22 de Junio de 2022
Ficha N° 20 A.14.1.2
CSIRT DE GOBIERNO

Ficha de Control Normativo A.14.1.2

Aseguramiento de servicios de aplicación en redes públicas

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	Repetible o Planificado	40%	Se planifica y se aprueba formalmente. Se programa la realización de actividades
3	Definido o Ejecutado	60%	Se ejecuta e implementa de acuerdo con lo aprobado y planificado

[1] https://www.auditoriainternadegobierno.gob.cl/wp-content/upLoads/2018/10/DOCUMENTO-TECNICO-N-107-MODELO-DE-MADUREZ.pdf

4	Gestionado o Verificado	80%	Se realiza seguimiento y medición de las acciones asociadas a la ejecución
5	Optimizado o Retroalimentado	100%	Se retroalimenta y se toman medidas para mejorar el desempeño

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. Incorporar el concepto de madurez en el ámbito de ciberseguridad, permitirá ir evolucionando a los SS.PP. en cuanto a la calidad de los controles de ciberseguridad implementados.

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 Nch-ISO/IEC 27032.
- 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/

- Ley N°21.180 sobre Transformación digital del Estado[9] y las normas técnicas derivadas de su reglamento[10].
    - Norma Técnica de Interoperabilidad
    - Norma Técnica de Seguridad de la Información y Ciberseguridad
    - Norma Técnica de Documentos y Expedientes Electrónicos
    - Norma Técnica de Notificaciones
    - Norma Técnica de Calidad y Funcionamiento
    - Norma Técnica de Autenticación

[9] https://www.bcn.cl/leychile/navegar?idNorma=1138479
[10] https://www.bcn.cl/leychile/navegar?idNorma=1169585

II. La importancia seguridad de la información en cuanto al uso de redes públicas

En general las normas sobre privacidad y comunicaciones electrónicas tienen por objeto garantizar la privacidad, la confidencialidad y la protección de los datos personales de las comunicaciones electrónicas en amparo de los derechos y libertades fundamentales de las personas naturales y jurídicas.

En este contexto, las instituciones deben procurar que las comunicaciones que se producirán producto del acceso a sus servicios o en las comunicaciones que han de tener con los ciudadanos, que en general ocurrirán a través de la Internet, estén protegidas de acciones maliciosas.

Dichos servicios y comunicaciones contendrán información potencialmente sensible, pudiendo incluir datos personales o información comercial protegida por las leyes de propiedad industrial e intelectual, que en caso de ser conocida por terceras partes podrían afectar o dañar a los propietarios de dicha información, exponiendo a su vez al estado a potenciales juicios por el resguardo inadecuado de la información que obra en su poder.

Vale la pena resaltar las exigencias que hace el decreto supremo N °1 de 2015, del Ministerio Secretaría General de la Presidencia:

Artículo 6º.- Para el desarrollo o implementación segura de los sistemas web y sitios web, deberán aplicarse estándares de desarrollo, compatibilidad y las directrices principales de las normas internacionales y nacionales sobre seguridad, de manera de permitir el debido resguardo de la disponibilidad, integridad y confidencialidad de la información tanto del sistema en sí como de los datos institucionales o de los ciudadanos que se encuentren o estén accesibles en dichos sistemas web y sitios web. Para estos efectos, se considerarán los estándares internacionales definidos por la W3C, las normas de la familia ISO27000 o las que las reemplacen y las buenas prácticas de los fabricantes o proveedores de plataforma o de los lenguajes de los sistemas.

Artículo 13.- Todo sitio web deberá hacer uso del dominio ".gob.cl", registrándolo previamente ante la División de Informática del Ministerio del Interior y Seguridad Pública, y en el sitio electrónico http://nic.gob.cl

De igual modo, los sitios web deberán registrar en sus servicios de nombres las tablas reversas de la o las direcciones IP asociadas al dominio ".gob.cl" correspondiente. En caso que se informe al público un nombre distinto al asociado a ".gob.cl", ese nombre deberá de todos modos redireccionar al dominio ".gob.cl".

