12 de Octubre de 2021
Ficha N° 16 A.12.6.1
CSIRT DE GOBIERNO

Ficha de Control Normativo A.12.6.1

Gestión de las vulnerabilidades técnicas

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 Nch-ISO/IEC 27010.
- La norma ISA/IEC-62443[8] (estándar global de ciberseguridad para la automatización industrial).
- 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. Vulnerabilidades

Este control requiere manejar algunos términos relevantes, cuyo conocimiento es crucial para poder articular las actividades relativas a la implementación de este control y de sus interrelaciones con otros controles.

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.

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.

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.

Análisis de vulnerabilidades

Consiste en la búsqueda y documentación de fallos, carencias o debilidades físicas (inundaciones, incendios, controles de acceso…) y lógicas (configuraciones, actualizaciones…) en un sistema informático, que puedan ser empleados por terceros con fines ilícitos, suponiendo un riesgo para la

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

organización y los propios sistemas. El análisis propone vías de mitigación a implementar para subsanar las deficiencias encontradas y evitar ataques a los sistemas informáticos.

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.

Escaneo de puertos

Técnica intrusiva en la que los atacantes buscan de manera activa los puertos y servicios que pudieran estar a la escucha, en busca de recopilar infrormación de la víctima con la finalidad de intentar encontrar vulnerabilidades que explotar en la fase de ataque. Este tipo de técnica también es denominada fingerprinting.

Escaneo de vulnerabilidades

Actividad en la que se buscan vulnerabilidades en redes y sistemas, mediante diferentes técnicas y aplicaciones especializadas, con el fin de identificarlas y subsanarlas para evitar que sean utilizadas por los ciberdelincuentes en su beneficio. El escaneo se centra en las aplicaciones, puertos y servicios desplegados en una empresa.

Puerto

Es una interfaz o «puerta» a través de la cual se pueden enviar y recibir datos. Existen dos tipos de puertos: los físicos, que serían los conectores de un equipo que permiten la comunicación entre dispositivos, y que a su vez se dividen en varios tipos según el conector y su función; y los lógicos, generalmente implementados por software, que son aquellos que permiten la comunicación entre dos máquinas en una red, mediante áreas de memoria reservadas en un sistema. Los puertos lógicos están limitados a 65536 al tratarse de números de 16 bits, que son manejados por las máquinas para establecer las comunicaciones. Los puertos son el principal objetivo de un ciberatacante para identificar posibles vías de entrada a un sistema.

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.

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.

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

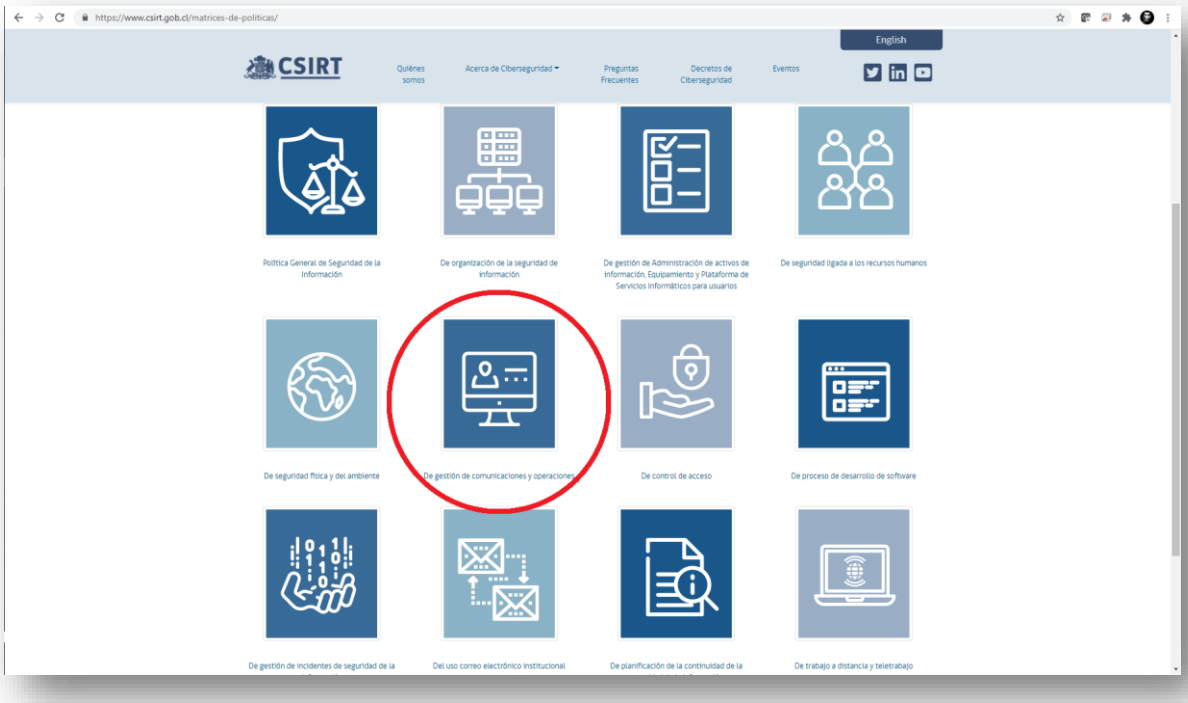
El control: Gestión de las vulnerabilidades técnicas

Se debe obtener la información acerca de las vulnerabilidades técnicas de los sistemas de información usados, se debe obtener de manera oportuna, evaluar la exposición de la organización a estas vulnerabilidades y se deben tomar medidas apropiadas para abordar el riesgo asociado.

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 implementar y utilizar los software operacionales de manera segura.

