CORFO

GERENCIA DE TECNOLOGÍA
UNIDAD DE CONTRATACIÓN PÚBLICA
CCVH

RESOLUCIÓN EXENTA

CORFO
OFICINA DE PARTES
12.11.19 01092
SANTIAGO

DEJA SIN EFECTO LA RESOLUCIÓN EXENTA N° 1.623, DE 2018, DE CORFO, Y APRUEBA LA "POLÍTICA INFORMÁTICA Y DE SEGURIDAD DE LA INFORMACIÓN DE CORFO".

V I S T O: EXENTA - DE TOMA DE RAZON

Las facultades conferidas en la Ley Nº 6.640, y en el Reglamento General de la Corporación, aprobado por Decreto Supremo Nº 360, de 1945, del Ministerio de Economía; el Decreto Supremo N° 93, de 2019, del Ministerio de Economía, Fomento y Turismo (en trámite), que nombra al Vicepresidente Ejecutivo de la Corporación de Fomento de la Producción; lo dispuesto en la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; la Ley N° 19.880, que Establece Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado; el DFL N° 29, de 2004, que Fija Texto Refundido, Coordinado y Sistematizado de la Ley N° 18.834, Sobre Estatuto Administrativo; las normas establecidas en la Ley N° 19.799, sobre Documentos Electrónicos, Firma Electrónica y los Servicios de Certificación de dicha firma, y su Reglamento, aprobado por Decreto N° 181, de 2005, modificado por Decreto Supremo N° 14, de 2014, ambos del Ministerio de Economía, Fomento y Turismo; la Ley N° 20.285, que Regula el Principio de Transparencia de la Función Pública y el Derecho de Acceso a la Información de los Órganos de la Administración del Estado, y su Reglamento, aprobado por Decreto N° 13, de 2009, del Ministerio Secretaría General de la Presidencia; la Ley N° 19.628, sobre Protección de la Vida Privada y Datos Personales, y su Reglamento, aprobado por Decreto N° 799, de 2000, del Ministerio de Justicia; la Ley N° 17.336, sobre Propiedad Intelectual, y su Reglamento, aprobado por Decreto N° 277, de 2013, del Ministerio de Educación; el Decreto Supremo Nº 77, de 2004, del Ministerio Secretaría General de la Presidencia, que aprueba la Norma Técnica sobre Eficiencia de las Comunicaciones Electrónicas entre Órganos de la Administración del Estado y entre Estos y los Ciudadanos; el Decreto Supremo Nº 81, de 2004, modificado por el Decreto Supremo Nº 158, de 2006, ambos del Ministerio Secretaría General de la Presidencia, que aprueba la Norma Técnica para los Órganos de la Administración del Estado sobre Interoperabilidad de Documentos Electrónicos; el Decreto Supremo N° 83, de 2005, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos; el Decreto Supremo N° 93, de 2006, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para la Adopción de Medidas destinadas a Minimizar los Efectos Perjudiciales de los Mensajes Electrónicos Masivos no Solicitados Recibidos en las Casillas Electrónicas de los Órganos de la Administración del Estado y de sus Funcionarios; y el Decreto Supremo Nº 533, de 2015, del Ministerio del Interior y Seguridad Pública, que crea el Comité Interministerial de Ciberseguridad; y lo establecido en la Resolución Nº 7, de 2019, de la Contraloría General de la República,

que Fija normas sobre exención del trámite de toma de razón, junto con la Resolución N° 8, de 2019, del mismo Órgano Contralor, que Determina los montos en UTM a partir de los cuales los actos que se individualizan quedarán sujetos a toma de razón y a controles de reemplazo cuando corresponda.

C O N S I D E R A N D O:

1. Que, las Resoluciones Conjuntas de los Ministerios de Economía y de Hacienda N° 60, de 1998, y N° 05, de 2005, y sus respectivas modificaciones, otorgan al personal de la Corporación de Fomento de la Producción, la asignación de modernización que en dichos actos se regula, la que contempla un incremento por desempeño institucional que se concederá en atención a la ejecución eficiente y eficaz por parte de Corfo, de los distintos Programas de Mejoramiento de la Gestión (PMG), dando derecho a los incrementos que allí se indican, según el grado de cumplimiento de los objetivos de gestión anuales que se hayan comprometido en la correspondiente Resolución Conjunta de los Ministerios de Economía, Interior, Hacienda, y Secretaría General de la Presidencia.

2. Que, mediante Decreto Exento N° 324, de 2018, Conjunto de los Ministerios de Hacienda, Interior y Seguridad Pública, y Secretaría General de la Presidencia, se aprobó el Programa Marco de los Programas de Mejoramiento de la Gestión (PMG) para el año 2019, el cual contempló en el Objetivo N° 1 "Gestión Eficaz", el Indicador "Controles de Seguridad de la Información", en adelante "PMG-SSI", el que tiene por objeto implementar, de forma progresiva, los controles establecidos en la norma Nch-ISO 27001 con la finalidad de gestionar los riesgos de seguridad de la información, de los activos vinculados a los procesos de provisión de productos estratégicos, mediante la instalación de un Sistema de Gestión de Seguridad de la Información con foco en la ciberseguridad, asegurando la continuidad de los servicios críticos del Estado para lograr conservar la confidencialidad, integridad y disponibilidad de la información.

3. Que, mediante el Decreto Exento N° 554, de 2018, Conjunto de los Ministerios de Economía, Fomento y Turismo, Hacienda, Interior y Seguridad Pública, y Secretaría General de la Presidencia, se fijaron los objetivos de gestión del año 2019 para, entre otros organismos, la Corporación de Fomento de la Producción, estableciendo como compromiso de indicador transversal en el "PMG-SSI", la implementación de 54 nuevos controles de la norma Nch-ISO 27001.

4. Que, con la finalidad de cumplir este compromiso es necesario dejar sin efecto la actual "Política Informática y de Seguridad de la Información de Corfo", formalizada mediante la Resolución Exenta Nº 1.623, de 2018, de Corfo, a fin de establecer un nuevo texto refundido, coordinado y sistematizado que incorpore todas las actualizaciones y modificaciones que se requieren para su adecuación al "PMG-SSI".

5. Que, el objeto de la "Política Informática y de Seguridad de la Información de Corfo" es establecer y dar a conocer en forma clara y precisa los procedimientos de Corfo para la seguridad de la información y las comunicaciones por medio del establecimiento de instrucciones para la utilización de servicios y recursos computaciones e institucionales, lo que constituye, no sólo parte del cumplimiento del "PMG-SSI", sino que una significativa contribución a la mejora organizacional a través de la generación de una adecuada gestión de procesos por medio de la identificación, documentación, perfeccionamiento, monitoreo y optimización, tendiendo a la mejora continua

6. Que, en la Sesión Extraordinaria N° 1/2019, de 30 de septiembre de 2019, del Comité de Seguridad de la Información de Corfo, se aprobaron los principios,

normas y lineamientos generales de la "Política Informática y de Seguridad de la Información de Corfo", que se sanciona en la presente Resolución.

7. El Memorándum N° 63, de 24 de octubre de 2019, de la Gerencia de Tecnología, por el cual se solicita formalizar la "Política Informática y de Seguridad de la Información de Corfo", confeccionada en virtud de los lineamientos aprobados por el Comité de Seguridad de la Información de Corfo.

R E S U E L V O:

1° **DÉJASE** sin efecto la Resolución Exenta Nº 1.623, de 2018, de Corfo, que "Deja sin Efecto la Resolución (E) N° 1.676, de 2017, de Corfo, y Aprueba la Política Informática y de Seguridad de la Información de Corfo".

2° **APRUÉBASE** la "**Política Informática y de Seguridad de la Información de Corfo**", cuyo texto es el siguiente:

POLÍTICA INFORMÁTICA Y DE SEGURIDAD DE LA INFORMACIÓN DE CORFO

1. Objetivo general

Actualizar las directivas generales que orienten el uso de los sistemas computacionales y promuevan las buenas prácticas en Corfo, reflejando el compromiso, apoyo, interés, fomento y desarrollo de una cultura de seguridad informática y de seguridad de la información institucional.

Tener y mantener una mejora organizacional continua a través de la generación de una adecuada gestión de procesos por medio de la identificación, documentación, perfeccionamiento, monitoreo y optimización.

2. Ámbito de aplicación

Corfo buscará garantizar que se implemente y opere un sistema de seguridad de la información de acuerdo con las políticas y procedimientos institucionales, previniendo así incumplimientos a requisitos legales, normativos y/o contractuales.

Los objetivos y productos estratégicos del Formulario A1 de la Gerencia Corporativa de Corfo, que definen el alcance del sistema de seguridad de la información de la presente Política, son:

Objetivo Estratégico	Producto Estratégico A1
Promover el desarrollo de las PYMES, el fortalecimiento de las capacidades y procesos de innovación dentro de las empresas, la sofisticación de la oferta existente mediante I+D y el apoyo a nuevas formas de innovación que impacten positivamente a la sociedad y que permitan resolver grandes desafíos de Chile.	Subsidios para el Desarrollo de la Innovación
Fomentar el emprendimiento mediante subsidios, plataformas de apoyo y promoción de cultura para mejorar la productividad de las empresas y la diversificación productiva.	Subsidios para el Desarrollo de Emprendimientos

3. Marco regulatorio

Corfo, en la búsqueda constante de mejorar los principios de eficiencia y eficacia que rigen la Administración del Estado, estableció e implementó una primera versión de la "Política de Usos Generales de los Sistemas Computacionales de Corfo" el año 2006.

A contar del año 2009, la Dipres incorporó al Programa de Mejoramiento de la Gestión del Estado (PMG), un nuevo sistema, denominado "Seguridad de la Información" (PMG-SSI), el que tiene por objeto implementar, de forma progresiva, los controles establecidos en la norma NCH-ISO 27001 a la actuación de los órganos de la Administración. Esta situación ha generado la continua necesidad de actualizar la Política de Seguridad de Corfo, razón por la cual esta Corporación ha dictado los siguientes actos administrativos:

- Resolución Exenta Nº 1.669, de 2012.
- Resolución Exenta Nº 1.341, de 2013.
- Resolución Exenta Nº 1.926, de 2016.
- Resolución Exenta Nº 1.676, de 2017.
- Resolución Exenta Nº 1.623, de 2018, que establece la actual "Política Informática y de Seguridad de la Información de Corfo".

Como consecuencia de las nuevas normas dictadas en materia de seguridad de la información, así como los cambios tecnológicos, la Dipres, en virtud de la facultad establecida en el Decreto Exento Nº 1.232, de 2007, del Ministerio de Hacienda, dictó la Circular Nº 26, de 31 de octubre de 2018, mediante la cual incorporó en el PMG-SSI del año 2019 la implementación de 54 nuevos controles de la norma NCH-ISO 27001, razón por la cual es necesario modificar la actual "Política Informática y de Seguridad de la Información de Corfo", formalizada mediante la Resolución Exenta Nº 1.623, de 2018, de Corfo, a fin de incorporar todas las actualizaciones y modificaciones que se requieren para adecuarla a lo solicitado en el PMG-SSI.

Finalmente, se deja constancia de que esta Política incorpora y da cumplimiento, tanto a la normativa relativa al PMG-SII, como a lo dispuesto en los siguientes cuerpos normativos, reglamentarios e Instructivos Presidenciales:

- Ley N° 19.799, sobre Documentos Electrónicos, Firma Electrónica y los Servicios de Certificación de dicha firma, y su Reglamento, aprobado por Decreto N° 181, de 2005, modificado por Decreto Supremo N° 14, de 2014, ambos del Ministerio de Economía, Fomento y Turismo.

- Ley N° 19.880, que Establece Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado.

- Ley N° 20.285, que Regula el Principio de Transparencia de la Función Pública y el Derecho de Acceso a la Información de los Órganos de la Administración del Estado, y su Reglamento, aprobado por Decreto N° 13, de 2009, del Ministerio Secretaría General de la Presidencia.

- Ley N° 19.223, sobre Delitos Informáticos.

- Ley N° 19.927, sobre Delitos de Pornografía Infantil.

- Ley N° 19.628, sobre Protección de la Vida Privada y Datos Personales, y su Reglamento, aprobado por Decreto N° 799, de 2000, del Ministerio de Justicia.

- Ley N° 17.336, sobre Propiedad Intelectual, y su Reglamento, aprobado por Decreto N° 277, de 2013, del Ministerio de Educación.

- Decreto Supremo Nº 77, de 2004, del Ministerio Secretaría General de la Presidencia, que aprueba la Norma Técnica sobre Eficiencia de las

Comunicaciones Electrónicas entre Órganos de la Administración del Estado y entre Estos y los Ciudadanos.

- Decreto Supremo Nº 81, de 2004, modificado por el Decreto Supremo Nº 158, de 2006, ambos del Ministerio Secretaría General de la Presidencia, que aprueba la Norma Técnica para los Órganos de la Administración del Estado sobre Interoperabilidad de Documentos Electrónicos.

- Decreto Supremo N° 83, de 2005, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.

- Decreto Supremo Nº 1.299, de 2005, del Ministerio del Interior y Seguridad Pública, que establece nuevas normas que regulan la red de conectividad del Estado que administra el Ministerio del Interior y fija los procedimientos, requisitos y estándares tecnológicos para la incorporación a dicha red de instituciones públicas.

- Decreto Supremo N° 93, de 2006, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para la Adopción de Medidas destinadas a Minimizar los Efectos Perjudiciales de los Mensajes Electrónicos Masivos no Solicitados Recibidos en las Casillas Electrónicas de los Órganos de la Administración del Estado y de sus Funcionarios.

- Decreto Supremo Nº 271, de 2009, del Ministerio de Economía, Fomento y Turismo, que aprueba el Reglamento sobre la Inscripción de Esquemas Documentales en el Repositorio Administrador de Esquemas y Metadatos para los Órganos de la Administración del Estado.

- Decreto Supremo Nº 1, de 2015, del Ministerio Secretaría General de la Presidencia, que aprueba Norma Técnica sobre Sistemas y Sitios Web de los Órganos de la Administración del Estado.

- Decreto Supremo Nº 533, de 2015, del Ministerio del Interior y Seguridad Pública, que crea el Comité Interministerial de Ciberseguridad.

- Instructivo Presidencial Nº 3, de 2001, que establece la Política Nacional para la Participación Activa de los Órganos Públicos en el uso de Internet.

- Instructivo Presidencial Nº 5, de 2001, sobre Gobierno Electrónico, que imparte instrucciones para su desarrollo.

