24 de Agosto de 2021
Ficha N° 9 A.11.1.4
CSIRT DE GOBIERNO

Ficha de Control Normativo A.11.1.4

Protección contra amenazas externas y del ambiente

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] y a la Nch-ISO IEC 27001[7].

[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

II. PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y DEL AMBIENTE

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 Física y del Ambiente, que permita a los funcionarios acercarse e internalizar los conceptos para aplicarlos de manera transversal en su quehacer diario.

Esta directiva de Seguridad Física y del Ambiente se orienta a definir medidas de protección para toda la infraestructura de la empresa ya sea tecnológica o no, en particular contra las amenazas externas y del ambiente. Se deben tener en consideración aquellas amenazas físicas y del ambiente que pueden afectar a las plataformas tecnológicas y las instalaciones en general, pero con foco en la seguridad de las personas y las instalaciones de procesamiento de la información, ya sea en los centros de procesamientos de datos (CPD) o en los equipos bajo la cobertura de los usuarios. Se han de mencionar como principales amenazas objetivo, sin que sea una lista exhaustiva, pero que ilustre el amplio espectro de situaciones a tener en consideración, a la siguiente:

- daño físico por acción del fuego
- daño físico por acción del agua
- daño físico por acción de la contaminación
- daño físico por acción de incidente tangible importante
- destrucción de equipamiento o medios
- daño físico por acción del polvo
- la corrosión o el congelamiento
- daños por acciones terroristas o vandálicas o disturbios
- daños por acción de eventos naturales tales como: fenómenos climáticos, fenómenos sísmicos, fenómenos volcánicos, fenómenos meteorológicos, inundaciones

- otras formas de desastres naturales
- daños provocados por el hombre

Para esto se ha de aplicar una estrategia de seguridad basada en las mejores prácticas y controles sobre estos recursos con el fin de protegerlos de accesos no autorizados, de daños a la integridad, de impactos relevantes en su disponibilidad, y finalmente garantizar su operación y seguridad. En específico, se buscará:

- Velar por la protección de la Infraestructura tecnológica de almacenamiento de información y de provisión de servicios tecnológicos de apoyo a la gestión institucional.
- Protección de los espacios Físicos.
- Dar condiciones de continuidad operacional a la gestión institucional en el contexto del cumplimiento de los requisitos normativos, estatutarios, reglamentarios y contractuales, que están orientados hacia la seguridad de la información.

Es importante que se profundice y especifique el alcance que esta política ha de tener en la institución. Se sugiere analizar la siguiente estructura de alcance a considerar dentro de sus directrices propias:

Esta política se aplica a todos los trabajadores y terceras partes que tengan o no una relación directa o indirecta de acceso a la información que pueda afectar los activos de información de la Institución. También se aplica a cualquiera de sus relaciones con terceros que impliquen el acceso a sus datos, utilización de sus recursos o a la administración y control de sus sistemas de información. Esta política rige independientemente del lugar en el trabajador presta sus servicios a la organización, total o parcialmente, e indistintamente de la modalidad de trabajo ya sea “presencial”, “a distancia”, “teletrabajo” u otra, en las condiciones que establezca la legislación vigente, los planteamientos de la Dirección del Trabajo o los Estados de Excepción Constitucional decretados por el Presidente de la República. Esta política gobierna la seguridad de la información de todos los procesos estratégicos de la Institución, establecidos en el documento institucional denominado Definiciones Estratégicas o equivalente, cubriendo a toda la organización independiente de su ubicación geográfica en el país (Chile Continental, Chile Insular o la Antártica Chilena).

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

III. RECOMENDACIONES Y MEJORES PRÁCTICAS ASOCIADAS AL CONTROL

El control:

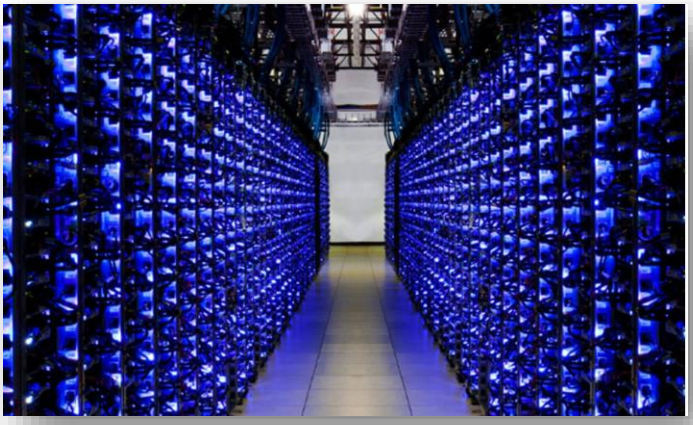
Se debe diseñar y aplicar la protección física contra daños por desastre natural, ataque malicioso o accidentes.

