7 de Septiembre de 2021
Ficha N° 11 A.12.3.1
CSIRT DE GOBIERNO

Ficha de Control Normativo A.12.3.1

Respaldo de la Información

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 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 ISA/IEC-62443[8] (estándar global de ciberseguridad para la automatización industrial).

[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. Respaldos o Backups

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 integrar uno de los controles más relevantes: el respaldo de la información.

La experiencia nos indica que si bien se pueden aplicar las mejores medidas preventivas y defensivas para evitar incidentes destructivos, éstos últimos en algún momento cruzaran nuestros perímetros defensivos y dañarán nuestros sistema o la información institucional.

Para este caso, contar con una adecuada estrategia de respaldo de la información relevante será un factor clave para una recuperación rápida y sin pérdida de información.

El respaldo de información es la copia de los datos importantes de un dispositivo primario en uno o varios dispositivos secundarios, ello para que en caso de que el primer dispositivo sufra una avería electromecánica o un error en su estructura lógica, sea posible contar con la mayor parte de la información necesaria para continuar con las actividades rutinarias y evitar la pérdida generalizada de datos.

Como dato curioso tenga en consideración que el 31 de marzo se celebra el Día Mundial del Respaldo (*backup*) como recordatorio de la importancia que tienen las copias de seguridad digitales, en el ecosistema digital de hoy en día.

¿Que puede llegar a ocasionar daño de sistemas e información institucional?

Algunos ejemplos pueden ser:

- Virus o malware. Aunque en general los códigos maliciosos, vinculados a Cibercrimen, hoy en día no tienen su foco en destruir los sistemas o su información, existen clases de éstos

que usan técnicas de cifrado que permiten sin sacar la información de un sistema, secuestrarla; estos son los llamados ransomware. En esta situación o bien se paga el rescate para recuperar los datos, o se logra obtener una llave de descifrado o bien recurrimos al valioso activo denominado “el respaldo”.

- Pueden ocurrir desastres naturales importantes que afecten a la infraestructura de nuestros sistemas y con ellos a la información.
- Pueden existir fallas de los equipamientos, dispositivos y componentes que sustentan a los sistemas y la información que almacenan.
- Pueden existir errores de configuración.
- Pueden existir fallas humanas.
- Pueden existir sabotajes perpetrados por actores internos o externos con fines diversos.
- Pueden existir modernizaciones de plataforma y por tanto es necesario migrar los datos, situación en la que a veces un respaldo facilita estos movimientos.

Al emprender la tarea de instaurar un sistema de respaldo se deben tener en consideración al menos las siguientes directivas:

Priorizar la eficiencia

El tiempo de restauración lento del archivo suele ser un signo revelador de la ineficiencia del respaldo como consecuencia de haber implementado una solución que no satisface las necesidades de la institución. Por lo tanto, es importante elaborar un plan detallado que contemple los sistemas, aplicaciones y datos que se integrarán con la solución de respaldo y que ayudarán a mejorar la eficiencia, la organización y, en última instancia, la productividad.

Ser predecible

El uso de procesos de respaldo consistentes y la realización de pruebas proporcionará la seguridad necesaria para evitar futuros problemas de recuperación de los datos. Tener procesos documentados que pueden repetirse reducirá el tiempo de respuesta, los costos de soporte, y minimizará los tiempos de inactividad. Aquí es importante seguir la regla del 3-2-1: tener, al menos, tres copias de

un conjunto de datos, almacenarlas en al menos dos medios diferentes, y que una de ellas esté ubicada en otro espacio físico.

Pensar en el respaldo como una práctica diaria

Hay que tener en cuenta que el respaldo no es únicamente tener copias de datos sino que su verdadero objetivo es la recuperación ante desastres. Si las copias de seguridad se realizan con regularidad, se reducirán tiempos de recuperación en caso de un incidente, ya que será más fácil localizar exactamente qué copia de seguridad tratará el incidente de pérdida de datos.

No asumir que se está seguro

A medida que las empresas migran cada vez más a los servicios en la nube, existe la suposición común de que los proveedores de SaaS como Google Drive y Office 365 tienen cobertura de respaldo. Sin embargo, aunque muchos proveedores están preparados para proteger los datos de sus clientes en la nube, no pueden ayudar cuando suceden hechos como ataques de ransomware, que cifran archivos, o si un empleado los elimina accidentalmente o maliciosamente.