- Instructivo Presidencial Nº 6, de 2004, sobre Firma Electrónica, que imparte instrucciones sobre su implementación en los actos, contratos y cualquier tipo de documento en la Administración del Estado, para dotar así de un mayor grado de seguridad a las actuaciones gubernamentales que tienen lugar por medio de documentos electrónicos y dar un mayor grado de certeza respecto de las personas que suscriben tales documentos.

- Instructivo Presidencial Nº 8, de 2006, sobre Transparencia Activa y Publicidad de la Información de la Administración del Estado.

- Instructivo Presidencial Nº 2, de 2012, sobre Digitalización de Trámites Públicos, especialmente en lo relativo a la simplificación y eliminación de estos.

- Instructivo Presidencial Nº 5, de 2012, sobre Participación Ciudadana y "Gobierno Abierto".

- Instructivo Presidencial Nº 7, de 2014, sobre Participación Ciudadana.

- Instructivo Presidencial Nº 1, de 2017, que instruye la implementación de la Política Nacional de Ciberseguridad.

- Instructivo Presidencial Nº 1, de 2018, que entrega directrices sobre evaluación y adopción preferente de servicios en la nube por parte de los órganos de la administración central del Estado.

- Instructivo Presidencial Nº 8, de 2018, que imparte instrucciones en materia de ciberseguridad,

- Instructivo Presidencia Nº 1, de 2019, sobre transformación digital en los Órganos de la Administración del Estado.

- Norma NCH-ISO 27.001, sobre Sistemas de Gestión de Seguridad de la Información, que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

4. Glosario, procedimientos, estándares e instructivos

Los documentos operacionales que permiten implementar las presentes políticas se encuentran publicados en el Repositorio Documental de la Gerencia de Tecnología. Dichos documentos se refieren al Glosario de Términos, Procedimientos, Estándares e Instructivos de Seguridad de la Información.

5. Roles y responsabilidades

A continuación, se individualizan los roles, y las respectivas responsabilidades, de los órganos, funcionarios y terceros involucrados en la determinación y ejecución de las presentes Políticas.

a. **Comité de Seguridad de la Información**: El Decreto Exento N° 239, de 21 de agosto de 2014, del Ministerio de Hacienda, que fija los Programas de Mejoramiento de la Gestión de los Servicios en el Año 2015, dentro del programa específico de seguridad de la información, estableció la creación de un Comité de Seguridad de la Información.

   Este Comité, creado por Resolución Exenta Nº 1.814, de 2015, de Corfo, modificada por las Resoluciones Exentas N° 16 y N° 862, ambas de 2019, y de Corfo, es responsable de supervisar la implementación de los procedimientos y estándares que se desprenden de estas Políticas, proponer estrategias y soluciones específicas para la implantación de los controles necesarios para su materialización, y la debida solución de las situaciones de riesgo detectadas, así como arbitrar conflictos en materia de seguridad de la información y los riesgos asociados, y proponer soluciones sobre ello, coordinarse con los Comités de Calidad y de Riesgos para mantener estrategias comunes de gestión.

b. **Encargado de Seguridad:** Tiene a su cargo el desarrollo de las políticas de seguridad al interior de Corfo y el control de su implementación, velando por su correcta aplicación. Gestionar los procedimientos de respuesta a incidentes.

   Asimismo, debe disponer y ejecutar las medidas para estos fines, las que deben cumplir con lo dispuesto en la normativa relativa a Gobierno Digital, individualizada en el número 3 de estas Políticas.

c. **Encargado de Ciberseguridad:** Asegurar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información. Realizar la planificación y preparación de la respuesta a incidentes, así como también el

monitoreo continuo de eventos de seguridad para la correcta detección y análisis de eventos.

d. **Funcionarios Corfo:** Cumplir en el desarrollo de sus funciones las medidas de seguridad de la información contenidas en esta Política, las que revisten el carácter de obligatorias.

   Por esta razón las presentes Políticas forman parte del Reglamento Interno de Higiene, Orden y Seguridad de Corfo, aprobado por Resolución Exenta Nº 2.215, de 2009, y sus modificaciones posteriores.

e. **Proveedores de Corfo:** En la ejecución de contratos de prestación de servicios que involucren el acceso a los sistemas de información de Corfo, así como a activos de información de esta, deberán dar cumplimiento a lo establecido en las presentes Políticas.

f. **Gerencia de Tecnología:** Entregar acceso a los auditores. Establecer las excepciones a las normas de las políticas y procedimientos de seguridad de la información.

g. **Unidad de Continuidad Operativa:** Administrar la plataforma TI de Corfo y gestionar sus componentes y usuarios.

h. **Gerencia de Auditoría Interna:** Ejecución de las auditorías internas en la Corporación.

i. **Vicepresidente Ejecutivo:** Definir y aprobar el conjunto de Políticas Informáticas y de Seguridad de la Información, y asegurar su cumplimiento

j. **Gerencia de Administración y Finanzas:** Hacer toma de razón de los robos, hurtos o destrucción accidental de los equipos de comunicación móvil y periféricos. Eventualmente establecer controles de acceso a proveedores. Participar en revisiones y entrenamientos relacionados con la privacidad de la información personal

k. **Fiscalía:** Participar en revisiones y entrenamientos relacionados con la privacidad de la información personal y la regulación relativa a seguridad de la información.

l. **Subgerencia de Tecnología:** Definir procedimientos para que la seguridad de la información sea una parte integral de los sistemas de información en todo su ciclo de vida.

6. Periodicidad de revisión

La revisión de estas Políticas, y todos sus anexos, será revisada una vez al año, o al generarse cambios normativos, o contingencias que la afecten, y será sometida a validación del Comité de Seguridad de la Información.

7. Excepciones al cumplimiento

En casos especiales el Comité de Seguridad de la Información evaluará y podrá adoptar medidas puntuales de excepción para el cumplimiento de las directrices de esta Política de Seguridad de la Información. Toda excepción deberá ser justificada y documentada, generando un proceso de revisión de la Política, para determinar si es necesario hacer cambios en ésta.

8. Medios de difusión

Los medios a través de los cuales será difundida la presente Política Informática y de Seguridad de la Información de Corfo, serán uno o más de los que se indican a continuación, de acuerdo a la estrategia de difusión que haya establecido el Comité de Seguridad de la Información para el período en curso:

a) **Intranet:** Texto completo y actualizado de la Política Informática y de Seguridad de la Información de Corfo, las Políticas anexas y sus documentos operacionales y anexos.

b) **Todos en Red:** Informando actualizaciones aplicadas a la Política, así como un manual para usuarios con los principales puntos de este documento y recomendaciones.

c) **Videoconferencia:** cuando la actualización de la Política contemple modificaciones sustanciales y/o de fondo, y la situación lo amerite.

d) **Capacitación On-Line:** A través de plataforma e-Learning de Corfo.

9. Control de cambios

Teniendo en consideración que esta Política Informática y de Seguridad de la Información de Corfo es aprobada por un acto administrativo, y que deroga la versión anterior de la Política, se concluye que esta Política Informática y de Seguridad de la Información de Corfo no debe tener un historial de modificaciones o control de cambios.

10. Contenido

Esta Política establece recomendaciones para la utilización de los servicios y recursos de tecnologías de la información y comunicaciones (TIC) entregados por Corfo a los usuarios de sus sistemas, así como las medidas de seguridad de la información que se indican a continuación, las que revisten el carácter de obligatorias para las personas que trabajan para Corfo y los proveedores de servicios, quienes deberán ajustar su desempeño.

Su inobservancia dará lugar al inicio de procedimientos disciplinarios que podrían concluir con la aplicación de sanciones administrativas, conforme a lo dispuesto en el Reglamento Interno de Orden, Higiene y Seguridad de Corfo; el Decreto con Fuerza de Ley N° 29, de 2004, que Fija Texto Refundido, Coordinado y Sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo; y en la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

Todas y cada una de las personas que trabajan para Corfo, independiente de su calidad contractual, deben cumplir y respetar las políticas establecidas en los siguientes capítulos, según las atribuciones que les ha entregado la Institución:

a) Política de seguridad de la información

b) Política de control de acceso lógico

c) Política de acceso a Internet

d) Política de correo electrónico

e) Política de antivirus

f) Política de respaldo

g) Política de uso de equipos de comunicación móvil y periféricos computacionales

h) Política de uso y seguridad de equipamiento computacional fuera de Corfo

i) Política de escritorios y pantallas limpias

j) Política de seguridad física y ambiental

k) Controles de auditoría de sistemas de información

l) Política de seguridad en relación con proveedores

m) Política de privacidad y protección de datos personales

n) Política de gestión de incidentes de seguridad de la información

ñ) Política de gestión de vulnerabilidades técnicas

o) Política de separación de ambientes

p) Política de desarrollo seguro

q) Política de la continuidad de la seguridad de la información

r) Política de seguridad para el desarrollo de personas

s) Otros alcances

En los contratos que Corfo celebre con proveedores de bienes o servicios en los que se requiera el acceso a los sistemas o activos de información de Corfo, esta Política deberá formar parte integrante de los respectivos contratos u otros instrumentos en que conste la contratación.

POLÍTICA DE SEGURIDAD DE INFORMACIÓN

1. Objetivo

Proporcionar el marco de trabajo para establecer los objetivos de seguridad de la información y definir las reglas que deben seguir las personas que trabajan en Corfo.

2. Definición

2.1. Cumplimiento transversal

Todas y cada una de las personas que trabajan para Corfo, independiente de su calidad contractual, así como los prestadores de bienes y servicios, deberán cumplir los siguientes principios básicos, tanto como sea posible en atención al ejercicio de sus funciones o actividades, según las atribuciones que les ha entregado la Institución o los servicios contratados.

a) Conocer esta Política Informática y de Seguridad de la Información de Corfo y aplicar los criterios de confidencialidad, integridad y disponibilidad, establecidos respecto de activos de información de Corfo.

b) Cuidar la información a su cargo, especialmente en relación a su confidencialidad, integridad y disponibilidad. Asimismo, deberán cuidar los medios de soporte (material impreso, computadores, archivadores, u otros) y los accesos a sistemas de procesamiento (software, aplicativos, correo u otros), a fin de que se mantengan los requisitos señalados en estas Políticas.

c) Recibir capacitación sobre seguridad de la información, en general, y sobre esta Política en particular. Además, se deberá realizar una amplia difusión adicional de esta Política en términos simplificados para un correcto entendimiento de todos los funcionarios o prestadores de servicios.

d) En concordancia con lo establecido en el objetivo general de la Política Informática y de Seguridad de la Información de Corfo, las cláusulas pertinentes en los contratos de trabajo o de honorarios, las resoluciones de nombramiento de los funcionarios de Corfo y/o los contratos de prestación de servicios, contemplarán la aplicación de las sanciones establecidas en el ordenamiento jurídico por el mal uso de información desde los sistemas informáticos y activos de información de Corfo. Por lo tanto, toda persona deberá procurar proteger y no exponer la información que está bajo su responsabilidad.

e) Para prevenir potenciales fugas de información o proteger la información contenida en los equipos computacionales, o a solicitud del Gerente del área respectiva, se podrán realizar bloqueos de los puertos USB, u otros del mismo tipo, a determinados usuarios. De ser necesario, este bloqueo podrá ser aplicado a cualquier otro dispositivo que permita la grabación de datos en forma externa, así como el bloqueo o regulación del acceso a Internet.

f) Para reducir el riesgo causado por modificaciones de la información no autorizadas y por uso inadecuado de los activos de la información, se deben segregar las funciones o servicios.

2.2. De la Vicepresidencia Ejecutiva

Al Vicepresidente Ejecutivo de Corfo, en su calidad de Jefe Superior de Servicio, le competen directamente los siguientes lineamientos de seguridad de la información:

a) Disponer la realización de acciones destinadas a la inducción, capacitación y concientización de seguridad de la información a todas las personas que trabajan en o para Corfo, independiente de su calidad contractual.

b) Definir y aprobar un conjunto de Políticas Informáticas y de Seguridad de la Información, las que serán luego publicadas para todas las personas que trabajan en o para Corfo.

c) Establecer las medidas y procedimientos necesarios para asegurar el cumplimiento de estas Políticas, así como los mecanismos para establecer las sanciones que correspondan en caso de su incumplimiento.

d) Instruir a las unidades de Corfo directamente relacionadas en la aplicación y ejecución de estas Políticas sobre las acciones necesarias para asegurar su cumplimiento.

CORFO

POLÍTICA DE CONTROL DE ACCESO LÓGICO

Los sistemas para la gestión de contraseñas deberán asegurar contraseñas de calidad, que permitan la identificación inequívoca y personalizada del usuario.

1. Objetivo

Limitar el acceso a los recursos de información de acuerdo a los requisitos del negocio y de seguridad de la información.

2. Definiciones

2.1. Contraseñas para administradores

a) Ante un cambio de contraseña, por parte del usuario administrador, el sistema debe estar configurado para aceptar sólo lo definido como el estándar Corfo "Contraseñas para Administradores".

2.2. Contraseñas para usuarios

a) Todas las contraseñas deben ser difíciles de adivinar. No se deben utilizar palabras completas, secuencias conocidas de caracteres, datos personales, etc. Se deben usar combinaciones de letras, números y signos.

b) La contraseña no debe ser ni contener el nombre del usuario.

c) Los usuarios no deben construir contraseñas idénticas o muy parecidas a contraseñas anteriores, por ejemplo, usar series como Sesamo1, Sesamo2, Sesamo3, etc.

d) Se debe cambiar frecuentemente de contraseña, en especial cuando tenga sospechas de que alguien más pueda conocerla.

e) No se debe copiar o registrar la contraseña en papeles u otros medios que se encuentren visibles para otras personas.

f) El usuario tiene prohibido revelar la contraseña. Las excepciones deben ser autorizadas caso a caso.

g) Ante un cambio de contraseña por parte del usuario, el sistema debe estar configurado para aceptar sólo lo definido como el estándar Corfo para esto.

