Dirección del Trabajo

Gobierno de Chile

004

ORDEN DE SERVICIO Nº_____/

ANT.: 1) Orden de servicio N° 6 del 30 de julio de 2010.

2) Res. Exenta N° 2.279 del 21 de diciembre de 2012 que establece política general de seguridad

3) Res. Exenta N° 1.523 del 30 de noviembre de 2011 que designa encargado de seguridad.

4) Orden de servicio N° 6 del 30 de julio de 2010 que informa políticas de seguridad de documentos electrónicos.

5) Res. Exenta N° 1.602 del 30 de diciembre de 2010 que crea el Comité de Seguridad de la Información de la Dirección del Trabajo.

MAT.: Actualiza marco normativo de seguridad.

Santiago, 24 DIC 2018

Lo dispuesto en los artículos N°6 y N°8, de la Constitución Política de la República de Chile, cuyo texto refundido, coordinado y sistematizado fue fijado por el decreto N°100, de 2005, del Ministerio Secretaria General de la Presidencia, el Decreto con fuerza de Ley N°1/19.653 del año 2000, del Ministerio Secretaria General de la Presidencia, que fijo el texto refundido, coordinado y sistematizado de la ley N°18.575, Orgánica constitucional de Bases Generales de la Administración del estado, Ley N°20.285, de 2008, sobre acceso a la información Pública; el Decreto Supremo N°83, del 03 de junio de 2004, del Ministerio Secretaria General de la Presidencia, publicado en e l Diario Oficial el 12 de enero de 2005, que impone la obligación de establecer una Política de Seguridad que fije las directrices generales que orientan la materia de seguridad dentro de cada Institución.

1.- Antecedentes Generales:

La Dirección del Trabajo, es un Servicio Público, altamente comprometido, profesional y competente, orientado a promover la satisfacción de los requisitos de sus clientes, mediante la provisión de productos y/o servicios que incorporen en su gestión criterios de calidad. Además la Institución compromete como uno de los ejes principales en su quehacer, el asegurar toda la información que ingresa y se genera desde las unidades operativas y de apoyo en términos de mantenerla integra, confiable y disponible para nuestros usuarios.

1.1 Objetivos Política General del Seguridad

La necesidad de mantener actualizada la política de seguridad de la información Institucional, así como también, entregar continuidad al proceso de gestión de la seguridad de la información en concordancia con lo establecido en las resoluciones exentas indicadas en los antecedentes.

Así como la exigencia de generar un proceso que minimice el riesgo, - entendido como toda amenaza, impacto o vulnerabilidad asociada al mismo-; y garantice la protección de los activos de información del Servicio, a través de un sistema integrado que permita la trazabilidad de la información y su confidencialidad, se hace necesario que la Institución rediseñe, actualice y difunda las políticas y procedimientos de seguridad que rigen el funcionamiento de la Dirección del Trabajo.

Para contribuir al logro de este objetivo, es indispensable contar con la determinación de ciertos elementos, tales como la designación de roles y responsabilidades, metodologías y procesos específicos, evaluación de controles de seguridad y de revisión de incidentes asociados al producto, a través de un cuerpo normativo sistematizado.

Que, con el objeto de apoyar el cumplimiento de sus funciones, la Dirección del Trabajo, ha desarrollado una plataforma tecnológica, a través de la que registra, procesa, trasmite y almacena datos, mediante distintos activos de información que permite interactuar con diferentes usuarios internos y externos del servicio, las que se encuentran resguardadas por una política general de seguridad de la información.

1.2 Marco Normativo

Se ha establecido el siguiente marco normativo del rubro, que viene a reemplazar el diseño de políticas y procedimientos desarrollado en años anteriores, sistematizando la información en el presente cuerpo normativo.

Los aspectos que cubre el actual marco regulatorio dan cuenta de la evolución y realidad tecnológica de la Dirección del Trabajo y su plataforma tecnológica, el cual se ha desarrollado de acuerdo a lo que indica la norma NCh ISO 27001:2013.

I.- Cláusulas

I.1 Políticas de seguridad de la información.

I.2 Organización de la seguridad de la información.

I.3 Seguridad de recursos humanos.

I.4 Administración de activos.

I.5 Control de acceso.

I.6 Criptografía.

I.7 Seguridad física y ambiental.

I.8 Seguridad de las operaciones.

I.9 Seguridad en las comunicaciones.

I.10 Adquisición, desarrollo y mantenimiento de sistemas.

I.11 Relaciones con los proveedores.

I.12 Administración de incidentes de seguridad de la información.

I.13 Aspectos de la seguridad de la información de la administración de la continuidad de los procesos.

I.14 Cumplimiento.

1.3.- Alcance

El alcance del Sistema de Gestión de Seguridad de la Información está determinado por los procesos que dan soporte a los productos estratégicos de la Dirección del Trabajo, definidos en la Ficha de Definiciones Estratégicas vigente.

Esta Política General de Seguridad de la Información debe ser conocida y aplicada por todos quienes trabajan en la DT, en cualquier nivel jerárquico, ya sean funcionarios de planta, contratados asimilados a grados, honorarios o en cualquier calidad que se desempeñen, que laboren o cumplan funciones dentro de las áreas y departamentos de la institución, así como los proveedores, terceros autorizados o cualquiera que use o tenga acceso a los activos de información de la Institución.

1.4.- Roles y Responsabilidades:

Jefe de Servicio:
Aprueba la presente Política General de Seguridad y valida el proceso de gestión de Seguridad de la Información, sanciona las estrategias y mecanismos de control para el tratamiento de riesgos que afecten a los activos de información institucionales, que se generen como resultado de los reportes o propuestas del Comité de Seguridad de la Información (CSI), así como los recursos necesarios para su ejecución.

