31 de agosto de 2021
Ficha N° 10 A.12.2.1
CSIRT DE GOBIERNO

Ficha de Control Normativo A.12.2.1

Controles contra Códigos Maliciosos

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], a la Nch-ISO IEC 27001[7] y a la norma ISA-62443[8] según corresponda.

[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/

II. CONTROLES CONTRA CÓDIGOS MALICIOSOS

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 Seguridad de las Operaciones, que permita a los funcionarios acercarse e internalizar los conceptos para aplicarlos de manera transversal en su quehacer diario.

Esta directiva de debiera incorporar instrucciones, medidas y controles para prevenir la acción de código malicioso.

El código malicioso es lo que comúnmente conocemos como virus o malware. En este sentido las instituciones destinan un gran esfuerzo en luchar contra estas amenazas, por eso es importante saber cuáles son las más comunes y en que pueden afectar a sus usuarios y a la institución misma a través de sus sistemas tecnológicos para el procesamiento de información o gestión de sus servicios internos y externos.

Se debe tener especial atención por parte de las instituciones en asegurar que sus herramientas y dispositivos aseguren una integridad, confidencialidad y disponibilidad de los datos. No olvidemos que los datos de una institución son lo que garantizan la continuidad de la misma. Una pérdida o robo de los mismos, perjudicaría gravemente a la institución afectando tanto a su reputación como a la actividad normal

de la institución, pudiendo significar incluso el cierre operacional del servicio público por tiempos prolongados.

¿Qué es el código malicioso o malware?

Son programas que tienen como objetivo acceder a tu sistema sin que detectes su presencia. En función de la intención del Cracker, el programa podría:

- Robar credenciales, datos bancarios, información o cualquier activo de información.
- Crear redes botnet con los computadores institucionales.
- Utilización no autorizada de los recursos computacionales (CPU/RAM/DISCO).
- Destruir o inutilizar un sistema de tratamiento de información o sus partes o componentes, o impedir, obstaculizar o modificar su funcionamiento.
- Usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma, interceptarla, interferirla o acceder a él.
- Alterar, dañar o destruir los datos contenidos en un sistema de tratamiento de información.
- Revelar o difundir los datos contenidos en un sistema de información.
- Cifrado del contenido. Con esto se intenta que los usuarios paguen un rescate por sus datos.

¿Cuáles son los tipos de código malicioso más comunes?

Virus

Tiene como objetivo alterar el funcionamiento de los equipos infectados, su modo de actuar es mediante la ejecución del código, alojarse en la memoria RAM. Por lo que son realmente dañinos a la hora de consumir recursos de nuestro equipo, provocando una pérdida de productividad o daños a nuestros datos.

Gusanos

También conocidos como Worms tienen como peculiaridad replicarse a si mismo sin la necesidad de una persona. Estos se adhieren a la memoria RAM y ocasionan problemas debido a que al multiplicarse consumen

recursos. Son capaces de auto propagarse por medio de la red.

Troyanos

Los troyanos son denominados así por el hecho de aparentar un software inofensivo para el usuario, pero que al ejecutarlo permite al atacante hacerse con el acceso al equipo infectado. Estos por lo general no provocan daños al sistema, pero se usan para el robo de datos y credenciales personales.

Keyloggers

Son software con intención de registrar las pulsaciones realizadas en el teclado, de esta forma el registro de lo que escribimos es enviado al delincuente, lo que pone en peligro contraseñas importantes como: números de tarjetas bancarias u información privada.

Spyware

Estos programas recopilan información de tu equipo sin el consentimiento del propietario, estos softwares utilizan CPU y memoria RAM. Entre sus funciones reduce el rendimiento del sistema, enseñan anuncios de programas (por lo que en ocasiones se les denomina adwares), abren ventanas emergentes, instalan otros programas…

Bots maliciosos

Son considerados como troyanos de puerta trasera, se instalan en equipos vulnerables mediante un sistema de rastreo en internet, una vez infectado el equipo, los ordenadores forman parte de una botnet y cumplen las órdenes de los ciberdelincuentes.

Virus de macros

Estos virus usan documentos de Word o Excel para ejecutar macros en nuestra biblioteca de macros y acabará ejecutándose en diferentes documentos que se abran con la aplicación.