2.3. Control de acceso

a) Perfilamiento de acceso

- Los derechos de acceso a los sistemas y plataformas deben estar plasmados en perfiles de acceso, para facilitar su gestión.
- La asignación y uso de los perfiles de acceso deben ser debidamente autorizados, ajustándose al principio de privilegios mínimos necesarios para el ejercicio de sus funciones.
- Los perfiles de acceso definen los derechos de acceso a los sistemas y plataformas.
- La asignación y uso de los perfiles de acceso deben ser debidamente autorizados por los propietarios de los procesos o sistemas, ajustándose al principio de privilegios mínimos necesarios para el ejercicio de sus funciones.

b) Accesos privilegiados

- La asignación y uso de derechos de acceso con privilegios especiales o privilegios de administrador, debería ser restringido y controlado, de

acuerdo con las necesidades requeridas para el cumplimiento de sus funciones.

c) Inicio de sesión seguro
- A cada funcionario se le asignará una cuenta de red asociada al correo electrónico y a las aplicaciones de Corfo, con una clave única, la que no debe ser revelada a ninguna persona.
- Al momento de ingresar al computador, se solicitarán los datos de "Nombre de Usuario", "Contraseña" y "Conectarse a (Dominio)". El usuario debe fijarse que el nombre del usuario se encuentre escrito en la primera casilla y que corresponda al que se le asignó. Si no corresponde con el que habitualmente usa en el computador significa que otra persona ha utilizado su equipo y deberá cambiarlo para ingresar. Sólo la combinación del nombre de usuario y contraseña correcta le permitirá ingresar al computador.
- El usuario debe solicitar asistencia a la Mesa de Ayuda, en caso de que se equivoque al ingresar la contraseña correcta de su cuenta y ésta se bloquee y le impida iniciar la sesión.

d) Segregación de funciones
- El otorgamiento de accesos a recursos de información de Corfo deberá tomar en consideración la segregación de funciones que exista.
- La asignación de atributos de acceso deberá ser definida respecto a usuarios individuales, de forma que la responsabilidad por las acciones ejercidas con los accesos otorgados sea directamente atribuible a una persona individualizable.
- El dueño de la información, según se establezca en el inventario y catálogo de los activos de la información, es el responsable de decidir respecto al acceso a los datos por parte del usuario.
- La asignación de acceso a funciones de negocio u opciones tecnológicas y el acceso a los datos se debe limitar sólo a aquello que el usuario necesita saber o utilizar.
- Las necesidades de los usuarios deben ser determinadas en función de las tareas asignadas por Corfo.
- El control de acceso debe ser administrado considerando las distintas instancias que un usuario debe resolver para tener acceso a los datos, p.ej. redes, sistemas operativos, aplicaciones y administradores de bases de datos.

2.4. Administración y gestión de cuentas de usuario

a) Autorización y aprobación de cuentas de usuario
- Toda nueva cuenta de usuario Corfo sólo podrá ser solicitada por la Subgerencia de Personas y Desarrollo, en el marco del proceso de contratación de este.
- Para un usuario externo, en el contexto de la gestión de un proyecto determinado, la creación de la cuenta será evaluada y autorizada por el jefe directo del usuario, quien hace de contraparte interna para el proyecto respectivo.
- La cuenta de usuario con el rol o perfil solicitado debe estar completamente alineada con las funciones desempeñadas por éste. En caso de que sea solicitada una cuenta de usuario con un perfil o rol distinto a las funciones desempeñadas, se creará como una excepción, las que serán evaluadas y gestionadas por la Unidad Continuidad Operativa o la Unidad de Servicios Tecnológicos, dependiendo del alcance del requerimiento.
- En caso de que el jefe directo del usuario no se encuentre disponible, la autorización podrá ser realizada, en primera instancia por quien lo subrogue, de acuerdo con la ley o a lo establecido en las subrogancias.

b) Análisis y definición de la clasificación de un rol o perfil en un nivel de seguridad

Para cada rol o perfil de un sistema se deberá:

- Clasificar el rol o perfil en un nivel de seguridad de acuerdo al alcance funcional y de configuración que dicho rol o perfil posea dentro del sistema (Ejemplo: El rol administrador tiene acceso a toda la información del sistema, puede crear, editar y eliminar usuarios).
- Definir condiciones especiales (ejemplo: Tener asignado sólo un usuario).
- Comunicar al área usuaria el proceso de creación de cuenta de usuarios y la clasificación de los perfiles.

De acuerdo a lo anterior, los lineamientos para realizar este procedimiento son los siguientes:

- La Unidad Continuidad Operativa, o la Unidad de Servicios Tecnológicos, son las únicas habilitadas para ejecutar la clasificación de roles o perfiles en los niveles de seguridad, ya sea a nivel de plataforma y/o sistema aplicativo.

- En caso de que el área usuaria no esté de acuerdo con la clasificación, podrá enviar un correo para reponer esta decisión, o para realizar una evaluación de la clasificación.

- Todo rol o perfil que sea creado en un sistema deberá ser establecido en un nivel de seguridad. En caso de no efectuarse esta acción, no podrán ser creadas o modificadas las cuentas de usuario que requieran utilizar este perfil o rol.
- Cualquier excepción a las normas precedentes deberá ser tratada y gestionada por la Unidad de Continuidad Operativa.

c) Mantención de cuentas de usuarios

Se define como el proceso de monitorear, modificar y eliminar las cuentas de usuario.

- La Unidad de Continuidad Operativa es responsable de la mantención de las cuentas de usuario, operando siempre contra una solicitud desde la Subgerencia de Personas y Desarrollo, del jefe directo del funcionario, o contraparte técnica de un tercero, de creación, modificación o eliminación de cuentas. Sin perjuicio de lo anterior, en un escenario de contingencia será posible crear, modificar o deshabilitar cuentas de usuario sin una solicitud, situación que quedará publicada en el registro de gestión de cuentas de usuario.
- Periódicamente se debe realizar un análisis de las cuentas vigentes para deshabilitar cuentas de usuario de funcionarios que ya no tenga vínculo con la Institución.

d) Eliminación de cuentas de usuarios

La eliminación de cuentas de usuario puede ser realizada en las siguientes circunstancias:

- A expresa petición de la Subgerencia de Personas y Desarrollo, como canal oficial, atendida la solicitud que efectúe de la Jefatura o de la contraparte técnica, según corresponda.
- En caso de que la cuenta no haya sido utilizada en los últimos tres meses, previo visto bueno de la Subgerencia de Personas y Desarrollo.
- La eliminación de la cuenta será realizada por la Unidad de Continuidad Operativa.
- Cualquier excepción, fundada en una situación de caso fortuito o fuerza mayor, y que no se trate de los casos antes señalados, será evaluada y gestionada por el Gerente de Tecnología, pudiendo proceder o no a la eliminación de la cuenta.

CORFO

POLÍTICA DE ACCESO A INTERNET

El acceso a internet tanto de servicios de información como de usuarios debe ser controlado para evitar riesgos tecnológicos.

1. Objetivo

Definir restricciones de acceso a Internet para usuarios y servicios de información.

2. Definiciones

a) Los recursos computacionales asignados a cada usuario, en particular la estación de trabajo y el servicio de acceso a Internet, en cualquier horario, no deben ser utilizados para propósitos ajenos a sus actividades laborales.

b) No está permitida ninguna aplicación Peer to Peer (software para efectuar conexiones directas a otros computadores fuera de la red corporativa).

c) No está permitida ninguna aplicación de transmisión de contenidos on-line (música, videos, etc.), excepto aquellos autorizados expresamente por la Gerencia de Tecnología.

d) No está permitido bajar desde Internet o instalar programas del tipo freeware (software gratis) o shareware (software gratis por un tiempo), ni ningún tipo de software externo, a excepción de aquellos autorizados expresamente por la Gerencia de Tecnología.

e) Está permitido el acceso a sitios relacionados con redes sociales, chats, y otros similares, en los horarios definidos por la Gerencia de Tecnología.

f) No se permite publicar, exponer, cargar, distribuir o diseminar en la red corporativa de Corfo, cualquier contenido o información inapropiado, injurioso, difamatorio, infractor, obsceno, inmoral o ilegal.

g) Todo lo que no esté explícitamente aprobado o autorizado por esta Política o por la Gerencia de Tecnología, se encontrará bloqueado o prohibido.

POLÍTICA DE CORREO ELECTRÓNICO

El correo electrónico (e-mail) es una herramienta de comunicación, tanto al interior como al exterior de la Corporación, que requiere estrictas directrices para su uso, mantención y administración. Desde el punto de vista técnico, esta herramienta se encuentra compuesta por una plataforma –servidores, estaciones de trabajo y otros componentes– que está implícita en las normas de esta Política de Correo Electrónico.

1. Objetivo

Definir restricciones de uso de correo electrónico para usuarios de Corfo.

2. Definiciones

2.1. Uso del Correo Electrónico

a) Sólo las personas que trabajan para Corfo o sus Comités pueden hacer uso de la plataforma de correo electrónico.

b) El servicio está destinado para ser utilizado en materias relacionadas con las funciones del usuario.

c) Sólo se permite el software cliente establecido como estándar para el servicio de correo electrónico, de acuerdo a lo indicado por la Gerencia de Tecnología.

2.2. Obligaciones de los usuarios

a) El usuario es responsable de la información contenida en su buzón de correo.

b) Todo usuario debe ser consciente que la dirección del correo electrónico representa a la Corporación, y, por lo tanto, cualquier mensaje enviado por este medio conlleva la responsabilidad de dicha representación.

c) El servicio de correo electrónico puede ser utilizado para uso personal, siempre que el uso dado cumpla todas las siguientes condiciones copulativas: 1) no interfiera con las actividades de Corfo; 2) no se relacione a actividades comerciales y/o personales; 3) no comprometa la gestión e imagen corporativa de Corfo; y 4) no contenga, ni en su cuerpo o en archivos adjuntos, información de propiedad de Corfo o que se refiera a ella.

d) Los usuarios deberán reportar a la Gerencia de Tecnología la recepción de correos sospechosos (phishing)

2.3. Configuración de la estación de trabajo

a) La creación de casillas de correo se regirá por los lineamientos de gestión de cuentas de usuario definidas en la Política de Control de Acceso.

b) Las cuentas de correo tendrán distintos perfiles, de acuerdo al cargo, rol o dependencia del usuario, lo que puede derivar en privilegios especiales para determinados perfiles que requieran mayores funcionalidades para el desarrollo de su función.

c) Está prohibido modificar la configuración definida para el servicio de correo electrónico en la estación de trabajo.

2.4. Mensajes masivos

a) El envío de mensajes masivos a grupos o listas de destinatarios externos está restringido y será autorizado explícitamente por la Unidad de Continuidad Operativa.

b) Se prohíbe el envío de mensajes conocidos como "cadenas".

c) Se prohíbe expresamente los usos de técnicas de ataque a sistemas de correo electrónico, tanto internos como externos.

2.5. Prohibición de usar cuentas ajenas

a) Los usuarios tienen prohibido enviar o recibir mensajes electrónicos usando la identidad de otro usuario.

2.6. Restricciones al contenido de los mensajes

a) No se podrán incluir contenidos que eventualmente puedan comprometer el nombre de Corfo o que puedan dañar o provocar menoscabo en la imagen o prestigio de empresas, instituciones o personas.

b) Se encuentra prohibido:
- Enviar mensajes que infrinjan el ordenamiento jurídico, disposiciones contenidas en el Estatuto Administrativo, Código del Trabajo, y/o normativas internas.
- Enviar o reenviar mensajes, imágenes o videos que incluyan contenidos sexuales o que ofendan sobre la base del género, nacionalidad, orientación sexual, raza, religión, orientación política o discapacidad.
- Difundir softwares o links a través del correo electrónico.
- Enviar mensajes con contenido institucional de Corfo (información que sea de propiedad o relacionada con sus fines) a un usuario ajeno a la Corporación, cuando no se efectúe en ejercicio de las funciones propias del cargo, a excepción de que se cuente con autorización directa del jefe superior directo.
- Enviar o reenviar mensajes que contengan datos personales, sean de funcionarios de Corfo o de terceros relacionados con ella.
- La dirección de correo electrónico pertenece a la Corporación y ésta podrá acceder al contenido de los correos en cumplimiento de las normas legales y las dispuestas en esta Política. Es responsabilidad del usuario informar a sus contactos que no le envíen correspondencia no relacionada con su trabajo al correo que tiene asignado en Corfo.
- De esta manera, las partes entienden que toda comunicación recibida por el usuario en la cuenta de correo electrónico corporativo es de carácter laboral, sin perjuicio del respeto a su privacidad y el principio de inviolabilidad de las comunicaciones, de forma tal que el acceso a sus mensajes deberá efectuarse ante causales justificadas, mediante medios idóneos y proporcionales a los que se persiguen con la medida, situación que deberá ser autorizada por el Fiscal de Corfo, quien dará fe del cumplimiento de los requisitos precedentes.

2.7. Privacidad de los mensajes electrónicos

a) El correo electrónico debe ser considerado, desde el punto de vista del contenido del mensaje, como de mensajería insegura. Eso significa que no se debe incluir información sensible, a menos que el correo electrónico se envíe cifrado.

b) Está prohibido enviar, en cualquier parte del correo o en archivos adjuntos, información confidencial, reservada o secreta a personas no autorizadas a conocerla o poseerla.

c) Los usuarios no deben reenviar un mensaje electrónico a un destinatario externo a Corfo. Las excepciones a este punto son:
- Que este forward esté explícitamente autorizado,
- Que el remitente lo haya autorizado, o
- Que la información sea de naturaleza pública.

2.8. Manejo de espacio de almacenamiento

a) Los sistemas de correo electrónico centrales (carpetas públicas), no deben ser usados como bases de datos, debiendo, por lo tanto, descargar la información a los equipos personales.

b) Son excepción al punto anterior las asesorías que, por factibilidad técnica, no dispongan de un servicio de Internet permanente para la conexión del correo electrónico.

c) En caso de que el tamaño de un correo electrónico supere la capacidad de almacenamiento entregada por el sistema provisto de Corfo, deberá comunicarse esta situación a la Gerencia de Tecnología a fin de que autorice el uso de una herramienta alternativa que permita la recepción, envío o reenvío de estos correos.

2.9. De la Unidad de Continuidad Operativa

La Unidad de Continuidad Operativa es responsable de:

a) Definir o establecer el software cliente establecido como estándar para el servicio de correo electrónico.

b) Definir o establecer la configuración definida para el servicio de correo electrónico en la estación de trabajo.

c) Autorizar el envío de mensajes masivos a grupos o listas de destinatarios externos.

d) Habilitar los mecanismos tecnológicos a su alcance para prevenir ataques a la plataforma de correos.

e) Autorizar un software que sea permitido difundir a través de correo electrónico.

f) Implementar herramientas para filtrado de correo basura (Spam).

g) Implementar habilitar un sistema de cifrado para los usuarios que lo requieran.

h) Entregar a los usuarios herramientas que permitan enviar, recibir o reenviar correos que superen la capacidad de almacenamiento del software de correo electrónico institucional.