Por eso es importante realizar una copia de seguridad de una segunda copia de los datos de la nube en local, lo que facilitará la restauración de los datos.

Proteger al Sistema de Respaldo con su propio castillo

El sistema que genera y gestiona los respaldos debe estar accesible, para prestar sus servicios de la manera más eficiente posible y alcanzar desde su punto central a todos los componentes que está respaldando su información. En este punto vale la pena recordar que el sistema de respaldo también es un sistema que puede ser atacado por código malicioso o ransomware, y sería un desastre mayúsculo si los datos o sistemas son afectados por un ransomware y al mismo tiempo el sistema de respaldo es también contaminado con este código malicioso: datos y respaldo terminarían cifrados, haciendo prácticamente imposible la recuperación de éstos. Por esta razón el sistema de respaldo debe estar en su propio castillo de seguridad y las

comunicaciones entre el sistema de respaldo con las unidades a respaldar debe ser protegidas y reducidas a las estrictamente necesarias.

Mantenerse actualizado

Aunque el respaldo no es algo nuevo, las tecnologías avanzan rápidamente siendo más fáciles de utilizar, más rápidas y menos costosas. Un claro ejemplo son las soluciones de "respaldo en la nube", que se están convirtiendo en una forma rentable de almacenar copias de datos fuera de su ubicación y reducir los requisitos de almacenamiento local.

Estar siempre preparado para lo peor

Aunque es inherente a la naturaleza humana esperar lo mejor, en un contexto empresarial, lo más inteligente es tener siempre un plan de contingencia para lo peor. Las instituciones deben operar siempre con la suposición de que sus datos están bajo constante amenaza, porque así es. Ya sea por un fallo de hardware, un error humano, una violación de datos, un ataque de ransomware o un desastre natural. Disponer de un plan respaldado por las soluciones tecnológicas, los conocimientos y los procesos adecuados garantizará que, en caso de crisis, se puedan recuperar los datos rápidamente evitando la discontinuidad de negocio

Contemplar todo tipo de amenazas

La amenaza más popular hoy en día son los ataques de ransomware donde la última defensa de las instituciones es poder recuperar los datos que han sido cifrados desde una copia de seguridad. Pero no hay que olvidar que los errores humanos o los fallos de hardware siguen produciéndose y son los principales motivos de recuperación de datos en las instituciones en el día a día.

La importancia del RPO[9] y RTO[10]

Algunas organizaciones olvidan que el objetivo principal de la protección de datos es la capacidad de recuperación. Cuando se implanta un sistema de respaldo, hay que centrarse no

[9] El RPO define la frecuencia con la que se necesitan hacer copias de seguridad.
[10] El RTO indica la rapidez con la que necesita recuperarse de un tiempo de inactividad.

sólo en la eficiencia y el costo de la copia de seguridad, sino en los tiempos y las métricas que son importantes para el proceso de recuperación. El objetivo de punto de recuperación y el objetivo de tiempo de recuperación son las dos métricas más importantes que deberían estar siempre presentes en los acuerdos de nivel de servicio entre los departamentos de TI y de negocio.

Aumento de la complejidad en el entorno de TI

Durante este último tiempo, se han visto varias tendencias en los entornos de TI de las instituciones, que han añadido complejidad a los mismos y que generan nuevos retos.

El efecto de la dispersión de los datos

Esta complejidad en el entorno también ha generado una dispersión de los datos, que, a su vez, multiplica los factores de amenaza. Por ello, es fundamental contar con una solución que no sólo proteja los datos, sino que también los recupere rápidamente en caso de necesidad, que se ajuste a la criticidad de la aplicación y los datos, al tiempo que reduzca el costo para la institución, así como la simplicidad de las operaciones.

Despega la demanda del respaldo como servicio

Las soluciones de *Backup-as-a-Service* se están popularizando por varias razones: ofrecen una óptima experiencia de usuario, con un entorno amigable, sencillo y sin fisuras. Además, el tiempo de despliegue y adopción es mínimo, y no requieren que se dedique ningún recurso al mantenimiento, gestión y custodia de sus activos. Por otro lado, ofrecen previsibilidad y reducción de costos, ya que se paga sólo por lo que se consume y no hay costos adicionales de activos sobredimensionados y ociosos. Al mismo tiempo, ofrecen fiabilidad y flexibilidad para desplegar nuevos servicios de respaldo de forma transparente, incluso con múltiples proveedores de nube. Por último, aprovechan las tecnologías de la nube para mejorar la seguridad.