De esta forma se pueden infectar equipos mediante documentos aparentemente normales como un Word, Excel, Access y similares.

Sus efectos suelen ser desde el robo de los contactos de correo electrónico, hasta borrar tus datos.

Estos son algunos ejemplos de amenazas que conocemos como código malicioso, y para evitar ser víctima de estos malwares siempre debemos tomarnos la seguridad informática enserio y contar con elementos como firewalls (en todos los canales de entrada y salida de información institucional) y antivirus (modernos y con actualizados inspeccionado todos los computadores y servidores institucionales). Además de asegurarnos de que contamos con una buena formación en seguridad informática y un equipo que esté vigilando las consolas centrales que monitorean estos dispositivos para actuar lo más rápidamente posible cuando alguno de esto códigos maliciosos logre infiltrase en nuestros sistemas.

Es muy importante tener en cuenta que es muy probable que en algún momento algún malware traspasará nuestras defensas y alcanzará a afectar alguno de nuestros sistemas, servidores o computadores, y para esta situación tenemos que estar preparados con un plan de respuesta específico, que le permita al equipo de seguridad actuar rápidamente para aislar el incidente y contenerlo rápidamente.

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

III. RECOMENDACIONES Y MEJORES PRÁCTICAS ASOCIADAS AL CONTROL

El control:

Se deben implantar controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto con los procedimientos adecuados para concientizar a los usuarios.

Recomendaciones generales

La protección contra el malware se debería basar en controles de software de detección de malware y de reparación, la concientización sobre la seguridad de la información, el acceso adecuado al sistema y la administración de cambios. Se deberían considerar las siguientes pautas:

a) establecer una política formal que prohíbe el uso de software no autorizado (ver 12.6.2 y 14.2.);

b) implementar controles que evitan o detectan el uso de software no autorizado (es decir, la creación de una lista blanca de aplicaciones);

c) implementar controles que eviten o detecten el uso de sitios web desconocidos o que se sospecha son maliciosos (es decir, la elaboración de una lista negra).

d) establecimiento de una política formal para protegerse contra los riesgos asociados al obtener archivos y software ya sea de redes externas o a través de cualquier otro medio, indicando las medidas de protección que se deberían tomar;

e) reducción de las vulnerabilidades que se podrían desencadenar por el malware, es decir, a través de la administración de vulnerabilidades técnicas (ver 12.6);

f) realizar revisiones periódicas del software y del contenido de los datos de los sistemas que apoyan los procesos críticos del negocio; se debería investigar formalmente la presencia de cualquier tipo de archivos o modificaciones no autorizados;

g) instalación y actualización periódica de software de detección de malware y reparación para analizar computadores y medios como control de precaución o, de manera rutinaria; el análisis debería incluir:

1) analizar solo los archivos recibidos a través de redes o mediante cualquier forma de medios de almacenamiento, en busca de malware antes de su uso;

2) analizar datos adjuntos de correos electrónicos en busca de malware antes de su uso; este análisis se debería realizar en diferentes lugares, es decir, en servidores de correo electrónico, computadores de escritorio y al ingresar a la red de la organización;

3) analizar páginas web en busca de malware;

h) definir procedimientos y responsabilidades que involucren la protección contra malware en los sistemas, capacitándose sobre su uso, informando sobre y recuperándose ante ataques de malware;

i) preparar planes de continuidad comercial adecuados para recuperarse contra ataques de malware, incluidos todos los datos, respaldo de software y disposiciones de recuperación necesarios (ver 12.3);

j) implementar procedimientos para recopilar información de manera regular, como la suscripción a listas de correo electrónico o verificar los sitios web que brindan información sobre el nuevo malware;

k) implementar procedimientos para verificar la información relacionada al malware y asegurarse de que los boletines de advertencia son precisos e informativos; los gerentes se deberían asegurar de que se utilicen fuentes calificadas, es decir, publicaciones de reconocido prestigio, sitios de internet o proveedores productores de software de protección contra malware confiables para diferenciar entre malware falso y el real; todos los usuarios deberían estar en conocimiento del problema de malware falso y qué hacer en caso de recibirlo;

l) aislar entornos donde pueden se pueden generar impactos catastróficos.