POLÍTICA DE ANTIVIRUS

El sistema de software antivirus es una herramienta de control permanente de contención de virus computacionales para la red y estaciones de trabajo.

1. Objetivo

Asegurar que los activos de información de Corfo cuenten con protección ante virus o malware.

2. Definiciones

2.1. Antivirus en estaciones de trabajo

a) La Gerencia de Tecnología deberá definir como estándar corporativo un producto de software antivirus oficial y único que dé cumplimiento a las leyes y normas vigentes.

b) Toda estación de trabajo deberá contar con un producto antivirus instalado y actualizado en su versión de software y en los patrones de búsqueda de virus.

c) Se deberá establecer un proceso central y automatizado de dichas actualizaciones.

d) Se deberá establecer un mecanismo alternativo, en caso de falla del primero para actualizar el software antivirus en forma manual, cuando este proceso no pueda efectuarse en forma centralizada y automática.

2.2. Protección antivirus de estaciones portátiles

a) Los computadores portátiles deberán configurarse para actualizar software y patrones de virus en forma automática al conectarse a la red de Corfo.

b) Los equipos remotos autorizados que operan en conexión esporádica se deberán considerar como equipos portátiles para su actualización.

2.3. Configuraciones en estaciones de trabajo

Como regla general, el software antivirus deberá configurarse como mínimo para que:

a) Se active en forma automática y permanezca siempre activo en la estación de trabajo, sea estacionaria o portátil.

b) Notifique el evento e impida la propagación en caso de detección de un virus.

c) En la partida efectúe revisión en archivos de sistema, área de inicialización (master boot), y memoria.

d) Revise en forma automática cualquier medio de almacenamiento removible que se intente leer o grabar, en los correspondientes dispositivos de la estación.

e) Toda detección positiva de virus debe ser registrada.

Una vez instalado y configurado el software antivirus, el usuario tendrá las siguientes prohibiciones:

a) No podrá cambiar la configuración o deshabilitar el software antivirus, sin la debida autorización y ésta debe ser otorgada sólo en forma temporal y justificada.

b) No podrá utilizar herramientas que impidan o bloqueen la normal funcionalidad del software antivirus.

2.4. Protección a nivel de red

a) Se deberá instalar y configurar un servicio o esquema de antivirus a nivel de red que proteja el servicio de navegación en Internet.

2.5. Acciones de protección de virus

a) Todo archivo, independiente de su origen o transporte, deberá ser verificado por el software antivirus antes de su uso.

b) Todo medio de almacenamiento recibido desde el exterior deberá ser considerado inseguro, y, por lo tanto, debe ser verificado por el software antivirus antes de su uso.

2.6. Servicio de alertas

a) Corfo deberá estar permanentemente suscrita a un servicio de alertas y actualizaciones del software y patrones de virus informáticos.

b) La Unidad de Continuidad Operativa definirá un responsable de las acciones relativas al software de antivirus, con su correspondiente respaldo.

c) Actualizar el software antivirus cada vez que el fabricante provea nuevas versiones y estar preparado para ejecutar actualizaciones de emergencia.

d) La Unidad de Continuidad Operativa establecerá un mecanismo de verificación manual alternativo en caso de fallas o discontinuidad del sistema de alertas.

CORFO

POLÍTICA DE RESPALDO

La protección en contra de la pérdida de datos es un componente importante para el Plan de Continuidad del Negocio.

1. Objetivo

Todos los datos y software críticos residentes en los servidores de Corfo deberán ser respaldados periódicamente, con la frecuencia que permita soportar las situaciones de contingencia posibles. Asimismo, los registros críticos deben ser conservados y retenidos por el tiempo establecido en el número 2.2 de esta Política, y se debe garantizar su destrucción una vez caducados.

Las actividades de respaldo, retención y eliminación de información son permanentes y su cumplimiento deberá ser controlado.

2. Definiciones

2.1. Servidores y estaciones de trabajo

a) La información contenida en los servidores de Corfo será respaldada periódicamente.

b) La información contenida en las estaciones de trabajo no se respaldará en forma centralizada, sólo a solicitud de los usuarios.

c) Toda la información sensible de Corfo deberá ser almacenada en sus servidores. Los usuarios podrán utilizar carpetas compartidas en la red corporativa, repositorios documentales u otros sistemas similares disponibles en la plataforma corporativa, para almacenar sus archivos locales que no son parte de un sistema central contenido en un servidor, siempre y cuando no se trate de información sensible, confidencial, reservada o que se encuentre sujeta a cualquier tipo de comunicación y/o transmisión por el ordenamiento jurídico.

d) El administrador de plataforma, de la Unidad de Continuidad Operativa, deberá realizar los respaldos periódicos y mantener un inventario de la información respaldada y almacenada externamente.

e) El encargado de inventario deberá verificar que los elementos que se desechen (computadores o medios de respaldo) no contengan información de Corfo antes de entregarlos al exterior.

f) Deberá existir un procedimiento o instructivo destinado a la destrucción de medios físicos de almacenamiento cuando éstos dejan de ser necesarios o presenten fallas, y para el borrado de información en los equipos.

2.2. Frecuencia y tipo de respaldo

a) Deberá existir un estándar que defina los tipos de respaldos que pueden ser utilizados para proteger la información magnética que utiliza Corfo.

b) Para prevenir pérdidas accidentales, todos los archivos, bases de datos e información existente en los sistemas centrales de Corfo, se deberán respaldar en dispositivos de almacenamiento externo.

c) Las solicitudes especiales de respaldo deben contar con la autorización de la Unidad de Continuidad Operativa.

d) La Unidad de Continuidad Operativa deberá definir e implementar los procedimientos para el respaldo de todas las plataformas tecnológicas.

2.3. Medios de almacenamiento

a) Los archivos, bases de datos e información existente en los sistemas centrales, se respaldarán a cinta, DLT (Digital Linear Tape), disco u otro medio similar.

b) Toda información crítica almacenada en algún medio de respaldo por un lapso de tiempo prolongado deberá ser sometida a pruebas de recuperación, en forma selectiva, al menos cada seis meses.

c) Toda información crítica almacenada en algún medio de respaldo que se encuentre próxima a la fecha de vencimiento, según la recomendación del fabricante, que además tenga un período de vigencia mayor, deberá ser traspasado a un medio nuevo, eliminando el anterior una vez validada la copia.

d) Las mismas medidas anteriores deberán ser consideradas ante un cambio tecnológico en los medios de respaldo que pueda generar obsolescencia tecnológica en los medios de respaldos existentes.

2.4. Almacenamiento histórico

a) El respaldo de datos y software críticos se deberá almacenar en un lugar protegido, con acceso controlado, el que no deberá encontrarse en el mismo sitio donde se ubican los servidores centrales.

b) El Administrador de Plataforma deberá mantener un inventario actualizado de la información almacenada externamente, de acuerdo al procedimiento definido por la Unidad de Continuidad Operativa.

2.5. Resguardo en el traslado de los medios de respaldo

a) Para prevenir la fuga de información, especialmente aquella definida como crítica, ésta deberá ser grabada en respaldos (cintas, DLT, cartuchos, etc.), los que serán almacenados fuera de las dependencias de Corfo. Asimismo, esta información deberá ser trasladada con los elementos de seguridad que garanticen su integridad, de modo de caucionar su seguridad ante intentos de acceso físico no autorizado.

b) Todo almacenamiento fuera de las dependencias de Corfo deberá cumplir con los siguientes requerimientos:

- Acuerdo de no divulgación de información (NDA) suscrito entre Corfo y el tercero encargado de la custodia de los medios.

- Que el lugar de almacenamiento se encuentre en Chile o en otro país que asegure el cumplimiento de estándares de seguridad iguales o superiores a los requeridos por nuestro ordenamiento jurídico, y que cuente con condiciones de seguridad de las instalaciones (físicas y lógicas), incluyendo condiciones ambientales, que aseguren la integridad, confidencialidad y seguridad de la información.

- Transporte seguro de los medios.

- Obligación de eliminación de la información y sus soportes al término de la contratación.

2.6. Rotación de respaldos

a) La retención de la información magnética se define como estándar de seis años.

b) Todos los datos técnicos, financieros, contables, legales y tributarios, deberán ser retenidos por el plazo que indique la normativa y leyes vigentes.

2.7. Destrucción de información

a) Toda información respaldada que pierda vigencia será borrada del medio que la contiene.

b) Previo a que un servidor o medio de almacenamiento sea reasignado, dado de baja o donado, deberá ser examinado por el Administrador de Plataforma para comprobar que toda la información sensible ha sido borrada, siguiendo el debido protocolo de limpieza y borrado seguro.

c) La destrucción de medios físicos de almacenamiento que contienen información sensible deberá ser gestionada por el Administrador de Plataforma.

d) Toda información confidencial en vías de ser destruida debe estar protegida contra accesos no autorizados, a la espera de su posterior retiro por parte del personal calificado.

POLÍTICA DE USO DE EQUIPOS DE COMUNICACIÓN MÓVIL Y PERIFÉRICOS COMPUTACIONALES

Los equipos de comunicación móvil y periféricos computacionales son parte del universo tecnológico de Corfo, y por su condición de contenedores de información y elementos de conectividad con la red corporativa, deben ser tratados adecuadamente para el cumplimiento de las Políticas Informáticas y Seguridad de la Información de Corfo.

1. Objetivo

Protección de seguridad de la información para equipamiento tales como: smartphones, celulares, e-token y pendrives de propiedad de Corfo, o estén arrendados por ésta, que son entregados a una de las personas que trabajan en Corfo (el usuario) en calidad de comodato, con el objeto de utilizarlo para el cumplimiento de los fines y objetivos propios de la Corporación, optimizando de esta manera el cumplimiento de las funciones inherentes a su cargo, rol o dependencia.

2. Definiciones

2.1. Restricciones

Para los teléfonos celulares y smartphones, contratados por Corfo y entregados en comodato para el uso de sus funcionarios, se aplicará la "Política de Telefonía Móvil de Corfo", aprobada por Resolución (E) N° 1.701, de 2015, de Corfo, en concordancia con lo establecido en el Instructivo Presidencial N° 2, de 4 de abril de 2018, de la Presidencia de la República, que versa sobre "Austeridad y Eficiencia en el Uso de los Recursos Públicos".

Para los otros dispositivos las restricciones y/o condiciones de uso aplicadas son las enumeradas a continuación:

a) El usuario está obligado a emplear la máxima diligencia en el cuidado del equipo o periférico que le fuere asignado para el cumplimiento de las funciones inherentes a su cargo, rol o dependencia.

b) El equipo o periférico será entregado al usuario junto con un formulario de asignación, documento en el cual se referenciarán, entre otros detalles, las

características técnicas, de identificación, y el valor comercial del dispositivo asignado, dejando constancia expresa que el funcionario ha leído, entendido y aceptado, en todas sus partes, las condiciones estipuladas y convenidas en el documento, confirmándolo con su firma.

c) En caso de extravío, robo, hurto o destrucción del equipamiento, el usuario responsable deberá informar, por escrito, a la Gerencia de Administración y Finanzas y a la Subgerencia Legal, con copia a la Gerencia de Tecnología, en un plazo no mayor a un día hábil después de ocurrido el hecho y dejar constancia en Carabineros de Chile, cuando corresponda. La Subgerencia Legal iniciarán el procedimiento administrativo que corresponda para determinar las responsabilidades y sanciones, si corresponden. En caso que el funcionario no realice ninguna de las acciones antes descritas en tiempo y forma, será responsable de la restitución del equipo.

d) El usuario estará obligado a restituir el equipo o periférico entregado en comodato cuando así lo solicite la Corporación, o cuando deje de prestar servicios a la Institución. La devolución del equipo o periférico será respaldada mediante un documento de entrega o desasignación, en el cual se registrarán todas las observaciones que sean necesarias para describir el estado y/o condiciones de devolución.

e) En caso que el equipo o periférico sea devuelto en condiciones no operacionales y/o con claras evidencias de descuido en el uso del mismo, la Corporación podrá exigir al usuario la restitución del bien, aplicando los criterios mencionados en los literales anteriores. La Gerencia de Tecnología será la encargada de verificar las condiciones de devolución de los equipos o periféricos entregados en comodato.

2.2. Recomendaciones

a) Evitar guardar el equipo o periférico en el mismo bolsillo donde transporta monedas, llaves, o cualquier objeto metálico que pueda dañar físicamente la pantalla, teclado u otro componente del dispositivo.

b) Cualquier otro dispositivo electrónico de bolsillo, como reproductores de música, agendas electrónicas o celulares, que posean una batería, pueden afectar la calidad de la señal del equipo, e incluso, dañar su sistema operativo.

c) No guardar el equipo o periférico en el bolsillo posterior de su pantalón, ya que cualquier tipo de presión que se ejerza sobre él puede dañarlo.

d) Evitar mojar o exponer el equipo o periférico a cualquier tipo de líquido. Si por alguna razón se moja, se deberá sacar inmediatamente la batería y recurrir a un servicio técnico autorizado y/o recomendado por Corfo a la brevedad.

e) Evitar exponer prolongadamente el equipo o periférico a radiaciones solares.

f) Evitar exponer el equipo a temperaturas extremas como hornos, parrillas, estufas, etc.

g) En caso de los equipos que requieren ser cargados (baterías), si se ocupa el cargador para vehículo, no dejar el equipo conectado a éste al apagar el motor, ya que la puesta en marcha del vehículo puede provocar un daño en la batería del dispositivo.

h) Si no posee el conocimiento necesario, no se debe intentar abrir el equipo o periférico por ningún motivo. En caso de que éste requiera limpieza, ésta se deberá realizar con un paño suave y seco.

i) No intente ocupar ningún accesorio que no sea compatible con el equipo, como audífonos, manos libres o cargadores, ya que los audífonos y manos libres puede dañar la entrada y salida de audio, y en el caso de los cargadores se puede dañar la batería.

j) En la medida en que sea posible mantener siempre el equipo en una funda compatible con su modelo.

POLÍTICA DE USO Y SEGURIDAD DE EQUIPAMIENTO COMPUTACIONAL FUERA DE CORFO

Los equipos computacionales, de propiedad de Corfo o arrendados por ésta, que sean utilizados fuera de las instalaciones de la Corporación, requieren definiciones aplicadas a su uso y seguridad.