¿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.

Ransomware

El malware de rescate, o ransomware, es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos.

Gusanos

También conocidos como Worms tienen como peculiaridad replicarse a sí 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; 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. El sistema de respaldo de información es uno de los componentes críticos en la respuesta a estos incidentes.

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

III. RECOMENDACIONES Y MEJORES PRÁCTICAS ASOCIADAS AL CONTROL

El control: Respaldo de Información

Se deben hacer copias de respaldo y pruebas de la información, del software y de las imágenes del sistema con regularidad, de acuerdo con la política de respaldo acordada.

Recomendaciones generales

Se debería establecer una política de respaldo para definir los requisitos de la organización para el respaldo de información, del software y de los sistemas.

La política de respaldo debería definir los requisitos de retención y protección.

Se debería contar con instalaciones de respaldo adecuadas para garantizar que toda la información y el software esencial se pueden recuperar después de un desastre y ante una falla de los medios.

Al asignar un plan de respaldo, se deberían considerar los siguientes elementos:

a) se deberían producir registros precisos y completos de las copias de respaldo y procedimientos de restauración documentados;

b) el nivel (es decir, respaldo completo o diferencial) y la frecuencia de los respaldos debería reflejar los requisitos del negocio de la organización, los requisitos de seguridad de la información involucrada y la criticidad de la información para la operación continua de la organización;

c) los respaldos se deberían almacenar en una ubicación remota, a una distancia suficiente para evitar cualquier daño ante desastres en la ubicación principal;

d) la información de respaldo debería tener un nivel de protección física y ambiental adecuada (ver cláusula 11) de acuerdo con las normas que se aplican en la ubicación principal;

e) los medios de respaldo se deberían probar de manera regular para garantizar que se puede confiar en ellos frente a su uso ante emergencias; esto se debería combinar con una prueba de los procedimientos de restauración y se debería comprobar contra la restauración según sea necesario; esto se debería combinar con una prueba de los procedimientos de restauración y se debería verificar contra el tiempo de restauración necesario. Se deberían realizar pruebas para probar la habilidad de restaurar los datos de respaldo en los medios de prueba, no sobrescribiendo los medios originales en caso de que falle el proceso de respaldo o restauración y provoque daños o pérdidas de los datos;

f) en las situaciones donde la confidencialidad es importante, se deberían proteger los respaldos mediante el cifrado.

Los procedimientos operacionales deberían monitorear la ejecución de respaldos y abordar las fallas de los respaldos programados para garantizar su integridad de acuerdo con la política de respaldos.

Se deberían probar regularmente las disposiciones de respaldos para los sistemas individuales a modo de garantizar que cumplen con los requisitos de los planes de continuidad del negocio. En el caso de los sistemas y servicios críticos, las disposiciones de respaldo deberían abarcar la información de todos los sistemas, aplicaciones y datos necesarios para recuperar al sistema completo en el caso de un desastre.

Se debería determinar el período de retención de la información esencial del negocio, considerando cualquier tipo de requisito para archivar copias que se deberían retener de manera permanente.

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/

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

La Unidad TIC, junto con los propietarios de los activos de información, determinará los requerimientos de respaldo, según su nivel de criticidad, nivel de riesgo, asegurando la confidencialidad, integridad y disponibilidad de la información.

Los respaldos son gestionados y administrados por la [Unidad TIC], cuidando el equilibrio de recursos tecnológicos y económicos disponibles, así como la clasificación de confidencialidad, integridad y disponibilidad de la información involucrada.

Metodología de Respaldo
El procedimiento de respaldo de la información incluye actividades de prueba de recuperación de la información. Las instalaciones de resguardo garantizarán las condiciones de seguridad ambientales necesarias para la conservación de los respaldos. El procedimiento de respaldo de la información contempla las siguientes directrices:

- Disponer un esquema de rótulo de las copias de respaldo, para permitir su fácil identificación.
- Destruir las copias de respaldo, cuando expire la vida útil de los medios de almacenamiento, de acuerdo con el procedimiento de destrucción o reutilización segura de equipos.
- Almacenar las copias de respaldo en un lugar fuera de las instalaciones del sitio de origen de la información, manteniendo un registro exacto y completo de cada una de ellas, así como de los procedimientos de restauración aplicados.
- Almacenar las copias de respaldo en condiciones de seguridad y ambientales adecuadas, consistentes a las aplicadas al sitio principal.
- Probar periódicamente la restauración de los medios de respaldo.
- La información de LOG's de auditoría, de seguridad y de los sistemas se mantendrá con una historia de por lo menos 1 año.

