



14 de Julio de 2021

Ficha N° 3 A.7.2.2

CSIRT DE GOBIERNO

Ficha de Control Normativo A.7.2.2

Concientización, educación y formación en seguridad 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 CAIGG¹.

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 / 2018², el Decreto Supremo N°83 / 2005³, el Decreto Supremo N°93 / 2006⁴, el Decreto Supremo N°1 de 2015⁵ y a la Nch-ISO IEC 27001⁶.

² <https://transparenciaactiva.presidencia.cl/instructivos/Instructivo-2018-008.pdf>

³ <https://www.bcn.cl/leychile/navegar?idNorma=234598>

⁴ <https://www.bcn.cl/leychile/navegar?idNorma=251713>

⁵ <https://www.bcn.cl/leychile/navegar?idNorma=1078308>

⁶ <https://ecommerce.inn.cl/nch-iso-iec-27001202078002>



II. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

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 de difusión y sensibilización sobre ciberseguridad de manera continua en el tiempo, que permita a los funcionarios acercarse e internalizar los conceptos para aplicarlos de manera transversal en su quehacer diario.

Un programa de concientización sobre seguridad de la información debería apuntar a hacer que los empleados y, donde resulte pertinente, los contratistas conozcan sus responsabilidades en cuanto a la seguridad de la información y los medios a través de los que se descargan esas responsabilidades.

En este orden de ideas, un programa de concientización de seguridad de la información se debería establecer de acuerdo con las políticas y procedimientos pertinentes de seguridad de la información de la organización, considerando la información de la organización que se va a proteger y los controles que se han implementado para proteger la información. El programa de concientización debería incluir varias actividades de concientización como campañas (por ejemplo, un “día de la seguridad de la información”) y la entrega de infografía o boletines informativos.

El programa de concientización se debería planificar considerando los roles de los empleados en la organización y, donde corresponda, la expectativa que tiene la organización sobre la concientización de los contratistas. Las actividades del programa de concientización se deberían programar con el tiempo, de preferencia de manera regular, para que las actividades se repitan y abarquen a los nuevos empleados y contratistas. El programa de concientización también se debería actualizar de manera regular para que esté de acuerdo con las políticas y procedimientos de la organización y se debería basar en las lecciones aprendidas de los incidentes de seguridad de la información.

Se debería realizar una capacitación de concientización según lo requiera el programa de concientización de





seguridad de la información de la organización. La capacitación de concientización se puede realizar a través de distintos medios incluida la capacitación en el aula, a distancia, en línea, autónoma y otros. Indudablemente atendiendo a las condiciones sanitarias presentes y futuras de mediano y largo plazo toman mucha relevancia las infografías didácticas, con mensajes claros y precisos y las instrucciones en línea, para temas más extensos, que se puedan entregar.

La educación y la capacitación de seguridad de la información deberían abarcar aspectos generales como:

- 🌈 indicar el compromiso de la dirección con la seguridad de la información en toda la organización;
- 🌈 la necesidad de conocer y cumplir con las normas y obligaciones de seguridad de la información pertinentes, según se define en las políticas, normas, leyes, normativas, contratos y acuerdos;
- 🌈 responsabilidad personal por las acciones e inoperancias propias y las responsabilidades generales hacia el aseguramiento y protección de la información que pertenece a la organización y a las partes externas.
- 🌈 procedimientos básicos de seguridad de la información (como la denuncia de incidentes de seguridad de la información) y controles de la línea de base (como seguridad de contraseñas, controles de malware y despeje de escritorios);
- 🌈 Puntos de contacto y recursos para la información adicional y asesoría sobre los asuntos de seguridad de la información, incluida una mayor información sobre la educación y los materiales de capacitación para la seguridad de la información.

La educación y la capacitación sobre la seguridad de la información se deben realizar de manera periódica.

La educación y la capacitación inicial se aplica a quienes se les traslada a nuevos cargos o roles con requisitos de seguridad de la información sustancialmente diferentes, no solo para quienes comienzan sus labores y, se debería realizar antes de que el rol se active.

La organización debería desarrollar el programa de educación y capacitación para poder realizar la educación y la capacitación de manera eficaz. El programa se debería establecer de acuerdo con las políticas y procedimientos pertinentes de seguridad de la información de la organización, considerando la información de la organización que se va a proteger y los controles que se han implementado para proteger la información. El programa debería considerar las distintas formas de educación y capacitación, es decir, charlas o estudio autónomo.

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



III. RECOMENDACIONES Y MEJORES PRÁCTICAS ASOCIADAS AL CONTROL

El control:

Todos los empleados de la organización y, en donde sea pertinente, los contratistas deben recibir información adecuada en concientización y actualizaciones regulares sobre las políticas y procedimientos organizacionales conforme sea relevante para su función laboral.