1. Objetivo

Protección de seguridad de la información para equipamiento tales como notebook, data show, y equipos no portátiles utilizados en eventos (estaciones de trabajo e impresoras, generalmente), de propiedad de Corfo o arrendados por ésta, que sean facilitados a un funcionario en calidad de comodato (asignación temporal), con el objeto de utilizarlo para el cumplimiento de los fines y objetivos propios de la Corporación, optimizando de esta manera el cumplimiento de las funciones inherentes a su cargo, rol o dependencia.

2. Definiciones

2.1. Restricciones

a) El funcionario está obligado a emplear la máxima diligencia en el cuidado del equipamiento facilitado por Corfo. Se deberá extender el mismo nivel de cuidado exigido respecto del equipamiento utilizado al interior de la Corporación.

b) El equipamiento involucrado será entregado al funcionario junto a un formulario de asignación temporal, documento en el cual se referenciarán, entre otros detalles, las características técnicas y de identificación, y se dejará constancia expresa de que el funcionario ha leído, entendido y aceptado, en todas sus partes, las condiciones estipuladas y convenidas en el documento, confirmándolo con su firma.

c) El equipamiento involucrado puede incluir cables, control remoto, insumos, bolsos, mouse, teclados, parlantes, etc., los que serán de responsabilidad del funcionario al que se le ha asignado el equipo.

d) En caso de extravío, robo, hurto o destrucción del equipamiento, el funcionario responsable deberá informar, por escrito, a la Gerencia de Administración y Finanzas y a la Subgerencia Legal, con copia a la Gerencia de Tecnología, en un plazo no mayor a 1 día hábil después de ocurrido el hecho y dejar constancia en Carabineros de Chile, o Policía de Investigación de Chile (PDI), cuando corresponda. La Subgerencia Legal iniciará el procedimiento administrativo que corresponda para determinar las responsabilidades y sanciones, si corresponden.

e) El funcionario deberá devolver el equipamiento y todos los accesorios facilitados, en el plazo establecido al momento de realizar el requerimiento. La entrega del equipamiento será respaldada mediante un documento de entrega, en el cual se registrarán todas las observaciones que sean necesarias para describir el estado y/o condiciones de devolución.

f) En caso de que el equipamiento sea devuelto en condiciones no operacionales o con claras evidencias de descuido en el uso del mismo, la Corporación podrá exigir al funcionario la restitución del bien, en las condiciones en las que fue entregado, aplicando los criterios mencionados en los literales anteriores.

g) La Gerencia de Tecnología será la encargada de verificar las condiciones de entrega y/o devolución del equipamiento en el marco de la solicitud planteada.

2.2. Recomendaciones

a) Aun cuando el equipamiento deberá revisado y preparado en detalle antes de ser entregado, se encomienda revisar el equipo antes de sacarlo de las dependencias de Corfo para saber en qué condiciones se encuentra éste. En caso de encontrarse un detalle éste debe ser informado a la brevedad.

b) Al momento de ser transportado se deberán adoptar las medidas necesarias para que éste se encuentre seguro y no se dañe en el trayecto. Nunca se deben dejar los equipos al interior de vehículos que deban quedar estacionados en la vía pública o en espacios que no cuenten con medidas de seguridad.

c) Antes de realizar la instalación, es recomendable revisar todo el equipamiento y sus accesorios a fin de determinar si existe algún detalle producido en el transporte de éstos.

d) La instalación deberá ser efectuada por una persona capacitada en el uso y manejo de este tipo de equipamiento.

e) Nunca se deberán dejar los equipos en el suelo o donde transiten las personas, ya que puede generarse un accidente y, tanto la persona como el equipo, pueden resultar dañados.

f) No permitir que una persona sin autorización manipule los equipos.

g) Una vez finalizado el uso del equipamiento, éste deberá ser guardado en un lugar seguro o avisar al personal de seguridad del local que no permita la manipulación por personas ajenas mientras el funcionario responsable esté ausente.

h) Si por algún motivo se necesita una configuración especial deberá solicitarse asistencia técnica en el lugar donde se encuentra, pudiendo ser al personal encargado, técnico autorizado o el servicio de Mesa de Ayuda de Corfo. La configuración deberá efectuarse conforme a lo que le indica el personal encargado.

i) Si el equipo falla, por cualquier motivo, no se debe intentar su reparación o permitir que una persona no autorizada lo intervenga.

j) No permitir que dejen objetos que puedan producir algún daño a los equipos como cajas, objetos pesados, herramientas, líquidos, cables, etc.

k) No exponer los equipos al sol ni a temperaturas extremas. En caso que el evento sea al aire libre, instale el equipamiento en un lugar seguro, fresco y a la sombra.

l) Evitar mojar los equipos o exponerlos a condiciones riesgosas similares.

m) La desinstalación del equipamiento deberá efectuarla la misma persona que realizó la instalación, y en caso que no sea posible, por otra persona autorizada para ello.

n) Al momento de desinstalar se revisará la existencia de todos los accesorios y equipos de Corfo que fueron utilizados en el evento.

ñ) Cualquier detalle o problema que haya presentado el equipamiento debe ser informado, exponiendo la situación, el equipo involucrado y la consecuencia del detalle o problema.

o) No está permitido instalar softwares adicionales que no estén expresamente autorizados. Cualquier solicitud de equipos que involucre un software específico debe ser efectuarse junto al requerimiento.

p) No entregar a terceros, por ningún motivo, las claves de acceso a los equipos Corfo.

q) No dejar información de Corfo al alcance de personas no autorizadas, por lo que se deberán adoptar las medidas necesarias para evitar su visualización, manipulación, acceso no autorizado, adulteración y/o destrucción.

POLÍTICA DE ESCRITORIO Y PANTALLAS LIMPIAS

El mantener escritorios y pantallas limpias, además del control del equipo desatendido de usuarios, permite el disminuir el riesgo de fuga de información o accesos no autorizados.

1. Objetivo

Definir las reglas de uso y control que deben cumplirse para el cuidado y protección de la información en caso de acceso no autorizado.

2. Alcance

Toda aquella información de uso interno de la Institución que se muestre en pantallas, como aquella información impresa, escrita contenida en estaciones de trabajos, impresoras, salas y pizarras, o expuesta en otros medios.

3. Roles y responsabilidades

- **Jefaturas de áreas:** Velar por el cumplimiento de esta Política.

- **Gerente de Tecnología:** Definir e implementar las medidas de protección automatizados que apoyen esta Política.
- **Encargado de Seguridad de la Información:** Efectuar revisiones periódicas respecto al cumplimiento de esta Política.

- **Usuario:** Cumplir con las definiciones establecidas en esta Política.

4. Definiciones

4.1. Escritorios limpios

a) Los escritorios de los funcionarios que se encuentren zonas de atención, o tránsito de público, o cercanas a ellas, deberán estar ubicados de forma que la pantalla de la estación de trabajo no pueda ser vista por terceras personas.

b) En el caso de información en papel, ésta también deberá cumplir lo señalado en el párrafo precedente.

c) Ante una ausencia prolongada de su lugar de trabajo, o al finalizar la jornada laboral, todo funcionario deberá asegurarse que la información quede fuera del alcance de terceros, en lo posible guardada con llave, cuando se trate de documentos en papel o dispositivos físicos de almacenamiento (como pendrive), así como bloquear o apagar el equipo computacional.

4.2. Ubicación de escritorios y equipos computacionales

a) Los escritorios de los funcionarios de Corfo deberán ser ubicados de forma de evitar que la información con la que trabaja pueda ser visualizada o accedida por personas no autorizadas, protegiendo, de esta forma, además, el equipamiento.

b) Los escritorios que queden ubicados cerca o en zonas de atención o tránsito de público, deberán situarse de forma que las pantallas del computador y la información impresa que utiliza el funcionario no puedan ser visualizadas o accedidas por terceros no autorizados.

4.3. Protección de equipo de usuario desatendido

a) Todas las estaciones de trabajo deberán tener activada la función de protector de pantalla para que éste se active luego de unos minutos sin uso, ocultando la información del usuario y bloqueando el equipo. La reactivación debe requerir contraseña.

b) Independiente del bloqueo automático, es responsabilidad del funcionario bloquear manualmente su estación de trabajo cuando tenga una ausencia prolongada de su escritorio, evitando así exponer la información a terceras personas. Para desbloquearla, se requiere una contraseña.

4.4. Protección en impresoras

a) Las impresoras ubicadas en zonas de atención o tránsito de público, deberán quedar protegidas de accesos no autorizados.

b) Cualquier información impresa deberá ser retirada de ella en forma inmediata de la impresora, evitando así el acceso de personas no autorizadas.

c) Cuando sea posible, y se trate de información sensible, deberá implementarse el control de impresión con el uso de una contraseña por usuario.

4.5. Salas y pizarras limpias

a) Las salas o áreas de reuniones, salas de conferencias y de capacitación, deberán quedar limpias de todo el material utilizado.

b) Después de las reuniones en que se utilicen pizarras, éstas deberán quedar limpias de la información que se ha expuesto en ellas.

c) En el caso que se utilice una estación de trabajo para presentaciones, si éste fuera de uso común, debe eliminarse la información antes presentada.

CORFO

POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL

Se generan los lineamientos correspondientes para disminuir los riesgos de seguridad física y ambiental y así proteger las áreas que contienen los sistemas de información de Corfo.

1. Objetivo

Evitar accesos físicos no autorizados, daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información; así como evitar pérdida, daños, robo o compromiso de sus activos relevantes.

2. Definiciones

2.1. Seguridad física general

a) Los perímetros de seguridad deberán ser definidos por el Encargado de Seguridad Física, y la ubicación y la fuerza de cada uno de los perímetros deberá depender de seguridad de los activos dentro del perímetro y las mejores prácticas.

b) Se deberá contar con una zona de recepción atendida por una o más personas, u otros medios para controlar el acceso físico al lugar o edificio. El acceso a los sitios y edificios debe restringirse sólo al personal autorizado.

c) Se deberán implementar barreras físicas para impedir el acceso no autorizado y la contaminación ambiental.

d) Los perímetros críticos de seguridad deberán contar con alarmas, se deben monitorear y evaluar con relación al nivel de resistencia contra incendios.

e) Se deberán instalar sistemas de seguridad electrónica, los que serán probados regularmente para cubrir todas las puertas exteriores.

f) Las instalaciones de procesamiento de información que administra la organización deberán estar físicamente separadas de aquellas que son gestionadas por entidades externas.

g) La aplicación de controles físicos, en especial para las áreas seguras, se deberá adaptar a las circunstancias técnicas y económicas de la organización, según se establece en la evaluación de riesgos.

2.2. Seguridad física del data center

a) El data center es un recinto diseñado y pensado especialmente desde sus cimientos para dar servicios de infraestructura de tecnologías de información (alojamiento, operación, administración y monitoreo de soluciones tanto de comunicación como de dato).

b) Con una superficie total de 35 metros cuadrados, el data center de Corfo cuenta con servicios provistos de la más alta tecnología disponible y aplicación de buenas prácticas internacionales, con personal especializado capaz de mantener las comunicaciones y servicios de usuario de Arica a Punta Arenas.

c) La Unidad de Continuidad Operativa tiene, entre otras funciones, la de velar por la seguridad de la información allí almacenada.

d) Las autorizaciones para el ingreso al data center con el fin de realizar operaciones, revisión o actividad las efectuará el Gerente de Tecnología y el Jefe Unidad de Continuidad Operativa, y de ser necesario, se informará al Jefe de Seguridad de Corfo para que se otorguen los permisos y/o privilegios de acceso en los sistemas electrónicos implementados en Corfo, según corresponda.

e) Para las modificaciones de datos o sistemas, solicitadas por otras unidades, se debe utilizar el sistema de "Service Desk" para requerimientos. Esto permite realizar este tipo de actividades sin tener que contar con la presencia externa en el recinto.

f) El acceso físico a los servidores cuenta con una puerta de alta seguridad, cuyas llaves de acceso se entregan únicamente a las personas responsables de esta área, lo anterior se debe complementar con un sistema de cámaras CCTV, que son monitoreadas desde la Unidad de Seguridad y cuyas imágenes respaldadas, en conformidad a lo establecido en el Plan de Seguridad de Corfo (aprobado por Carabineros de Chile).

g) Sólo pueden ingresar las personas autorizadas en los términos señalados precedentemente.

CONTROLES DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN

Las actividades de auditoría son necesarias para evaluar la calidad (efectividad) de los controles implementados, a fin de evaluar su funcionamiento, identificar vulnerabilidades y mitigar los riesgos presentes en los procesos de una Institución, así como de sus unidades.

Estas auditorías deberán ser debidamente coordinadas con el Gerente de Tecnología, o con quien él designe en su representación, para no interferir en la operación normal ni generar riesgos en la misma, como tampoco riesgos a los activos de información de los procesos.

1. Objetivo

Establecer las definiciones de auditoría para el ámbito de Tecnologías de la Información (TI), función que abarca el seguimiento de los controles derivados de la Política Informática y de Seguridad de la Información de Corfo.

2. Definiciones

2.1. Planificación

Con el fin de reducir las interferencias al negocio y minimizar los riesgos que conlleva esta actividad, la Gerencia de Auditoría Interna o la entidad que corresponda, deberá coordinar las revisiones que implique la ejecución de la auditoría con la Gerencia de Tecnología, para lo que deberá ejecutar las siguientes acciones:

a) Formalizar los requerimientos de auditoría, así como la oportunidad y alcance en que se efectuarán las mediciones.

b) Identificar los tipos de acceso a la información, los cuales sólo serán de lectura.

c) En aquellos casos en que se requieran accesos que no sean sólo de lectura, éstos serán otorgados sobre una copia de los datos y deberán ser utilizados sólo para efectuar las acciones necesarias para la auditoría, respetando las normas de privacidad de la información y protección de datos personales. Estas copias deberán borradas al término del proceso de auditoría. Las excepciones deben ser justificadas con un estudio de factibilidad técnica y concordadas con el Gerente de Tecnología.

d) Identificar claramente los activos de información que se verán involucrados durante la ejecución de la auditoría.

e) Asegurar la disponibilidad y oportuna entrega de la información que sea requerida a fin de permitir el normal desarrollo de las revisiones.

2.2. Registro

Para controlar las posibles intervenciones producto de una auditoría, deberá mantenerse un registro, el cual deberá contener, al menos:

a) Actualizaciones a las bibliotecas de programas operativos.

b) Accesos a las bibliotecas de fuentes de programas.

c) Accesos físicos a las áreas críticas.

d) Accesos lógicos a sistemas, almacenes de datos y/o aplicaciones.