Artículo 15.- Para todo sistema web que requiera autentificación o bien sea de acceso restringido, toda comunicación debe establecerse mediante un canal de comunicaciones privado, con el objetivo de cifrar los datos durante su transmisión mediante mecanismos SSL/TLS, o los protocolos que los remplacen, con el fin de aumentar el nivel de protección de la información.

Algunos términos que se emplean bajo este control son:

Certificado digital

Un certificado digital es un fichero informático generado por una entidad denominada Autoridad Certificadora (CA) que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet.

El certificado digital es válido para autenticar la existencia y validez de un usuario o sitio web por lo que es necesaria la colaboración de un tercero que sea de confianza para cualquiera de las partes que participe en la comunicación. El nombre asociado a esta entidad de confianza es Autoridad Certificadora pudiendo ser un organismo público o empresa reconocida en Internet.

El certificado digital tiene como función principal autenticar al poseedor pero puede servir también para cifrar las comunicaciones y firmar digitalmente. En algunas

administraciones públicas y empresas privadas es requerido para poder realizar ciertos trámites que involucren intercambio de información sensible entre las partes.

Cifrado

Proceso de codificación de información para poder evitar que esta llegue a personas no autorizadas. Solo quien posea la clave podrá acceder al contenido.

Confidencialidad

Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad de la información constituye la piedra angular de la seguridad de la información. Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información.

HTTPS

Protocolo seguro de transferencia de hipertexto, más conocido por sus siglas HTTPS, del inglés Hypertext Transfer Protocol Secure, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto. Dicho en otras palabras, es la versión segura de HTTP.

En HTTPS el tráfico HTTP es cifrado mediante un algoritmo de cifrado simétrico cuya clave ha sido previamente intercambiada entre el navegador y el servidor. Es utilizado por cualquier tipo de servicio que requiera el envío de datos personales o contraseñas, entidades bancarias, tiendas en línea, pago seguro, etc.

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

III. RECOMENDACIONES Y MEJORES PRÁCTICAS ASOCIADAS AL CONTROL

El control: Aseguramiento de servicios de aplicación en redes públicas

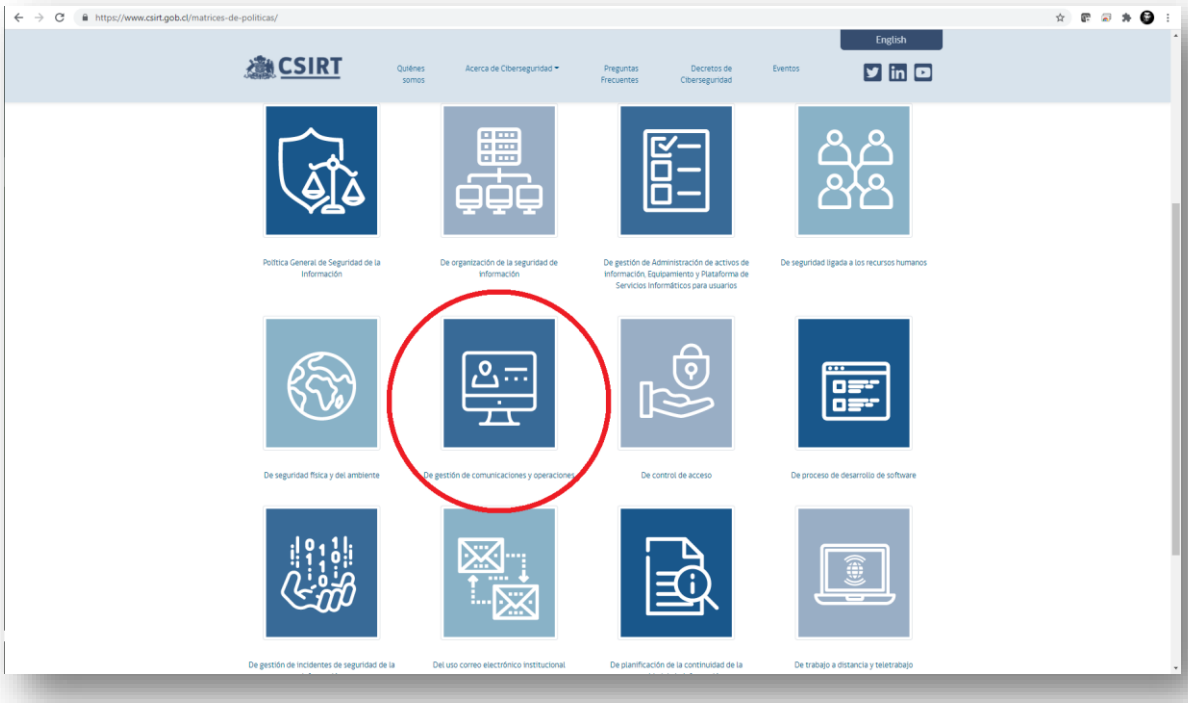
La información relacionada a servicios de aplicación que pasan por redes públicas debe ser protegida de la actividad fraudulenta, disputas contractuales y su divulgación y modificación no autorizada.