Recomendaciones generales

Se debe obtener asesoría de especialistas sobre cómo evitar los daños provocados por incendios, inundaciones, terremotos, explosiones, disturbios y otras formas de desastres naturales o provocados por el hombre.

La institución debe evaluar la ubicación de nuevos centros de tratamiento y almacenaje de información, para evitar daños de inundación por cañerías o por desastres naturales; de humedad, para los casos de almacenaje; de daños por vandalismo, al quedar expuestos o cercanos a entradas a edificios o en niveles cercanos a la entrada; entre otros aspectos.

Para las actuales instalaciones donde se manipula, explota y almacena información relevante de la institución, se deben implementar soluciones que permitan mitigar los efectos de daños producidos por desastres naturales, fallas de infraestructura o por vandalismo.



Complementariamente se deberán considerar e implementar donde corresponda para los perímetros de seguridad físicos las siguientes pautas:

a) se deberían definir perímetros de seguridad y el emplazamiento y la ubicación de cada uno de los perímetros debería depender de los requisitos de seguridad de los activos dentro del perímetro y los resultados de una evaluación de riesgos;

b) los perímetros del edificio o del sitio donde se albergan las instalaciones de procesamiento de información deberían ser físicamente sólidos (es decir, no deberían haber brechas en el perímetro o en las áreas donde se podría generar un agrietamiento fácilmente); el techo exterior, las paredes y el piso del sitio deberían ser de construcción sólida y todas las puertas externas deberían estar protegidas adecuadamente contra el acceso no autorizado con mecanismos de control, (es decir, barras, alarmas, candados); las puertas y ventanas se deberían cerrar con llave correctamente, cuando se dejan sin vigilancia y se debería considerar una protección externa para las ventanas, en particular a nivel del suelo;

c) se debería contar con un área de recepción atendida por una persona u otros medios para controlar el acceso físico al sitio o al edificio; el acceso a los sitios y al edificio se debería restringir solo al personal autorizado;

d) se deberían construir barreras físicas donde corresponda para evitar el acceso físico no autorizado y la contaminación ambiental;

e) todas las puertas contra incendios en un perímetro de seguridad deberían tener una alarma, ser monitoreadas y probadas en conjunto con las paredes para establecer el nivel de resistencia necesario de acuerdo con las normas regionales, nacionales e internacionales correspondientes; deberían operar, de acuerdo con el código de incendios local y a prueba de fallos.

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[8].

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

La institución debe implementar sistemas de control de acceso físico a sus instalaciones.

Debe considerar controles de resguardo de las instalaciones u oficinas en las cuales se almacena información de carácter confidencial y/o estratégica para la Institución, por ejemplo: *Datacenter*, sala o racks de comunicaciones, área de Recursos Humanos, áreas de negocio donde se almacena información estratégica, entre otros.

En forma adicional debe contar con sistemas de registro a través de Circuito Cerrado de Televisión (CCTV) con retención mínima de un mes, además de sistemas de alarmas y de incendio.