2.3. Ejecución

a) Para mover, trasladar o retirar cualquier recurso informático, se generará una autorización, la que debe quedar explícitamente registrada (en formularios, correos electrónicos, memorándum u otros medios equivalentes). El concepto de recurso informático incluye soportes informáticos extraíbles, tales como cintas, discos y/o documentos impresos.

b) El inventario de activos de la Información deberá identificar en su levantamiento las pistas de auditoría (audit trail/ audit log) que posee el dispositivo. Estas pistas de auditoría deben ser claramente calificadas, con los atributos de activos del inventario, por ejemplo: clasificación, propietario, medios, etc.

c) Las herramientas que se utilicen para ejecutar las auditorías de los sistemas de información deberán estar protegidas de posibles accesos no autorizados o de una eventual mala utilización, considerando disponer de un ambiente separado de los ambientes de desarrollo y producción, con autorizaciones de acceso solamente para el equipo de auditores.

2.4. Auditorías al sistema de gestión de la seguridad de la información

a) La implantación de la Política de Seguridad Informática y la Información, y sus Políticas derivadas, deberán tener revisiones independientes para evaluar su efectividad. Los intervalos dependerán de lo recomendado por las auditorías específicas que se definan.

b) Estas auditorías pueden ser realizadas por la Gerencia de Auditoría Interna o bien por medio de la contratación de una auditoría externa, debiendo siempre existir coordinación entre ambas a fin de asegurar una adecuada cobertura y así evitar sobreposiciones.

c) En particular, se deberán realizar auditorías para controlar el correcto retiro de equipamiento, así como la utilización de licencias de software al interior de la Institución. Estas auditorías deberán ser coordinadas con el personal

responsable, y deben utilizarse para verificar el cumplimiento de las directrices pertinentes, las cuales incluyen, entre otros:

- Autorización previa, y determinación de responsables de la autorización,
- Aplicación a equipos, software e información,
- Registro de salida y de retorno.

d) En los contratos celebrados por la Corporación con terceros a la Institución deberá incluirse, en la medida de su factibilidad legal, cláusulas que autoricen a Corfo a realizar auditorías al tercero, así como acuerdos de confidencialidad (NDA) y protección de la información. Además, deberán incluirse las normas de la Política de Seguridad en la Relación con Proveedores.

e) Deberán considerarse la realización de revisiones a los servicios prestados por terceros que estén relacionados con activos de información. La ejecución de estas revisiones no excluye la obligación de la Gerencia de Tecnología de disponer de un monitoreo permanente sobre éstos.

POLÍTICA DE SEGURIDAD EN LA RELACIÓN CON PROVEEDORES

Ante la introducción de un servicio o producto externo, se debe procurar que la información de Corfo mantenga su confidencialidad, integridad y disponibilidad. Asimismo, se deberá asegurar que las instalaciones de procesamiento de la información no se verán afectadas.

1. Objetivo

Los lineamientos de esta Política se orientan a garantizar la protección de los activos de información sensibles de Corfo, cuando sean accesibles por los proveedores externos de servicios o productos.

Los presentes lineamientos entregan los requisitos de seguridad de la información orientados a mitigar los riesgos asociables al acceso de dichos proveedores, los que se deberán documentar adecuadamente.

2. Seguridad en los contratos con proveedores

a) En su texto se deberán regular claramente las responsabilidades relativas al nivel y medidas de seguridad que los proveedores aceptan al momento de celebrar un contrato.

b) Las relaciones de prestación de servicios con proveedores que impliquen el acceso, captura, almacenamiento, transporte, comunicación, procesamiento y/o entrega de información, deberán estar explícitamente reguladas en el respectivo contrato, indicando la obligación del proveedor de adoptar los controles de seguridad pertinentes, así como el acatamiento y cumplimiento de las Políticas Informáticas y de Seguridad de la Información de Corfo y sus Políticas accesorias, y las normas legales y reglamentarias que se apliquen a la ejecución del servicio.

c) El contrato deberá definir con claridad el tipo de información involucrada, la naturaleza de su manipulación y el propósito para estos actos, procurando restringir el uso y disposición de ésta a los mínimos necesarios para la correcta prestación de los servicios, la prohibición de efectuar copias y la obligación de

borrar ésta al término del contrato. La información se entregará en modo de lectura, a menos que sea necesaria su manipulación para prestar el servicio contratado.

d) Los servicios de proveedores que proporcionan componentes de infraestructura de TI deberán estar explícitamente regulados en el contrato del servicio, indicando la obligación del proveedor de adoptar los controles de seguridad pertinentes, así como el cumplimiento de la Política Informática y de Seguridad de la Información de Corfo, sus Políticas anexas, y las normas legales y reglamentarias pertinentes.

e) Corfo deberá asegurar la protección de los derechos de propiedad intelectual que le correspondan respecto de los productos entregados por el proveedor.

f) Las Políticas Informáticas y de la Seguridad de la Información de Corfo y sus Políticas anexas formarán parte integrante de los respectivos contratos para todos los efectos legales.

3. Definiciones en la relación con proveedores

En todo contrato, Orden de Compra u otro instrumento que regule la prestación de servicios se debe considerar, al menos, los siguientes puntos:

a) Definir un administrador del servicio (Encargado de Contrato de Corfo) y una Contraparte del proveedor. El Encargado de Contrato de Corfo será responsable, entre otras funciones, de administrar los cambios, medir el cumplimiento de los niveles de servicios (SLA), cumplimiento de los acuerdos de confidencialidad y aplicar las multas que correspondan o informar la procedencia del término anticipado del contrato por incumplimiento grave de las obligaciones contractuales.

b) En caso de corresponder se deberán formalizar Acuerdos de Confidencialidad y de no divulgación (NDA), tanto con el proveedor (en forma directa), como con sus funcionarios y terceros relacionados (en forma indirecta), los que deberán adecuarse al marco legal vigente.

c) Definir el nivel y calidad del servicio, indicando que éstos serán medidos y evaluados por Corfo, establecimiento de niveles de servicios y multas asociadas.

d) Definir escenarios de contingencia si el servicio prestado así lo requiriese, tanto si ésta ocurre en dependencias de Corfo como si ocurriesen en dependencias o en el ámbito de acción exclusivo del proveedor, así como medidas de contingencia.

e) Formalizar la adhesión a las Políticas Informáticas y de Seguridad de la Información de Corfo y sus Políticas anexas.

f) Incluir, en la medida en que su factibilidad técnica, comercial y legal lo permitan, cláusulas que autoricen a Corfo a realizar auditorías al proveedor.

g) Regular las relaciones del proveedor con subcontratistas, y limitar la responsabilidad de sus actos al proveedor.

4. Controles y procedimientos en la relación con proveedores

a) Corfo, a través de la Gerencia de Tecnología o la Gerencia de Administración y Finanzas, cuando corresponda, deberá establecer los controles de acceso físicos y lógicos necesarios para proteger los activos de información de la manipulación no autorizada por parte del proveedor. Estos controles deberán considerar, al menos, la indebida lectura, modificación, transporte, divulgación o destrucción de la información.

b) El proveedor deberá conocer y acatar los procedimientos de manejo de incidentes de seguridad de la información de Corfo.

c) Se debe realizar la devolución o la destrucción de todos los activos de información por parte del proveedor una vez finalizada la actividad externa, el hito de ejecución de un proyecto o del servicio total.

d) El proveedor deberá adscribir a los acuerdos de continuidad del negocio ante situaciones de crisis, así como de gestión de incidentes, capacidad de recuperación, realización copias de seguridad y recuperación de desastres (DRP), cada vez que el servicio otorgado esté relacionado con activos o procesos que forman parte de las situaciones o planes mencionados en el número 1 de estas Políticas.

e) El proveedor será responsable de capacitar a todo el personal destinado a la prestación del servicio contratado en las Políticas y procedimientos de seguridad de la información que estén relacionados con su trabajo en Corfo. A su vez, Corfo, a través de la Gerencia de Tecnología, deberá entregar las directrices y el material para la inducción y capacitación requeridas.

f) Corfo, a través de la Gerencia de Tecnología, deberá establecer los requisitos para abordar los riesgos de seguridad de la información a los que la Institución está expuesta ante escenarios que impliquen trastornos o fallas en la cadena de suministro de los servicios o de los productos provistos por el proveedor. Estas situaciones deben regularse en el contrato.

5. Supervisión, gestión de cambios y revisión de los servicios del proveedor

a) Corfo, a través de la Gerencia de Tecnología y/o la Gerencia de Administración y Finanzas, cuando corresponda, deberá establecer un monitoreo regular y permanente, además de revisiones periódicas de los servicios prestados, de tal forma que se pueda asegurar el cumplimiento de los términos y condiciones de la seguridad de la información de los servicios acordados en los contratos respectivos.

b) Como se indicó en el número 3 de estas Políticas, el proveedor deberá designar a una persona (Contraparte), quien actuará como su representante válido ante Corfo en la ejecución de los servicios, y será responsable de revisar el cumplimiento de las obligaciones establecidas en el respectivo contrato.

c) Corfo, a través de la Gerencia de Tecnología y/o la Gerencia de Administración y Finanzas, cuando corresponda, deberá revisar los incidentes o eventos de seguridad de la información que se hayan producido o que puedan presentarse en la prestación del servicio, a fin de validar que se están manejando de manera apropiada por parte del proveedor.

d) Se deberá asegurar que, ante un cambio en las condiciones bajo las que se brinda el servicio, exista un proceso que permita manejar estos cambios de manera adecuada y que no se está afectando la seguridad de la información.

e) Ante cambios en las condiciones de entrega del servicio, se deberá realizar una actualización de la evaluación de riesgos. Esto permitirá realizar los ajustes necesarios a las medidas de control y monitoreo de seguridad establecidos para el servicio prestado.

f) Corfo, a través de la Gerencia de Tecnología y/o la Gerencia de Administración y Finanzas, cuando corresponda, deberá velar por el cumplimiento de los procedimientos y acciones que correspondan por el término del contrato (devolución de antecedentes, borrado de información, cancelación de permisos, etc.).

POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

Corfo define, a continuación, su Política de Privacidad y Protección de Datos Personales de la organización para la privacidad y protección de información de identificación personal.

1. Objetivo

Definir el tratamiento de la información de identificación personal que se alinea con lo dispuesto en la Ley N° 19.628 sobre Protección de la Vida Privada y su Reglamento, aprobado por el Decreto N° 799, de 2000, del Ministerio de Justicia.

2. Implementación de la Política

Corfo, como parte de su proceso de gestión de la seguridad de la información, define esta Política de Protección de Datos de Carácter Personal, la que tiene por objeto que el personal encargado del manejo de datos personales conozca lo establecido en la Ley N° 19.628 sobre Protección de la Vida Privada. Conforme lo anterior se define:

a) La Gerencia de Tecnología deberá realizar, en conjunto con Fiscalía de Corfo, anualmente o cuando sea necesario, la revisión de la Ley y N° 19.628 e identificar cambios o nuevos lineamientos en relación a la regulación de la protección de datos personales.

b) La Gerencia de Tecnología deberá solicitar a las diferentes áreas y gerencias de Corfo la identificación de los funcionarios que, como parte de su gestión, manejen datos personales regulados por la Ley N° 19.628.

c) La Gerencia de Tecnología deberá realizar, en conjunto con Fiscalía de Corfo, un entrenamiento anual a los funcionarios identificados en el punto anterior.

d) La Gerencia de Tecnología deberá levantar la información de carácter personal que es manejada por cada funcionario, cuál es el origen de estos datos y la finalidad que justifica su tratamiento.

3. Privacidad y protección de información de identificación personal

Corfo define a continuación su Política de Privacidad y Protección Datos Personales, velando por la privacidad y protección de este tipo de información.

a) Corfo identificará y buscará medios para cumplir lo indicado en la Ley N° 19.628.

b) Los funcionarios de Corfo serán instruidos sobre las normas de dicha ley y deberán seguir los principios de ésta.

c) Toda persona que preste servicios para o en Corfo, sea funcionario o tercero, que maneje información de carácter personal, reportará esta situación al Encargado de Seguridad de la Información.

d) Los funcionarios y terceros que manejen datos personales asistirán a un entrenamiento anual orientado a conocer los lineamientos sobre esta materia.

4. Sitio web

a) Toda información personal que sea requerida en el sitio web de Corfo, bajo ninguna circunstancia será compartida con terceros, con la sola excepción de los casos en que esto sea autorizado por el ordenamiento jurídico.

b) Corfo no es responsable de los contenidos o prácticas de seguridad de los sitios enlazados desde la página web institucional.

c) Dada la falta de autoridad para modificar o auditar contenidos y procedimientos de los sitios web externos, Corfo no avalará los productos, servicios, políticas y contenidos utilizados en dichos sitios.

d) El sitio web corporativo deberá ser protegido con medidas de seguridad, tales como procedimientos de control de cambios, contraseña y controles de acceso físico.

e) Se deberán emplear las mejores prácticas para prevenir que los datos personales de los usuarios sean extraviados, mal utilizados o modificados inapropiadamente, así como el acceso no autorizado.

f) Si el titular del dato personal que figura en un sitio web desea rectificar o corregir los datos personales que eventualmente pudiera haber ingresado, Corfo proveerá de los procedimientos para estos efectos.

POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Ante incidentes de seguridad de la información se deben identificar responsabilidades y la correcta gestión para asegurar la mejor respuesta según las prioridades de Corfo.

1. Objetivo

Garantizar que los eventos de seguridad de la información y las vulnerabilidades asociadas a los sistemas de información sean atendidos de manera eficaz y oportuna, sin importar si estos provienen de vulnerabilidad internas de la red institucional o se deben a la acción de terceros ajenos a ella.

2. Definiciones

2.1. Atención de incidentes

a) Los eventos de seguridad de la información y las debilidades asociadas a los sistemas de información deberán ser atendidos de manera eficaz y oportuna.

b) Se deberán establecer responsabilidades y procedimientos formales para la detección, reporte, manejo e informe posterior de los incidentes de seguridad de la información.

2.2. Tipos de incidentes

a) Se deben definir procedimientos para los distintos tipos de incidentes, los cuales deberán estar previamente catalogados.

b) Se deberá utilizar una pauta de reacción a incidentes conocidos.