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 mantener seguras las redes y la información que fluye por ellas.

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/



La organización debe determinar y monitorear de manera regular la seguridad de sus servicios y de la capacidad para proteger las comunicaciones que se produzcan a través de redes públicas como lo es Internet.

Las consideraciones de seguridad de la información para los servicios de aplicación que pasan a través de redes públicas deberían incluir lo siguiente:

a) el nivel de confianza que requiere cada parte sobre la identidad manifestada de la otra, es decir, a través de la autenticación;
b) procesos de autorización asociados a las personas que pudieran aprobar los contenidos de, emitir o firmar documentos de transacciones clave.
c) garantizar que todos los socios en la comunicación estén completamente informados de sus autorizaciones de la provisión o el uso del servicio;

d) determinar y cumplir con los requisitos de confidencialidad, integridad, prueba de despacho y recepción de documentos clave y el no repudio de contratos, es decir, asociados con los procesos de licitación y contratos;
e) el nivel de confianza que se requiere en la integridad de documentos clave;
f) los requisitos de protección de cualquier tipo de información confidencial;
g) g). la confidencialidad y la integridad de cualquier transacción de órdenes, información de pago, detalles de la dirección de envío y la confirmación de los recibos;
h) el grado de verificación adecuado para verificar la información de pago proporcionada por un cliente;
i) selección del acuerdo más adecuado de forma de pago para protegerse contra los fraudes;
j) el nivel de protección necesario para mantener la confidencialidad y la integridad de la información de la orden;
k) evitar la pérdida o duplicación de la información de transacción;
l) responsabilidad asociada con cualquier tipo de transacciones fraudulentas;
m) requisitos de seguros.

Muchas de las consideraciones anteriores se pueden abordar con la aplicación de controles criptográficos, considerando el cumplimiento con los requisitos legales.

Las disposiciones de servicio de aplicaciones entre socios se deberían respaldar con un acuerdo documentado que comprometa a ambas partes a los términos de servicios acordados, incluidos los detalles de autorización (ver letra b) de arriba.

Se deberían considerar los requisitos de resiliencia contra ataques, los que pueden incluir los requisitos para la protección de los servidores de aplicaciones involucrados o garantizar la disponibilidad de las interconexiones de redes necesarias para entregar el servicio.

La institución debe asegurar durante sus procesos de desarrollo, ya sean internos o encomendados a un tercero, técnicas no solo de desarrollo seguro, sino que debe considerar otros requerimientos a nivel de seguridad tales como por ejemplo:

a) La conectividad entre el cliente y servidor, ya sea a través de un aplicativo o por medio de una conexión web debe ser cifrada.
b) No debe almacenar información en ambientes locales.
c) Debe contar con validadores para los procesos de intercambios de información, con el objeto de evitar corrupciones o pérdida de información, sobre todo si los canales de transmisión son a través de Internet.
d) Los datos deben ser guardados en forma cifrada.

Antes de la puesta en producción, se debe revisar que todos los requisitos de seguridad establecidos han sido cubiertos y no han quedado brechas que pongan en riesgo la información de los usuarios o de la institución, sobre todo aquella de carácter confidencial.

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