesos no autorizados a los datos, y de otro, se garantiza la no alteración de los mismos.

IPsec

Conjunto de protocolos cuyo propósito principal es asegurar las comunicaciones que se realizan a través del Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP que se envía o recibe.

LAN

Una LAN (del inglés Local Area Network) o Red de Área Local es una red informática de pequeña amplitud geográfica, que suele limitarse a espacios como una oficina, una vivienda o un edificio. Una Red de Área Local permite interconectar distintos dispositivos todo tipo, ordenadores, impresoras, servidores, discos duros externos, etc. Las Redes de Área Local pueden ser cableadas o no cableadas, también conocidas como redes inalámbricas. Por término general las redes cableadas son más rápidas y seguras, pero impiden la movilidad de los dispositivas.

Sinónimo: Red de Área Local

Malware

Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: malicious software. Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, backdoors, spyware, etc. La nota común a todos estos programas es su carácter dañino o lesivo.

Sinónimo: Software malicioso

Packet injection

Acción mediante la cual alguien intercepta una comunicación, capturando paquetes de información e introduciendo en la comunicación otros nuevos manipulados por el atacante con fines maliciosos.

Sinónimo: Inyección de paquetes

Software

Definimos software del inglés como un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en un dispositivo. El software conforma todas aquellas acciones que se pueden realizar gracias a las instrucciones previamente contempladas y programadas e incluidas dentro de un programa que permite al usuario interactuar con el sistema de forma fácil e intuitiva.

Red privada virtual

Una red privada virtual, también conocida por sus siglas VPN (Virtual Private Network) es una tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet. Al establecerlas, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado. Se trata realmente de una conexión virtual punto a punto entre dos redes LAN usando para la conexión una red pública como es Internet y consiguiendo que esta conexión sea segura gracias al cifrado de la comunicación.

Sinónimo: VPN

Riesgo

Es la posibilidad de que una amenaza o vulnerabilidad se convierta en un daño real para la empresa, que resulte en una pérdida o robo de información o en una detención de su actividad como consecuencia del daño ocasionado. El riesgo puede ser mitigado mediante políticas de seguridad y continuidad del negocio que suelen prever posibles ataques y proponen soluciones de actuación ante situaciones cuyo riesgo pueda ser elevado.

Segmentación de red

Técnica que consiste en dividir una red informática en otras redes más pequeñas o segmentos. El objetivo es aumentar el rendimiento de la red mejorando el ancho de banda al reducir el número de integrantes que se comunican entre sí. También se mejora la seguridad de la misma, permitiendo el acceso a determinados segmentos y solo al personal autorizado. De esta forma, en caso de un ciberataque a una red, solo se compromete el segmento afectado y no toda la red corporativa. Actualmente, algunas de las tecnologías más extendidas son las listas ACL (de control de acceso) y las VLAN (redes de área local virtuales).

Session Hijacking

También llamado secuestro de cookies, es un ataque basado en interceptar la sesión de un usuario en Internet para acceder a su información o servicios sin autorización. Se suele dar en sesiones no cifradas como las HTTP. Este tipo de ataque se ayuda de varias técnicas como Man-in-the-Middle o

XSS (cross site scripting) para lograr su objetivo, así como de programas de malware específicos para robar cookies de sesión.

Sniffer

Un sniffer es un programa que monitoriza la información que circula por la red con el objeto de capturar información. Las tarjetas de red pueden verificar si la información recibida está dirigida o no a su sistema. Si no es así, la rechaza. Un sniffer lo que hace es colocar a la placa de red en un modo el cual desactiva el filtro de verificación de direcciones (promiscuo) y por lo tanto acepta todos los paquetes que llegan a la tarjeta de red del ordenador donde está instalado estén dirigidos o no a ese dispositivo. El tráfico que no viaje cifrado podrá por tanto ser «escuchado» por el usuario del sniffer. El análisis de tráfico puede ser utilizado también para determinar relaciones entre varios usuarios (conocer con qué usuarios o sistemas se relaciona alguien en concreto). No es fácil detectar si nuestro tráfico de red está siendo «escuchado» mediante un sniffer, por lo que siempre es recomendable utilizar tráfico cifrado en todas las comunicaciones.