2.3. Informe de incidentes de seguridad

a) Todo funcionario de Corfo, prestador de servicios y/o terceros que tengan acceso a los sistemas de Corfo, es responsable de informar, mediante el canal que sea definido por la Gerencia de Tecnología, a la brevedad, los eventos de seguridad de la información que afecten o puedan afectar activos de información, considerando las prioridades de la Corporación.

b) La Gerencia de Tecnología deberá definirse un canal para realizar los reportes de incidentes, el que deberá ser conocido por todas las personas que eventualmente puedan informarlos. Cuando lo amerite, se debe definir un canal alternativo.

c) La Gerencia de Tecnología deberá definir los tiempos máximos de reporte de incidentes.

d) Todos los incidentes de ciberseguridad deberán ser informados al CSIRT del Gobierno. Para estos efectos, el Encargado de Ciberseguridad de Corfo, en conjunto con el Encargado de Seguridad de la Información de Corfo, deberán establecer los canales para la notificación interna de esta clase de incidentes y su comunicación al CSIRT.

2.4. Registro del incidente

a) Se deberá mantener un registro (electrónico y/o manual) de los incidentes reportados, con su adecuado seguimiento de estado y mejora.

b) Se deberán definir en el registro los diferentes estados que puede tener un incidente, desde su declaración como tal, hasta su cierre y los aprendizajes obtenidos.

2.5. Evaluación e identificación del incidente

a) Todo tipo de incidente deberá ser identificado y ponderado en su grado de impacto a los activos de información de Corfo.

b) El grado de impacto deberá determinar la prioridad del tratamiento y la necesidad de activar o no planes de continuidad apropiados.

c) Como parte de la evaluación deberá considerarse la recolección de evidencias y su resguardo.

2.6. Respuesta al incidente

a) Dependiendo de la identificación del tipo de incidente y la severidad del mismo, se deberá proceder a activar al equipo de respuesta correspondiente.

b) Deberá existir un proceso definido para las acciones que debe tomar el equipo de respuesta.

c) El equipo de respuesta antes incidentes que tome el caso deberá liderar la ejecución de las acciones de solución y validar ésta.

2.7. Aprendizaje del incidente y mejoras

a) Una vez superado el incidente, deberán ser analizadas las posibles causas que lo generaron a fin de definir, en caso que corresponda, las acciones preventivas a ejecutar y la implementación de nuevos controles.

b) Se deberá evaluar la calidad y efectividad de los procedimientos utilizados.

POLÍTICA DE GESTIÓN DE VULNERABILIDADES TÉCNICAS

La gestión de vulnerabilidades técnicas permite una reducción de los riesgos de los sistemas de información de Corfo, obteniendo información oportuna que permita adoptar las medidas correspondientes para afrontar el riesgo asociado.

1. Objetivo

Detectar en forma oportuna las vulnerabilidades técnicas de los sistemas de información utilizados por Corfo, evaluando la exposición a éstas, y adoptando las medidas apropiadas para abordar el riesgo asociado y no afectar los objetivos de negocio.

2. Definiciones

2.1. Gestión de vulnerabilidades

El proceso de gestión debe comprender las siguientes actividades:

a) Mantención de una Política de Gestión de Vulnerabilidades.

b) Descubrimiento o "escaneo" de vulnerabilidades sobre los activos tecnológicos de Corfo.

c) Realización de evaluaciones y pruebas de seguridad periódicas.

d) Análisis y evaluación del nivel de seguridad actual y la priorización de vulnerabilidades, según su nivel de amenaza e impacto al negocio.

e) Efectuar acciones de mitigación de las vulnerabilidades detectadas.

2.2. Controles preventivos

a) La Gerencia de Tecnología deberá disponer de un inventario de activos, actual y completo, para asegurar la correcta gestión de vulnerabilidades.

b) Todo elemento relevante de la plataforma tecnológica de Corfo, deberá contar con contrato vigente de soporte y mantención, con los correspondientes acuerdos de nivel de servicio y multas y sanciones contractuales asociadas.

c) Los cambios derivados de modificaciones a las configuraciones o la instalación de actualizaciones y/o mejoras que sean realizados o afecten a elementos de la plataforma tecnológica de Corfo, deberán considerar el descubrimiento o "escaneo" de vulnerabilidades sobre los elementos afectados por el cambio.

d) De acuerdo a lo dispuesto en la Circular N° 12, de 2019, de la Vicepresidencia Ejecutiva de Corfo, la instalación de cualquier elemento de software corresponderá sólo a aquel que ha sido autorizado explícitamente para su utilización en Corfo y cumplir con los requerimientos de seguridad establecidos por el proveedor o fabricante.

e) Se deberá establecer y gestionar el inventario de todos los componentes de la plataforma tecnológica de Corfo, incluyendo los sistemas de información.

2.3. Revisiones de vulnerabilidades

a) Todas las actividades de detección de vulnerabilidades deberán ser planificadas y estar regidas por procedimientos formales.

b) Se deberán realizar revisiones de vulnerabilidad, al menos una vez al año, que permitan validar la correcta gestión de este proceso a realizar sobre plataforma tecnológica.

c) Los terceros que realicen la evaluación, deberán someterse a las disposiciones legales y contractuales definidas por Corfo.

d) Según lo requieran eventos particulares efectuados sobre la plataforma, se deberán realizar acciones de revisión interna de vulnerabilidades.

2.4. Evaluación de vulnerabilidades

La evaluación de vulnerabilidades debe considerar, entre otros:

a) La configuración de dispositivos y sistemas para verificar que éstos se encuentran configurados de acuerdo con los estándares de seguridad definidos por Corfo.

b) La instalación de "parches" o actualizaciones de seguridad liberados por los fabricantes de los activos tecnológicos.

c) La facilidad con que la vulnerabilidad puede ser "explotada" por algún "atacante" informático.

d) La notificación de vulnerabilidades informadas por los equipos de respuesta a incidentes de seguridad al CSIRT de Gobierno.

e) El escaneo de funciones específicas, puertos, protocolos y servicios, entre otros, que no debieran estar disponibles a usuarios no autorizados.

2.5. Tratamiento de las mitigaciones

a) Las medidas de mitigación a efectuar deberán considerar los controles relacionados con la administración de cambios, así como también los procedimientos de respuesta ante incidentes de seguridad.

b) Toda vulnerabilidad catalogada como "crítica" o "de alto riesgo", reportada por un fabricante o entidad referente internacional que afecte algún componente de la plataforma, deberá generar las acciones de mitigación inmediata que correspondan.

c) Para aquellas vulnerabilidades catalogadas como "medias" o "bajas", se deberá definir un plan de acción para su mitigación, definiendo un plazo de ejecución.

d) Las vulnerabilidades administrativas asociadas a debilidades en la gestión de la seguridad de la información, que no involucren tecnologías, deberán ser sometidas a su evaluación de riesgo y proponer acciones de mitigación necesarias.

e) Se deberán establecer los resguardos apropiados para los informes de vulnerabilidades, evitando de esta forma, el riesgo de divulgación de esta información.

2.6. Información al Encargado de Ciberseguridad y al Comité de Seguridad de la Información

a) Toda vulnerabilidad tipificada como riesgo crítico, deberá ser informada de inmediato al Encargado de Ciberseguridad, el que evaluará y verificará la ejecución las acciones de mitigación correspondiente.

b) Aquellas vulnerabilidades de riesgo crítico que no puedan ser adecuadamente mitigadas, deberán ser consideradas e incluidas en los planes de contingencia asociados.

c) De acuerdo a la periodicidad definida en el estándar de seguridad de la información, se deberá informar al Comité, las vulnerabilidades identificadas, señalando los procesos y activos de información relacionados, así como también las acciones de mitigación efectuadas o por efectuar, a fin que éste adopte, en caso de ser necesario, las modificaciones que correspondan a la Política Informática y de Seguridad de la Información de Corfo, y sus Políticas anexas.

POLÍTICA DE SEPARACIÓN DE AMBIENTES

La separación de ambientes de desarrollo, testing y producción permite reducir los riesgos de acceso no autorizados o cambios al ambiente de producción de los sistemas de información de Corfo.

1. Objetivo

Corfo declara que la creación y mantención de sus sistemas aplicativos se debe realizar mediante tres ambientes separados de: desarrollo, test y producción. Este proceso de separación debe considera:

a) Cada ambiente deberá estar separado físicamente, esto es en servidores diferentes.

b) Se deberá mantener un estricto control de acceso lógico, que impida el acceso no autorizado desde un ambiente a otro.

2. Definiciones

2.1. Definición de ambientes

Las características y objetivos de los distintos ambientes definidos son:

a) Ambiente de Desarrollo: Destinado al desarrollo y mantención de los sistemas aplicativos de Corfo, lugar donde se efectúan las labores de construcción y modificación de los sistemas de Corfo.

b) Ambiente de Test: Donde se efectúan pruebas a las funcionalidades y chequeos adicionales que tienen el objetivo de certificar la calidad del software creado/modificado, asegurando la continuidad del servicio del sistema aplicativo. En este ambiente de prueba, los usuarios deben efectuar las pruebas necesarias para aprobar el paso al ambiente de Producción, siendo esta aprobación estrictamente necesaria.

Para el caso de pruebas de sistemas que administran proveedores externos, se deberán dar las facilidades y aseguramiento necesario para su utilización, de acuerdo a lo dispuesto en la Política de Seguridad en la Relación con Proveedores.

Las actualizaciones de sistemas operativos y parches deberán, en lo posible, utilizar este ambiente antes de su paso a producción.

c) Ambiente de Producción: Donde se encuentran todos los sistemas aplicativos de Corfo. Es el ambiente de mayor protección por lo que se deberán considerar los requerimientos establecidos en los controles de cambio. En cuanto a los accesos lógicos, se requiere que los accesos de los usuarios sean controlados y sus acciones registradas.

2.2. Responsables por ambiente

Cada uno de los ambientes definido por Corfo, deberá contar con un encargado responsable diferente.

Su responsabilidad es velar por el cumplimiento de los procedimientos y controles de cambios definidos para el ambiente a cargo.

2.3. Movimiento de elementos entre los ambientes

Con el objetivo de proteger los ambientes, los movimientos hacia ambientes más restrictivos, deberán realizarse en modalidad "PULL", esto es, el encargado del ambiente más restringido "saca" los elementos que le son ofrecidos por su contraparte del ambiente menos restringido.

Para estos efectos, se define que el nivel de restricción es:

- Desarrollo, nivel de restricción baja.
- Test, nivel de restricción media.
- Producción, nivel de restricción alta.

2.4. Consideraciones generales

La separación de estos ambientes, los que se encuentran orientados a asegurar un adecuado y seguro control de cambios, deberá cumplir los siguientes requisitos:

a) Para la incorporación de un sistema de aplicación o cambios en los existentes deberá existir un procedimiento que señale que todo cambio debe ser formalizado, como asimismo su autorización.

b) Se deberán establecer adecuados controles para asegurar el correcto traspaso de los sistemas aplicativos entre los distintos ambientes definidos, cuidando de que estos sistemas no puedan ser modificados desde otro ambiente.

c) En el caso de las personas que realizan labores de desarrollo, el acceso lógico al ambiente de producción se encuentra prohibido efectuar separaciones de ambientes o movimientos de elementos entre los ambientes sin la respectiva autorización.

d) Cualquier modificación planificada para las plataformas del ambiente de producción, como resultado de modificaciones a sistemas operativo o actualización de parches, debe ser formalmente solicitada y aprobada por el Jefe la Unidad de Continuidad Operativa.

POLÍTICA DE DESARROLLO SEGURO

La seguridad de la información debe ser una parte integral de los sistemas de información en todo su ciclo de vida, incluyendo los requerimientos para aquellos sistemas que proporcionan servicios en redes públicas.

1. Objetivo

Garantizar que la seguridad de la información sea una parte integral de los sistemas de información en todo su ciclo de vida, incluyendo los requerimientos para aquellos sistemas que proporcionan servicios en redes públicas. El objetivo de asegurar la inclusión de controles de seguridad y validación de datos aplica tanto para software adquirido, como para el desarrollo interno y en componentes desarrolladas por terceros para los sistemas de información de Corfo.

Los lineamientos de esta Política aplican a:

- Sistemas desarrollados tanto internamente, como contratados con terceros.
- Mantenimiento de los sistemas internos de la institución.
- La existencia de ambientes de trabajo de desarrollo, testing y producción, así como los protocolos de transición entre ambientes y la protección de datos de prueba.
- La protección necesaria en sistemas disponibles en redes públicas.

El desarrollo seguro es un requisito para generar un servicio, arquitectura, software y sistema seguro.

2. Planificación y documentación de requerimientos de seguridad

a) Los requerimientos puntuales de seguridad se deberán analizar, planificar y documentar según la criticidad y sensibilidad del sistema de información a adquirir, en desarrollo o en sus mantenciones y mejoras, especialmente aquellos que pudiesen significar riesgo de pérdida, uso indebido, acceso no autorizado o modificación de información sensible.

b) Dicho análisis deberá proporcionar una visión general de los requerimientos de seguridad del software, dar visibilidad de los riesgos de seguridad de la información y describir los controles a implementar para cumplir estos requerimientos en las etapas pertinentes de desarrollo.

c) Se deberán establecer criterios de aceptación para los sistemas que incluyan el cumplimiento de los requisitos de seguridad de la información previamente establecidos.

d) Toda necesidad de cambio de los requisitos de seguridad de la información deberá ser evaluada y autorizada, controlándose su implementación.

e) Cuando se aplican cambios al software que afecte la planificación de seguridad existente, la documentación de los requerimientos de seguridad deberá ser consecuentemente actualizada.

3. Protección de la Información en los sistemas

a) La información involucrada en aplicaciones o sistema de información para los ciudadanos, particularmente aquellos que utilizan infraestructuras públicas, se deberá proteger contra actividades que busquen fraudulentamente alterarla, que persigan el secuestro de información, la denegación de servicio u otra acción para explotar vulnerabilidades del sistema con fines ilícitos.

b) En las transacciones de los sistemas se debe proteger la información sensible para evitar una transmisión incompleta, enrutamiento incorrecto, alteración, divulgación, duplicación o reproducción no autorizada.

4. Competencias de seguridad en los equipos de trabajo

a) Se debe garantizar las competencias necesarias en seguridad de la información para cada rol relevante involucrado en los proyectos de desarrollo de software.

b) Se deben monitorear las actualizaciones de estándares y metodologías de seguridad de software, así como las amenazas y las distintas formas y

recomendaciones de su gestión. El personal ad-hoc a cada tema, debe estar en conocimiento de dichas actualizaciones y con ello actualizar sus competencias.

c) De surgir necesidades de capacitación se deberán seguir los protocolos corporativos de gestión de riesgos.