La Institución debe implementar diversas acciones para evitar infecciones de malware dentro de su red. Para ello, debe comenzar con una robusta Política de Protección al interior de la organización, considerando que todos los dispositivos conectados a su red deben contar con software para la detección y protección contra malware, cuyos privilegios para la deshabilitación temporal o permanente sean de responsabilidad exclusiva del administrador de esta plataforma. Por otra parte, se debe complementar esta política con otras que tienen relación con el uso de la plataforma, tales como, la restricción de privilegios de las cuentas de usuario de sistema operativo y aplicativos, uso adecuado de internet, uso de correo electrónico, segmentación adecuada de la red, uso de dispositivos de almacenamientos removibles (pendrives, discos duros, memorias, etc.), cierre de puertos no utilizados en estaciones de trabajo y servidores, entre otras.

Una vez establecida las Políticas, deberá realizar diversas jornadas de sensibilización al personal interno y externo que se conecta a la red institucional, y complementar estas sesiones con mensajes adecuados respecto al Phishing, qué hacer si se detecta un malware, Navegación segura en Internet, entre otros aspectos.

Además, todas las estaciones de trabajo y servidores, deben contar con las últimas actualizaciones de seguridad tanto de sistema operativo como a nivel de aplicativos, con el objeto de que el malware no aproveche alguna debilidad o vulnerabilidad no parchada o actualizada para propagarse dentro de la red.

Se deben aplicar reglas de uso de dispositivos removibles, sean estos personales e institucionales para el almacenamiento de información, que incluyan escaneo automático de estos dispositivos, bloqueo para uso, deshabilitación de *autorun* o autoejecución desde dispositivos de almacenamientos removibles, etc.

En la zona perimetral, la institución debe contar con soluciones *AntiMalware* para los servidores de correo y otras que protejan los sistemas o sitios web publicados a Internet.

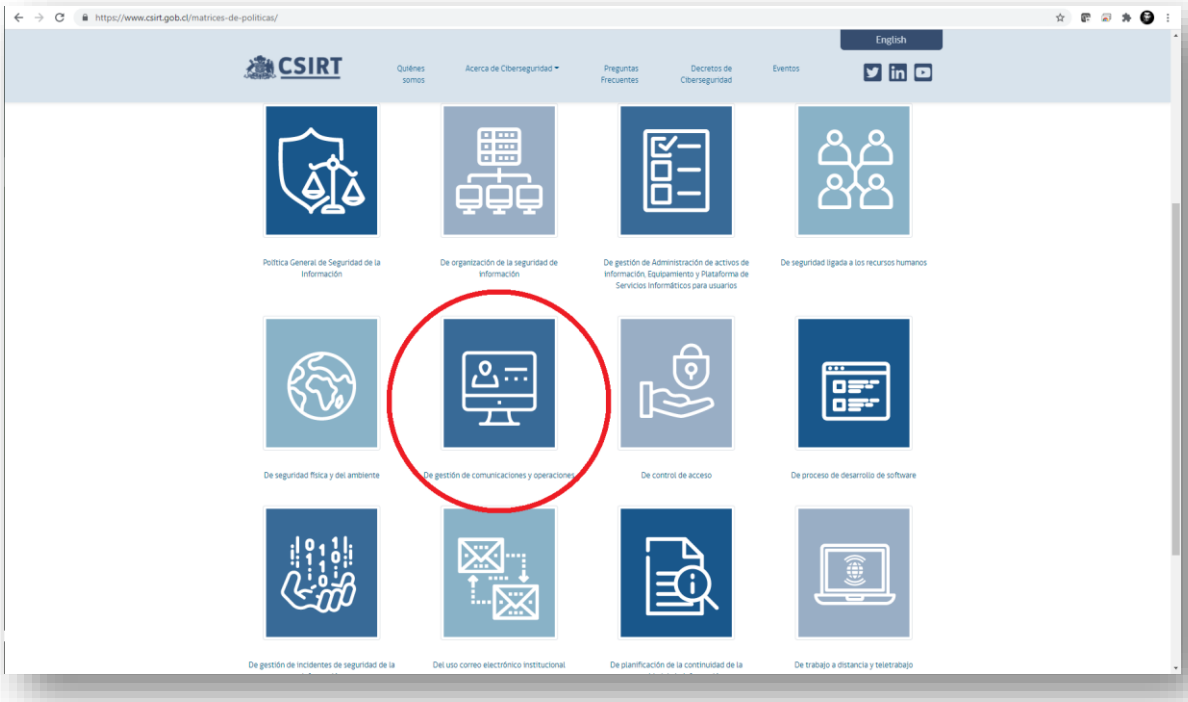
Por otra parte, la solución antimalware elegida por la institución debe cubrir activamente el 100% del parque de estaciones de trabajo y servidores, con las librerías y definiciones actualizadas en forma periódica.