Consideraciones especiales para uso de almacenamiento en la nube

Algunas razones para almacenar información de la empresa en la nube son:

- acceder a la información desde cualquier dispositivo y lugar;
- ahorro de recursos y ahorro económico;
- proporciona directorios compartidos con distintos permisos de acceso;
- y permite el trabajo colaborativo sobre un documento.

Antes de proceder a su implantación en la empresa deben valorarse los aspectos negativos como la dependencia de terceros o la necesidad de conexión a internet para tener acceso a la información.

Para que el personal haga un buen uso de los recursos de almacenamiento, la empresa dispone de una Política de clasificación de la información, donde se indica qué tipo de información puede subirse a la nube.

Junto a esta clasificación se elabora una normativa interna para el tratamiento de la información crítica y sensible, que indica cuándo debe ir cifrada y otras medidas de seguridad que le aplican como respaldos o borrado seguro de la información.

Los puntos clave a tener en consideración sobre el uso de almacenamiento en la nube:
Uso de servicios de almacenamiento en la nube públicas. La empresa debe decidir si está permitido el uso de servicios de almacenamiento nube pública. El personal no podrá utilizar este tipo de repositorios si así lo contempla la normativa de la empresa.

Lista de servicios de almacenamiento en la nube permitidos. La empresa dispone de una lista de los servicios de almacenamiento en la nube permitidos y prohibidos. De esta forma se evita el uso de servicios de almacenamiento que son considerados como no seguros.

Proceso de borrado de la información. Se aplicará una Política de borrado de la información que también se debe aplicar cuando se elimina información almacenada en la información en la nube.
Tipo de información almacenada. El personal debe conocer qué tipo de información puede almacenarse en la nube (y cual no) y en qué casos tendrá que almacenarse cifrada. La política de clasificación de la información incluye este dato.

Copias de seguridad en la nube. El personal tendrá presente las ventajas e inconvenientes de realizar copias de seguridad en la nube antes de realizarlas.

- Ventajas:
    - Disponer de más espacio para realizar la copia de seguridad a medida que lo necesitemos.
    - La mayoría de los servicios en la nube realiza copias de seguridad como garantía de disponibilidad.
    - Disponer de una copia fuera de las dependencias de la empresa. En caso de que se produjera un incidente, nuestra información no se vería afectada y podríamos recuperarla.
- Inconvenientes:
    - Depender de terceros que tendrán sus riesgos propios que pueden quedar fuera de nuestro control.

Contratación de servicios de almacenamiento en la nube. Al contratar un servicio de almacenamiento en la nube, la empresa se asegurará que cumple con los criterios de seguridad específicos que precisa la información que se va a almacenar en la nube (garantía de confidencialidad, disponibilidad de la información, copias de seguridad, información de auditoría, etc.), así como con las necesidades legales si se trataran de datos personales.

- Política de seguridad del proveedor. Antes de contratar servicios en la nube que traten información de la empresa, Confidencial e Interna o de datos personales, se debe leer y comprender la política de seguridad del proveedor de servicios para asegurar que cumple todas las necesidades de la empresa y legislación vigente sobre la materia.

La institución debe contar con políticas adecuadas de respaldo de información, no solo para los servidores y sistemas institucionales, sino que debe agregarse todo aquel dispositivo de carácter crítico (dispositivos de comunicaciones, dispositivos de seguridad) y aquellas estaciones de trabajo que tengan el carácter de suma importancia por la información que en ellas se encuentra o si se procesa información estratégica de la institución.

Se debe formular un calendario de respaldo y retención, según lo que defina la institución y que sea adecuado para sus necesidades de negocio.

Una copia de los respaldos, deben ser almacenados en lugares distintos al que es utilizado para el procesamiento de información (sitio alternativo), para asegurar su disponibilidad en el caso de que el sitio principal no esté disponible.

Se deben hacer pruebas periódicas de restauración de la información contenida en los respaldos y se debe agregar pruebas de validación de datos, esto para asegurarse de que el respaldo servirá en situaciones de contingencia.