5. Adquisición de sistemas a proveedores

a) Si se externaliza el desarrollo de algún componente de software, se deberá obtener la garantía y documentación de cómo la parte externa cumple la presente Política.

b) Deberá revisarse la evidencia necesaria de pruebas de aceptación del sistema, la que deberá incorporar los requisitos de seguridad de la información establecidos en la Política Informática y de Seguridad de la Información de Corfo.

c) Según la criticidad del sistema se deberá permitir la supervisión, monitoreo y prueba de los controles de seguridad del sistema en desarrollo, por parte de Corfo o de un tercero independiente definido por ésta.

d) En la ejecución de estos contratos se dará pleno cumplimiento a la Política de Seguridad en la Relación con Proveedores, la que formará parte integrante del respectivo contrato para todos los efectos legales.

6. Seguridad en la infraestructura de soporte

a) Se deberá integrar al desarrollo de los sistemas de información los requerimientos respectivos para la seguridad de la infraestructura TI que los soportará.

b) Todo software que procese, transfiera o almacene información sensible de Corfo deberá alojarse únicamente en sitios aprobados por la Corporación. La infraestructura TI de soporte deberá cumplir con las políticas y estándares de seguridad aprobados por Corfo.

c) Cuando se realicen cambios en las plataformas o entornos operativos TI, ante la eventualidad de afectar el comportamiento de las aplicaciones críticas para el servicio, éstas se deberán revisar y testear para asegurar que no se ha generado un impacto adverso en las operaciones o en la seguridad de los sistemas.

7. Seguridad en todos los entornos aplicativos

a) La seguridad de la información se deberá diseñar e implementar dentro del ciclo de vida de desarrollo de los sistemas de información, manteniendo entornos separados para desarrollo, pruebas y producción, de acuerdo a lo establecido en la Política de Separación de Ambientes.

b) Todo código desarrollado deberá ser revisado y aprobado formalmente antes de su paso a un entorno de producción.

8. Gestión de pruebas del código

a) Deberá existir un proceso de revisión integral para descubrir vulnerabilidades y riesgos específicos del proyecto de desarrollo a nivel del lenguaje. Se deberán considerar y aplicar, según la criticidad del sistema, los tipos de pruebas interactivas por el desarrollador, y el análisis estático de código y/o análisis dinámico del sistema, gestionando las mitigaciones a las vulnerabilidades que de ello se deriven.

b) Se deberán establecer, tanto programas de pruebas de seguridad, como programas funcionales y de aceptación para los nuevos sistemas de información y actualizaciones.

c) Las pruebas de aceptación del sistema deberán incluir la verificación del cumplimiento de los requerimientos de seguridad de la información y la adherencia a los estándares Corfo de desarrollo seguro. Las pruebas también se deben realizar en los componentes y sistemas integrados recibidos de terceros.

d) El acceso al código fuente y otros recursos críticos del software durante el ciclo de vida deberá limitarse sólo al personal autorizado con una necesidad relacionada con el trabajo que debe desarrollar.

e) Se deberá garantizar la protección de los datos que se utilizan para procesos de pruebas en los entornos pre productivos, evitando la utilización de datos productivos sensibles.

f) En caso de ser necesario, se deberán despersonalizar los datos antes de su uso en entornos pre productivos y aplicar controles de acceso equivalentes a los de producción.

9. Gestión de vulnerabilidades

a) Se deberán desarrollar y controlar las capacidades necesarias, respecto de cada uno de los roles vinculados al desarrollo, para prevenir, evitar, descubrir y/o solucionar vulnerabilidades que puedan afectar los sistemas de Corfo.

b) Se deberán realizar evaluaciones a los controles de seguridad del software, y de vulnerabilidades que busquen identificar las debilidades a explotarse en algún sistema en producción o en sistemas que experimenten cambios significativos. Se deberán considerar las codificaciones internacionales de vulnerabilidades, así como sus ponderaciones de criticidad y riesgo.

c) Las notificaciones de vulnerabilidades de los proveedores, terceros y otras fuentes apropiadas deberán ser monitoreadas y evaluadas para asegurar el cumplimiento de los requisitos establecidos en la Política Informática y de Seguridad de la Información de Corfo y sus Políticas anexas.

d) Se deberán establecer las responsabilidades y periodicidad de las validaciones de "salud" de los sistemas de información, y el estado de los entornos pre productivos y productivos, de acuerdo con las mejores prácticas establecidas por Corfo, así como el nivel de riesgo de cada proyecto.

10. Seguridad en el uso, operación y monitoreo del sistema

a) Se deberán establecer reglas de seguridad para los usuarios de los sistemas respecto de su operación y monitoreo.

b) Se deberá gestionar la evidencia de pruebas de aceptación de sistemas que incorporen los requisitos de seguridad de la información establecidos por Corfo.

c) Como regla de monitoreo, se deberá establecer qué tipo de LOG's (información, frecuencia, estados, formato) deberán ser generados y cómo se deben resguardar posteriormente.

11. Revisiones y auditorías de seguridad

a) Los sistemas de información y los protocolos de sus etapas de desarrollo se deberán revisar regularmente para verificar cumplimiento de la presente Política.

b) Se deberá exigir el cumplimiento de estas Políticas y los estándares propios establecidos por Corfo, así como de la normativa legal y reglamentaria vigente al momento de ejecutar acciones sobre los sistemas. Se deberá considerar, en particular, las regulaciones y leyes del país donde se esté implementando el software y/o donde se ubique la plataforma respectiva, en caso de ser en el extranjero, procurando que sea un país que cuente con estándares de seguridad de la información iguales o superiores a los establecidos por Chile.

c) Se deberán planificar, acordar y registrar los requisitos y las actividades de auditoría que involucren la verificación de los sistemas de información críticos para impedir modificaciones a los sistemas o datos relacionados, así como minimizar las interrupciones a los procesos de negocio.

12. Seguridad en la mantención y control de cambios

a) Se deberá hacer uso de procedimientos formales para las mantenciones y su control de cambios, tanto para desarrollo interno, como para el desarrollo encargado a terceros, así también en los paquetes de software adquiridos a terceros, garantizando la seguridad y continuidad operacional de los sistemas de Corfo.

b) Se deberán considerar las instancias de mantención para incluir mejoras en los controles de seguridad, teniendo presente los incidentes reales que hayan afectado los sistemas de Corfo y los riesgos de seguridad de la información actuales y proyectados.

c) Se deberá considerar una etapa específica de aprobación y aceptación del cambio, previo a que entre en su estado normal de operación. Dicho proceso deberá considerar criterios de seguridad en la aceptación, como cuantificación del riesgo, documentación de nueva operación y del proceso de vuelta atrás.

13. Seguridad en el retiro de sistemas de información

a) Cuando un sistema de información se transfiera, se vuelva obsoleto o deje de ser utilizado, se deberán gestionar explícitamente los riesgos de seguridad de la información asociados a la transferencia, eliminación y retiro.

b) Las actividades de transferencia, eliminación y retiro deberán asegurar la terminación ordenada del sistema y preservar la información vital para que pueda ser reactivada en el futuro, si es necesario.

14. Estándares de Seguridad TI para el desarrollo de software

a) Corfo deberá definir, formalizar y mantener actualizadas las definiciones y estándares para los aspectos, procesos, etapas del ciclo de vida del desarrollo de software, así como los productos que generen, los que deberán ser referenciados en los documentos de implementación que lo requieran.

b) Todos los desarrolladores y encargados de proyecto de desarrollo deberán seguir los estándares de desarrollo de software de Corfo.

c) Se deberán establecer, documentar, mantener y aplicar los principios de ingeniería de sistemas seguros para cualquier labor de diseño e implementación de los sistemas de información de Corfo.

d) Se deberá asegurar que la propiedad intelectual que proceda respecto de los productos desarrollados sea de Corfo, y que los elementos que se utilicen para el desarrollo de software no atenten contra la propiedad intelectual o industrial de terceros.

POLÍTICA DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

El plan de continuidad del negocio garantiza la continuidad de la seguridad de la información de Corfo, permite reducir el impacto ante un incidente o desastre, definiendo las estrategias y su implementación.

1. Objetivo

Definir los requerimientos de seguridad de la información y la continuidad de la gestión en situaciones adversas tales como crisis o desastres.

2. Definiciones

2.1. Elaboración de planes de continuidad del negocio (PCN)

Un Plan de Continuidad del Negocio establece los lineamientos con los cuales la organización evalúa, declara y notifica una situación de discontinuidad, cómo se realiza la recuperación y la restauración de la operación normal.

Corfo deberá contar con planes de continuidad que contemplen las definiciones y los procedimientos necesarios para efectuar una rápida recuperación de sus procesos críticos de negocio frente a eventos identificables que han generado una interrupción severa de ellos.

2.2. Principios

a) La protección y seguridad de las personas debe ser prioridad, tanto en operación normal, como en situación de crisis.

b) Los planes de continuidad de negocio se enfocarán en los procesos y subprocesos críticos de la corporación.

c) Deberán asignarse los recursos suficientes para realizar el análisis y selección de estrategias, el desarrollo de los planes de reacción, las pruebas y la capacitación.

d) El aprovechamiento de las sinergias generadas en el desarrollo e implantación de los Planes de Continuidad de Negocio de la Corporación deberán basarse en los medios y recursos de los que dispone Corfo.

e) Deberá comunicarse a todos los funcionarios de Corfo sus responsabilidades respecto del plan de continuidad del negocio, y los procedimientos que le competen en relación a su ejecución.

f) Deberá existir un proceso de mejora continua de los planes de continuidad de negocio, en forma de revisiones, pruebas y actualizaciones.

g) La seguridad de la información deberá considerarse un proceso crítico de la Corporación en todo análisis de continuidad.

2.3. Escenarios

Los principales escenarios globales que pueden afectar la continuidad de negocio y que deben considerarse en el análisis, son:

a) **Sin infraestructura física:** El lugar de trabajo no se encuentra disponible debido a que ya no existe o no se puede acceder.

b) **Sin personal:** No existe personal para efectuar los procesos críticos del negocio.

c) **Sin infraestructura tecnológica:** Interrupción de los servicios TIC con distintos niveles de impacto en los procesos críticos.

d) **Sin disponibilidad de proveedores que soporten procesos críticos de Corfo.**

e) **Aquellos que generan una crisis de alto impacto a la corporación:** Donde, no siendo generada por la indisponibilidad de un recurso de aquellas descritas en lo literales precedentes, se genere un daño a la reputación de Corfo o de sus autoridades y funcionarios.

2.4. Estrategia de continuidad

Se deberán identificar, analizar y evaluar las alternativas de solución que satisfagan los requerimientos de la Corporación ante los distintos escenarios planteados.

Una vez que se definen las alternativas, se deberán diseñar las estrategias de continuidad.

2.5. Desarrollo de los planes

Para cada escenario se deberán desarrollar los planes de evaluación, declaración y notificación, de recuperación y de restauración. Estos planes serán diferentes según el escenario y estrategia seleccionados, requiriendo desarrollos independientes, pero dentro del marco general establecido en el plan de continuidad del negocio. Por ejemplo, el DRP IT (Disaster Recovery Plan for Information Technology) es un caso particular de los planes de recuperación.

2.6. Formalización de los planes

Los planes de continuidad del negocio deberán formalizarse en un documento, el que deberá ser publicado, probado y adecuadamente actualizado.

2.7. Plan de administración de contingencias

Deberá definirse un plan de administración de contingencias como eje que controle cualquier escenario de contingencia definido.

2.8. Entrenamiento y pruebas de los planes de continuidad del negocio

Se deberá establecer un programa de entrenamiento para todo el personal involucrado en los diferentes planes de continuidad del negocio.

2.9. Pruebas

Se deberán definir, programar, ejecutar y auditar pruebas periódicas de los planes desarrollados. Estas deberán ser programadas con antelación y cuidando no dañar la continuidad de los procesos normales.

2.10. Resguardo

Se deberá proteger la información asociada a los planes particulares, particularmente para que no pierdan su integridad y disponibilidad. La confidencialidad deberá ser protegida en función de la clasificación de los activos de información que sean parte del plan.

2.11. Distribución

Se deberá velar por la adecuada distribución de los planes actualizados, a todos los involucrados en su formulación y ejecución.

2.12. Capacitación

Se deberá establecer una guía para la difusión y capacitación a todos los involucrados en cualquiera de las tareas que conforman parte de algunos de los planes derivados del plan de continuidad del negocio.

POLÍTICA DE SEGURIDAD PARA EL DESARROLLO DE PERSONAS

Esta Política tiene por finalidad establecer los lineamientos generales relativos a la seguridad de personas, a fin de proteger su seguridad e integridad, así como los intereses de Corfo.

1. Objetivo

Asegurar que los funcionarios, proveedores y terceros comprendan sus responsabilidades con la seguridad de la información, y sean aptos para el correcto desempeño de los roles que les sean asignados, con el objetivo de salvaguardar las definiciones de la Política Informática y de Seguridad de la Información de Corfo y sus Políticas anexas.

De esta forma, los objetivos específicos de esta Política son:

a) Que los funcionarios, proveedores y terceros estén en conocimiento, entiendan y cumplan las responsabilidades que les incumban en relación a la seguridad de la información, para así reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.
b) Proteger los intereses de Corfo durante el proceso de cambio o la finalización de la relación por parte de funcionarios y personas externas.

OTROS ALCANCES

1. Política de Gestión de Activos

Tiene por objetivo identificar los activos de información y definir las responsabilidades para la aplicación de un nivel adecuado de protección, evitando cualquier divulgación, modificación, retirada o destrucción de activos no autorizado.

3° **ADÓPTESE**, por cada uno de los Comités de la Corporación, la Política Informática y de Seguridad de la Información de Corfo, que por este acto se aprueba, estableciendo las adecuaciones que resulten necesarias para ajustarlas a su orgánica interna, y dictando los actos administrativos que correspondan.

4° **PUBLÍQUESE** la presente resolución, una vez que se encuentre totalmente tramitada, en la Intranet Corporativa de Corfo.

Anótese, comuníquese y archívese.

MARÍA ELINA CRUZ TANHNUZ
Fiscal

PABLO TERRAZAS LAGOS
Vicepresidente Ejecutivo

CCVH/XPG