TCP/IP

Por TCP/IP se conoce a una familia de protocolos sobre los cuales funciona Internet, permitiendo la comunicación entre todos los servidores conectados a dicha red. TCP/IP consta entre otros muchos, del protocolo IP (Internet Protocol), que se ocupa de transferir los paquetes de datos hasta su destino correcto y el protocolo TCP (Transfer Control Protocol), que se ocupa de garantizar que la transferencia se lleve a cabo de forma correcta y confiable. Entre otros muchos, esta familia consta de los protocolos ICMP, UDP, DNS, HTTP y FTP.

Virus

Malware que tiene como característica principal que infecta ficheros ejecutables o sectores de arranque de dispositivos de almacenamiento.

Vulnerabilidad

Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto.

Sinónimo: Agujero de seguridad

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

III. RECOMENDACIONES Y MEJORES PRÁCTICAS ASOCIADAS AL CONTROL

El control: Controles de red

Las redes se deben gestionar y controlar para proteger la información en los sistemas y aplicaciones.

Recomendaciones generales

Se deben construir políticas y procedimientos que ayuden a establecer las directrices de ciberseguridad y guías operacionales que permitan a todos los intervinientes mantener seguras las redes y la información que fluye por ellas.

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[11].

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

La organización debe implementar controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados del acceso no autorizado. En particular, se deben considerar los siguientes elementos:

a) Establecer las responsabilidades y procedimientos para la administración de los equipos de redes;

b) Separar la responsabilidad operacional para las redes de las operaciones informáticas donde corresponda (ver 6.1.2 de Nch-ISO 27002);

c) Establecer controles especiales para resguardar la confidencialidad y la integridad de los datos que se pasan a redes públicas o a través de redes inalámbricas y para proteger a los sistemas y aplicaciones conectados (ver cláusula 10 y 13.2 de Nch-ISO 27002); es posible que se requieran controles especiales para mantener la disponibilidad de los servicios de red y los computadores conectados;

d) Aplicar los registros y monitoreos adecuados para permitir el registro y la detección de acciones que pueden afectar o que son pertinentes a la información de seguridad;

e) Actividades de administración se deberían coordinar de cerca tanto para optimizar el servicio a la organización como para garantizar que los controles se aplican de manera coherente a través de toda la infraestructura de procesamiento;

f) Autenticar los sistemas de la red;

g) Restringir la conexión de los sistemas a la red.

La institución deberá determinar diversas acciones para asegurar el acceso a la red de datos, para ello tendrá que:

- A nivel de la administración de la red: Considerar roles específicos para esta labor, siendo distintos a los roles de administración de servidores, bases de datos, estaciones de trabajo, dispositivos de seguridad. Para la administración de los dispositivos de red, deberá utilizar herramientas utilitarias seguras y actualizadas.

- A nivel del acceso a la red física: Controlar el acceso a la red, permitiendo acceso solo a los equipos computacionales y dispositivos debidamente autorizados para ello. Para lograr esto, puede implementar soluciones básicas como la deshabilitación de puntos de red no utilizados, permitir acceso a través de la autorización de la MAC Address de la tarjeta de red, o incluso contar con soluciones robustas como la incorporación de NAC (Network Access Control).

- A nivel de acceso a la red inalámbrica: Permitir el acceso a aquellos debidamente autorizados para tales efectos. Sin embargo, ante la posibilidad de que se masifique el uso de redes inalámbricas para conectar a Internet, diversos dispositivos personales, se recomienda separar las redes inalámbricas, con VLAN independientes, según el acceso que se requiera, por ejemplo, para la red invitados, contar con una VLAN que solo permita acceder a Internet, sin permitir conectarse a algún dispositivo o servicio de la red institucional. Para las conexiones inalámbricas, se sugiere implementar un sistema de portal cautivo, para añadir una capa adicional a la seguridad de estas conexiones.

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[12] como en el CSIRT de Gobierno[13] (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.

[12] https://digital.gob.cl/
[13] https://www.csirt.gob.cl/

Anexo I: Ejemplo de estructura de Políticas y Procedimientos