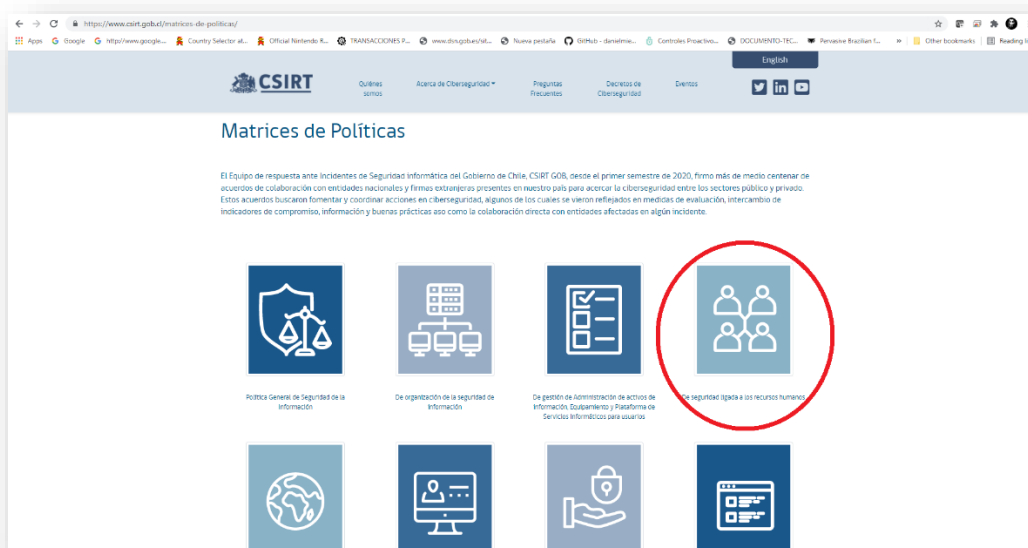
Recomendaciones generales

Se debe hacer capacitaciones formales de distintos aspectos de la seguridad de la información para todos los integrantes de la Institución y para el personal externo, ya sea temporal o permanente.

La institución debería incorporar además otras técnicas de difusión de las políticas de seguridad.

Toda capacitación formal y entrega de información sobre seguridad de la información se debe evidenciar y los registros de participación deben ser resguardados.








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 enlace⁷.



⁷ <https://www.csirt.gob.cl/matrices-de-politicas/>



Algunas evidencias requeridas para validar cumplimiento




-  Listados de participación en sesiones de capacitación formal respecto a la seguridad de la información.
-  Copias de distribuciones masivas o sectorializadas de infografías.
-  Desarrollos de materiales didácticos publicados en la intranet institucional.
-  Material creativo complementario: podcast, juegos, literatura asociada, cuentos y poesías para vincular y acercar la ciberseguridad.
-  Copias de material entregado.
-  Campañas informativas sobre temas de ciberseguridad contingente.
-  Plan de capacitación de Seguridad de la Información.

Responsable del Control





Recursos Humanos. Encargado de Ciberseguridad y/o Seguridad de la Información.

Recomendaciones específicas

Se sugiere que se evalúen caso a caso al menos las siguientes fuentes de información ya disponibles con campañas e infografías que genera el CSIRT⁸:

-  Revistas CIBER SUSESO
-  Ciber consejos
-  Ciber Guías

Difusión de acceso a RRSS del CSIRT:

-  <https://twitter.com/CSIRTOGOB>
-  <https://twitter.com/CSIRTConciencia>
-  <https://www.linkedin.com/in/csirt-gobierno-18584817b/>
-  <https://www.youtube.com/channel/UCua0E5Jz9V1Rn-VtLHPP4Nw/>



⁸ <https://www.csirt.gob.cl/recomendaciones/>



Al comprometerse en un programa de concientización, es importante no solo centrarse en el “qué” y en el “cómo”, sino que también en el “por qué”. Es importante que los empleados entiendan el objetivo de la seguridad de la información y el posible impacto, ya sea positivo y negativo, en la organización y en su propio comportamiento.

La concientización, la educación y la capacitación pueden ser parte de o realizarse en colaboración con otras actividades de capacitación, por ejemplo, un programa general de TI o de seguridad general. Las actividades de concientización, la educación y la capacitación deberían ser adecuadas y pertinentes para los roles, las responsabilidades y las habilidades de las personas.

Se puede realizar una evaluación del conocimiento de los empleados al final de un curso de concientización, educación y capacitación para probar la transferencia de conocimiento.

Si tiene alguna necesidad específica no dude en contactar al Equipo de Comunicaciones del CSIRT para averiguar si existe materia sobre algún tema específico de ciberseguridad, si existe lo guiarán para que pueda acceder a él y distribuirlo en su institución o bien si existe la disponibilidad de recursos se podría desarrollar y disponibilizar para la comunidad.

Estudie las múltiples opciones y recomendaciones para avanzar en la implementación de este control y 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 Digital⁹ como en el CSIRT de Gobierno¹⁰ (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.

⁹ <https://digital.gob.cl/>

¹⁰ <https://www.csirt.gob.cl/>



Anexo I: Ejemplo de estructura de Políticas y Procedimientos