En el caso que la institución, por razones de negocio posee equipos o soluciones *legacy*, que se encuentran bajo obsolescencia tecnológica, en los cuales no puede instalar o dejar activo la solución de *AntiMalware*, entonces la Institución deberá tomar medidas adicionales de protección, tales como dejar esta plataforma en redes aisladas del resto de la plataforma de la Institución, cerrar puertos, entre otras medidas. Si este tipo de soluciones es adoptado por la Institución, deberá contar con la autorización formal del encargado de Ciberseguridad o de Seguridad de la Información en conjunto con el Jefe de Servicio.

Con respecto al acceso a Internet de los usuarios, deberá contar con las protecciones adecuadas para la detección de malware durante la navegación y con la posibilidad de bloquear sitios web de carácter sospechoso.

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[9].

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



En estas políticas se contemplan las siguientes directrices que debieran ser consideradas como un mínimo en sus cuerpos normativos institucionales:

La aparición constante de nuevos virus y otros tipos de malware o código malicioso es una de las principales amenazas a las que se enfrentan hoy en día los sistemas de las empresas.
Las vías de contagio por malware son numerosas, destacando entre otras:

- las descargas de ficheros de todo tipo, adjuntos en correos o desde páginas web;
- la navegación por webs de dudosa fiabilidad;
- y la utilización de dispositivos ajenos, por ejemplo, pendrives.

El enorme daño que pueden causar a la empresa hace obligatorio el establecimiento de una política de control de malware. De este modo se podrá prevenir, detectar, controlar y eliminar la ejecución de cualquier software malicioso en los sistemas.

La Unidad TIC, implementará controles para prevenir y detectar código malicioso, lo cual se basa en software, concientización de usuarios y gestión del cambio. Los controles contemplan las siguientes directrices:

- Impedir el uso de software no autorizado.
- Impedir el compartir carpetas en los computadores y/o dispositivos personales.

- Implementar acciones y procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar en procedimientos de soporte a usuarios.
- Instalar y actualizar software de detección y reparación de virus, IPS de host, anti- spyware examinado computadores y medios informáticos, como medida preventiva y rutinaria.
- Mantener los sistemas con las últimas actualizaciones de seguridad disponibles, previa realización de pruebas en un ambiente dispuesto para tal fin.
- Chequear periódicamente el contenido de software y datos de los equipos de procesamiento, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
- Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
- Informar al personal acerca del problema de los falsos virus y de cómo proceder frente a los mismos.

Los aspectos estratégicos para el éxito de esta tarea son:

Determinar qué tipo de soluciones serán las más convenientes para la empresa. Dependiendo del tamaño, del nivel de seguridad necesario y de la complejidad de las configuraciones para la protección de los activos de información, se podrá determinar distintos tipos de soluciones:

- herramientas para el puesto de trabajo, el portátil o los dispositivos móviles,

- soluciones globales corporativas entre ellas:
    - UTM o gestión unificada de amenazas;
    - servicios gestionados que nos pueden facilitar loss proveedores de servicios de internet (ISP) u otros proveedores desde un centro de operaciones de seguridad o SOC;
    - soluciones de seguridad ofrecidas como servicios en la nube que monitorizan los equipos de forma remota.

Para el tipo de solución elegida, se seleccionará la más apropiada de entre las disponibles en el mercado buscando la compatibilidad con las infraestructuras y la versatilidad (antimalware, antiphishing, antispam, análisis de web y correo entre otros) de la herramienta.