Comité de Seguridad de la Información:
Tiene la responsabilidad de aprobar las políticas específicas de seguridad de la información, supervisando la implementación de procedimientos y estándares que se desprenden de las mismas, proponer estrategias y soluciones específicas para la implantación de los controles necesarios para materializar las políticas de seguridad establecidas y la debida solución de las situaciones de riesgo detectadas, 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 de la institución, para mantener estrategias comunes de gestión y reportar a la Alta Dirección, respecto a oportunidades de mejora en el SGSI, así como de los incidentes relevantes y su gestión.

Encargado de Seguridad de la Información:
Es un funcionario nombrado por el Jefe de Servicio como su asesor directo en materia de seguridad de la información. Debe organizar las actividades del CSI, coordinar la debida respuesta y priorización al tratamiento de incidentes y riesgos vinculados a los activos de información de los procesos institucionales y sus objetivos de negocio, monitorear el avance general de la implementación de las estrategias de control y tratamiento de riesgos, tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de la institución, controlar su implementación y velar por su correcta aplicación, así como mantener coordinación con otras unidades del Servicio para apoyar los objetivos de seguridad y establecer puntos de enlace con los Encargados de Seguridad de otros organismos públicos y especialistas externos, que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.

Dueño de proceso:
Es el responsable del proceso y de la información asociada. Su nivel jerárquico puede estar coligado con la responsabilidad de una Dirección, Departamento o Unidad.
Es quien determina el acceso a los distintos activos de información de su área de trabajo y quien autoriza sus distintos usos.

Funcionarios:
Deben cumplir toda la normativa existente en materia de seguridad de la información.

1.5.- Actualización del Marco Normativo:

La actualización o cambios en la normativa se podrá dar en los siguientes casos sin ser estos excluyentes uno de otro:

- Cuando se modifique todo o parte de la normativa de seguridad del Estado de Chile.
- Cuando se adquiera o se incorpore una nueva tecnología que administre activos de información o, cuando ocurra un cambio en la infraestructura computacional relevante.
- Cuando exista un proceso de cambio institucional relevante.
- Cuando se desarrolle un nuevo servicio.
- Cuando ocurra cualquier evento interno para el cual se requiere una protección apropiada para asegurar la continuidad del trabajo.
- Cuando ocurra un incidente de seguridad y/o se detecte una debilidad en la seguridad de un activo de información.

1.6.- Aprobación del Marco Normativo:

La normativa debe ser revisada y aprobada por el Comité de Seguridad de la Información y por el Encargado de Seguridad de la Información, lo cual debe quedar registrado en las actas de reunión del CSI. Luego de lo cual, el Encargado de Seguridad solicitará al (a la) Jefe (a) de Servicio el visto bueno del marco, lo que tendrá efecto de oficialidad del elemento normativo respectivo a través de una resolución exenta firmada por la autoridad.

1.7.- Auditoria Interna:

La Oficina de Auditoria Interna está autorizada por la Administración para evaluar el cumplimiento de todas las políticas institucionales, en cualquier momento.

1.8.- Difusión:

Para efectos de cumplir con el compromiso institucional de comunicar la normativa de seguridad de la información, se instruye a los Departamentos de Tecnología de Información y Oficina de Comunicaciones a se difunda el marco normativo de seguridad por medio del correo institucional a todo el personal, dejándolo disponible en la intranet institucional.

1.9.- Revisión del Marco Normativo:

Una de las tareas que deberán ser ejecutadas por el Comité de Seguridad de la Información de la Dirección del Trabajo, es la reevaluación de la Política General de la Seguridad de la Información. Esto deberá realizarse por lo menos una vez cada dos años o ante cualquier cambio significativo de tecnología, personal o evento que amerite su reevaluación para asegurar su continuidad, idoneidad, eficiencia y efectividad.

Se deberá, asimismo, programar, por lo menos una vez al año, la revisión de cumplimiento y la efectividad del Sistema de Gestión de Seguridad de la Información. En esa oportunidad se deberán revisar los incidentes ocurridos a la fecha y proponer planes de mejora en los casos que sea necesario.

1.10.- Sanciones:

Toda infracción a esta política y/o al Marco Normativo así como cualquier denuncia referida a funcionarios de la Dirección del Trabajo podrá ser investigado y/o denunciado ante la jefatura correspondiente, debiéndose aplicar las sanciones administrativas que procedan y ejercer las acciones civiles y penales que correspondan, conforme a la magnitud y características del incumplimiento de ésta.

1.11.- Vigencia:

Esta Orden de Servicio, comienza a regir a partir de su publicación en la página de intranet banner del Departamento de Tecnologías de la Información, dejando vigente la Orden de Servicio N°6, de 30 de julio de 2010, en todo aquello que no sea contraria.

Saluda atentamente a Ustedes,

DIRECCIÓN DEL TRABAJO
DIRECTOR
CHILE

DIRECCIÓN DEL TRABAJO
24 DIC 2018
OFICINA DE PARTES

MAURICIO PEÑALOZA CIFUENTES
ABOGADO
DIRECTOR DEL TRABAJO

LPG/cao
Distribución:

- Gabinete Sr. Director
- Gabinete Sr. Subdirección del Trabajo
- Jefes de Departamentos
- Jefes de Unidades
- Jefe oficina de Contraloría
- Jefe oficina de Auditoría
- Direcciones Regionales del Trabajo
- Inspecciones Provinciales y Comunales
- Centros de Conciliación y Mediación
- Escuela Técnica de Formación
- Oficina de Partes