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 principio es relevante destacar que un inventario de activos actual y completo (ver cláusula 8 de la norma Nch-ISO-27002) es un prerrequisito para la administración eficaz de vulnerabilidades técnicas. La información específica necesaria para apoyar la administración de vulnerabilidades técnicas incluye al proveedor de software, los números de versiones, el estado actual de la implementación (es decir, qué software se instala en qué sistemas) y las personas responsables del software dentro de la organización.

Se deben tomar medidas adecuadas y oportunas en respuesta a la identificación de las posibles vulnerabilidades técnicas. Se deberían seguir los próximos puntos de orientación para establecer un proceso de administración eficaz para las vulnerabilidades técnicas:

a) la organización debería definir y establecer los roles y las responsabilidades asociadas a la administración de vulnerabilidades técnicas, incluido el monitoreo de vulnerabilidades, la evaluación de riesgos de vulnerabilidad, los parches, el seguimiento de activos y cualquier tipo de responsabilidades de coordinación necesarias;

b) se deberían identificar los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas pertinentes y para mantener la concientización sobre ellas para el software y otras tecnologías (en base a la lista de inventario de activos, ver 8.1.1 de la norma Nch-ISO-27002); estos recursos de información se deberían actualizar en base a los cambios en el inventario o cuando se encuentran nuevos recursos útiles;

c) se debería definir una línea de tiempo para reaccionar frente a las notificaciones de vulnerabilidades técnicas posiblemente relevantes;

d) una vez que se ha identificado una vulnerabilidad técnica, la organización debería identificar los riesgos asociados y las medidas que se deberían tomar, dichas medidas podrían involucrar la aplicación de parches a los sistemas vulnerables o la aplicación de otros controles;

e) en función de la urgencia con la que se deba abordar una vulnerabilidad técnica, la medida tomada se debería realizar de acuerdo a los controles relacionados con la administración de cambios (ver 12.1.2 de la norma Nch-ISO-27002) o siguiendo los procedimientos de respuesta ante incidentes de seguridad (ver 16.1.5 de la norma Nch-ISO-27002);

f) si existe un parche disponible de una fuente legítima, se deberían evaluar los riesgos asociados a la instalación del parche (los riesgos que impone la vulnerabilidad se deberían comparar con el riesgo de instalar el parche);

g) los parches se pueden evaluar y probar antes de su instalación para garantizar que son eficaces y no involucran efectos colaterales que no se pueden tolerar; si no existen parches disponibles se deberían considerar otros controles como:

- desactivar todos los servicios o capacidades relacionadas a la vulnerabilidad;
- adaptar o agregar controles de acceso, es decir, firewalls, en las fronteras de la red (ver 13.1 de la norma Nch-ISO-27002);
- mayor monitoreo para detectar ataques reales;
- concientizar sobre la vulnerabilidad;

g) se debería mantener un registro de auditoría para todos los procedimientos que se realizan;

h) el proceso de vulnerabilidad técnica se debería monitorear y evaluar regularmente para poder garantizar su efectividad y eficiencia;

i) se deberían abordar primero los sistemas en alto riesgo;

k) se debería alinear un proceso de administración de vulnerabilidades técnicas eficaz con actividades de administración de incidentes para comunicar los datos sobre vulnerabilidades con la función de respuesta ante incidentes y proporcionar los procedimientos técnicos en caso de que ocurra un incidente;

l) definir un procedimiento para abordar la situación donde se ha identificado una vulnerabilidad, pero donde no existe una contramedida. En esta situación, la organización debería evaluar los riesgos relacionados con la vulnerabilidad conocida y definir las medidas detectivas y correctivas adecuadas.

La institución debe preocuparse de mantener los sistemas tecnológicos conectados a la red actualizados, para ello, debe mantener actualizados, al menos a la última versión disponible y estable:

- Sistemas operativos
- Motores de Bases de Datos.
- Aplicaciones de Ofimática
- Navegadores de Internet
- Otros programas utilitarios.
- Librerías
- Software de Seguridad (antimalware; DLP, etc.).
- Cualquier otro programa instalado en servidores y estaciones de trabajo.

En forma adicional, la Institución deberá mantener actualizados otros elementos conectados a la red, tales como:

- Equipos de comunicaciones (red, Telefonía).
- Firmware de Impresoras.
- Soluciones y equipos de seguridad.
- Equipos de respaldo.
- Otros dispositivos necesarios para el desarrollo de las actividades de la Institución.

Deberá contar con un catastro de todos estos dispositivos, su sistema operativo o firmware instalado (incluyendo versión), versiones de aplicativos instalados, etc., incluyendo fecha de la última actualización instalada.

Además deberá contar con las evidencias de pruebas de las actualizaciones a instalar sobre la plataforma tecnológica de la institución, antes de la puesta en los ambientes productivos, para validar que estas no afecten al normal funcionamiento de los sistemas institucionales. Por tanto, deberá considerar la implementación de los procesos asociados a control de cambios sobre la plataforma tecnológica, incluyendo las aprobaciones respectivas.

También deberá negociar con los proveedores de tecnología, además del licenciamiento respectivo, contar con soporte de actualizaciones, sean estas del tipo estándar o extendido. Esto para asegurar que contará con todas la actualizaciones necesarias en lo referente a seguridad.

Las actividades relacionadas con actualizaciones deben ser registradas a través de los logs de auditoria de los sistemas.

Algunas recomendaciones para evidenciar su cumplimiento son:

- Listado de soluciones tecnológicas conectadas a la red, la cual incluya: versión de Sistema Operativo o Firmware, Versión de aplicativos instalado (ofimática, base de datos, librerías, software propietario, etc).
- Evidencia de instalación en producción de actualizaciones, incluyendo documentación de control de cambios.
- Informes de hardening de sus servidores.
- Informes de escaneo y análisis de vulnerabilidades de sus activos.

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