Configurar las herramientas de detección de malware. Para un uso eficiente de las herramientas de control de malware se deberá realizar una correcta configuración de todas sus funcionalidades. La configuración deberá permitirnos, entre otros, establecer los siguientes controles:

- realizar análisis automáticos y periódicos para detectar malware;
- realizar comprobaciones automáticas de los ficheros adjuntos al correo y de las descargas web, ya que pueden contener código malicioso ejecutable;
- bloquear el acceso a ciertas aplicaciones o sitios web basándonos en una política de listas negras;
- permitir el acceso a ciertas aplicaciones o sitios web basándonos en una política de listas blancas;
- permitir el análisis de páginas web para detectar posibles amenazas incluidas en las mismas.

Actualizar las herramientas de detección de malware. Se deberá determinar la periodicidad con la que las herramientas de detección de malware son actualizadas. Actualmente se crean miles de virus al día, por lo que las actualizaciones de la base de datos de firmas de virus deberían ser automáticas y tener una periodicidad como mínimo diaria. Por otro lado, y como cualquier otra aplicación crítica, tendremos que actualizar convenientemente el propio software antivirus y el sistema operativo del servidor que permite su funcionamiento.

Establecer el procedimiento de respuesta ante la infección por ejecución de malware. En primer lugar, se deberá determinar qué sucesos serán considerados como incidencias por ejecución de malware, analizando:

- el impacto del ataque;
- los activos que puedan estar comprometidos;
- la forma de recuperar los activos impactados;
- los canales adecuados de aviso y notificación.

Después se establecerán las responsabilidades y la operativa a seguir en cada caso:

- desinfección de archivos y documentos;
- eliminación de archivos y documentos;
- aviso a soporte técnico del fabricante;
- reinstalación de software afectado;
- desconexión y asilamiento del equipo afectado;
- y el registro formal del incidente.

Política general de buenas prácticas para el control de malware. Con el fin de reforzar las medidas establecidas para el control del malware es conveniente tener concienciado al personal en los siguientes aspectos:

- Se deben considerar todos los contenidos y las descargas como potencialmente inseguros hasta que no sean convenientemente analizados por una herramienta de detección de malware.
- Deben prohibirse las siguientes acciones:
    - Ejecutar archivos descargados de servidores externos, de soportes móviles no controlados o adjuntos a correos, sin haber sido previamente analizados.
    - Configurar el programa cliente de correo electrónico para la ejecución automática de contenido recibido por correo.
    - Alterar la configuración de seguridad establecida para los sistemas y equipos de tratamiento de información.
- Debe utilizarse únicamente el software permitido la empresa. Este además debe estar convenientemente actualizado y licenciado.
- Para evitar la recepción de spam se deben seguir las directrices incluidas en la política de correo electrónico.

Para enfrentar las auditorías internas considere establecer formalmente algunas evidencias que serán requeridas para validar el correcto cumplimiento de estas directrices:

- Documento Política de Protección contra *Malware*
- Estadísticas de cobertura de solución *AntiMalware*, incluyendo despliegue última definición o actualización, cantidad de infecciones y desinfecciones.
- Estadísticas de infecciones por correo electrónico, navegación, archivos infectados en dispositivos de almacenamiento removibles, etc.
- Acciones de remediación ante infecciones masivas.
- Revisión de reglas en dispositivos de protección *Antimalware*.
- Vigencia de licencias.
- Declaración de excepciones para sistemas *legacy*, con autorización explícita del Jefe de Servicio y del Encargado de Ciberseguridad o de Seguridad de la Información.