Algunas evidencias requeridas para validar cumplimiento:

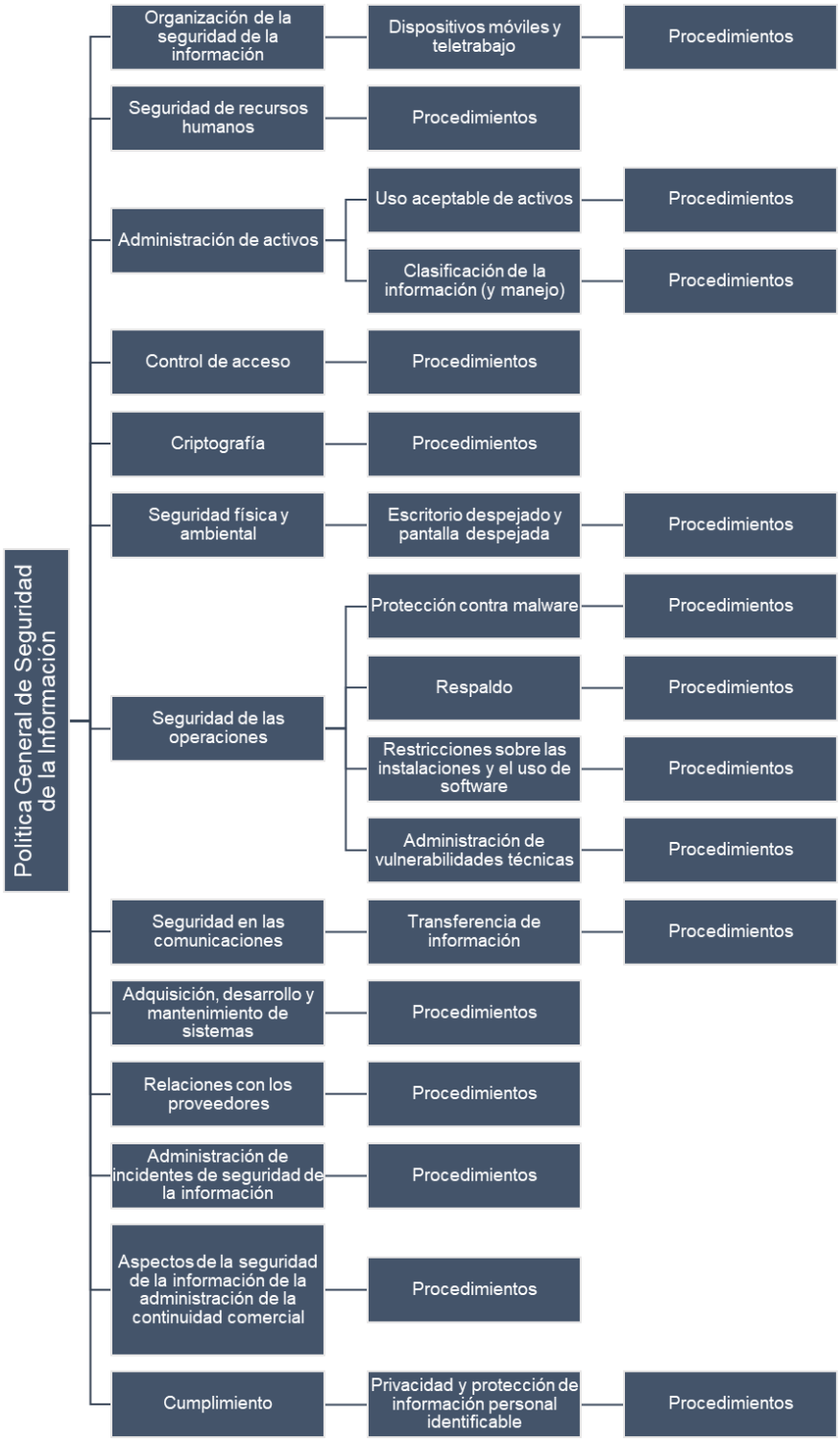
- Documento Política de Respaldo.
- Evidencias de restauraciones de respaldos y de validación de la información.
- Evidencias de envío/retiro de medios de respaldo desde el sitio alternativo de almacenamiento.
- Procedimiento de destrucción de medios de respaldo, cuando se dan de baja.

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.

Anexo I: Ejemplo de estructura de Políticas y Procedimientos

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