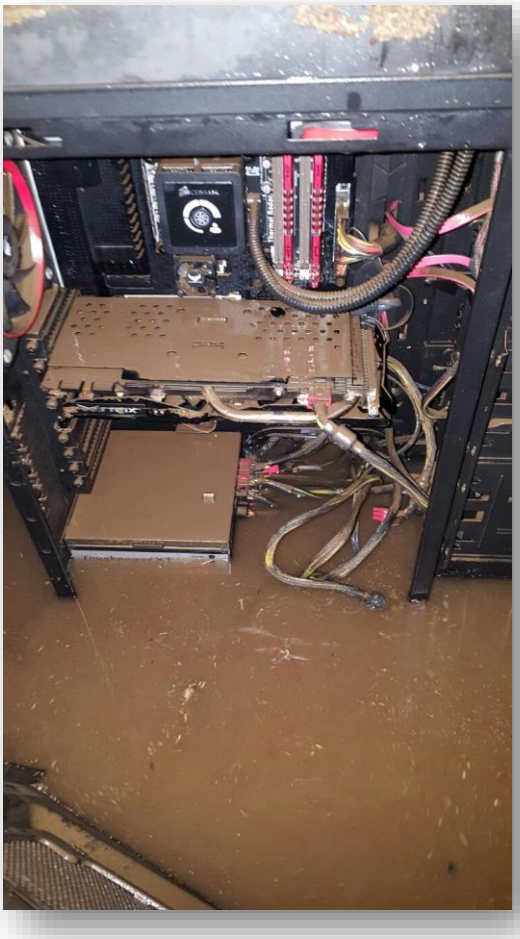
Para la aplicabilidad de este control, se suele trabajar en conjunto con los Prevencioncitas de Riesgos de la Mutual que atiende a la institución, con el objeto de desarrollar en conjunto los procedimientos de control de acceso físico, de evacuación y de detección.

Además se debe establecer protocolos respecto a la entrada y salida de dispositivos tecnológicos en las instalaciones, y en particular sobre aquellas ubicaciones en las que se procesa y almacena información estratégica y/o confidencial de la institución. El control en la entrada posibilita determinar que dispositivos personales o de terceros ingresaron a las oficinas e instalaciones, información que es útil en caso de existir un evento asociado a fuga de información. Por el contrario,

el control en la salida, es un buen disuasivo ante hurtos o robos de dispositivos móviles desde las instalaciones, (Notebooks, Teléfonos, *Tablets*, entre otros).

La Unidad TIC realizará el mayor esfuerzo en implementar y garantizar la efectividad de los mecanismos de seguridad física y control de acceso para proteger de las amenazas prioritarias y más probables, en base a una evaluación y priorización de riesgos, el perímetro de seguridad de los centros de procesamiento de datos (Salas Técnicas y CPD/*Datacenter*).

La [Unidad de Administración y Finanzas o unidad responsable por las instalaciones físicas] velará por la seguridad física de las áreas restringidas, áreas de funcionamiento del personal, áreas de carga y descarga, y en general de las instalaciones (*facilities*) así como entornos abiertos. Del mismo modo, establecerá controles contra potenciales amenazas físicas externas e internas y las condiciones medioambientales de las instalaciones de la empresa.



Para estas laboras, en cuanto a tecnología y respaldo técnico, deberá recurrir en primera instancia a la asesoría de la Unidad TIC, pudiendo recurrir a la asesoría externa solo si no están disponibles los recursos de apoyo internos.

La seguridad de instalaciones tendrá en cuenta los siguientes aspectos:

- Vías de acceso.
- Unidades de apoyo.
- Distribución interna.
- Sistema de prevención y extinción de incendios.
- Sistemas de vigilancia y control.
- Controles de acceso y perimetrales.
- Plan de emergencia.
- Seguridad externa/interna a las áreas de procesamiento y/o almacenamiento de información sensible, siempre que no se encuentre bajo la cobertura de la [Unidad TIC].
- Sistema abastecimiento continuo 7x24 de energía y combustibles.

- Continuidad operacional de los sistemas de climatización
- Sistema de estacionamientos y su monitoreo.
- Instalaciones en general (faclilities).
- Sistema de carga y descarga de productos.

En lo posible deberá establecer consideraciones respecto de:

- Áreas Seguras
- Seguridad de los equipos
- Servicios de Suministro de Energía
- Seguridad del Cableado
- Mantenimiento de los Equipos
- Seguridad de los equipos fuera de las instalaciones
- Destrucción o reutilización segura de equipos
- Recomendación de buenas prácticas para escritorio limpio y seguro
- Retiro de bienes de las instalaciones

El encargado deberá procurar la existencia de al menos los siguientes documentos para verificar su cumplimiento:

- Documento de evaluación de instalaciones de procesamiento de información.
- Política de control de acceso físico a las instalaciones.
- Plan anual de incorporación de soluciones de seguridad física.

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[9] como en el CSIRT de Gobierno[10] (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