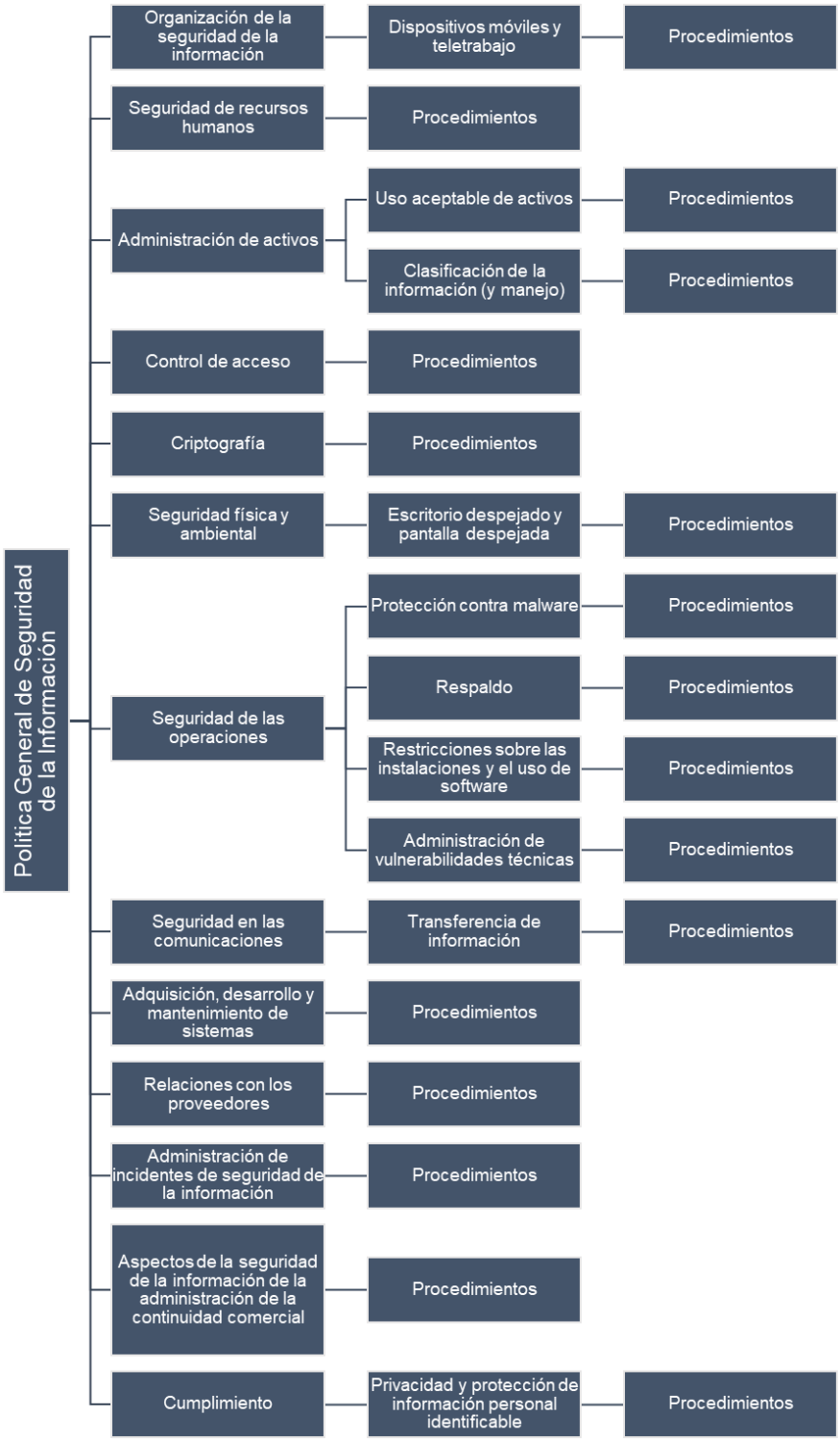
- Evidencia de acciones de sensibilización.

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[10] como en el CSIRT de Gobierno[11] (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.

Anexo I: Ejemplo de estructura de Políticas y Procedimientos

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


Politica General de Seguridad de la Información
Organización de la seguridad de la información
Dispositivos móviles y teletrabajo
Procedimientos
Seguridad de recursos humanos
Procedimientos
Administración de activos
Uso aceptable de activos
Procedimientos
Clasificación de la información (y manejo)
Procedimientos
Control de acceso
Procedimientos
Criptografía
Procedimientos
Seguridad física y ambiental
Escritorio despejado y pantalla despejada
Procedimientos
Seguridad de las operaciones
Protección contra malware
Procedimientos
Respaldo
Procedimientos
Restricciones sobre las instalaciones y el uso de software
Procedimientos
Administración de vulnerabilidades técnicas
Procedimientos
Seguridad en las comunicaciones
Transferencia de información
Procedimientos
Adquisición, desarrollo y mantenimiento de sistemas
Procedimientos
Relaciones con los proveedores
Procedimientos
Administración de incidentes de seguridad de la información
Procedimientos
Aspectos de la seguridad de la información de la administración de la continuidad comercial
Procedimientos
Cumplimiento
Privacidad y protección de información personal identificable
Procedimientos