Dirección del Trabajo
Ministerio del Trabajo y Previsión Social
Gobierno de Chile

DEPARTAMENTO DE TECNOLOGIAS DE INFORMACIÓN

ORDEN DE SERVICIO Nº 04 /

ANT.: 1) Orden de Servicio N° 6, de 30 de julio de 2010.

2) Res. Exenta N° 2.279, de 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.

MAT.: Establece nuevo marco normativo de seguridad.

Santiago, 30 MAR 2015

Lo dispuesto en los artículos 6 y 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 Secretaría General de la Presidencia; el Decreto con Fuerza de Ley N° 1/19.653 del año 2000, del Ministerio Secretaría General de la Presidencia, que fijó el texto refundido, coordinado y sistematizado de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; la Ley N° 20.285, de 2008, sobre Acceso a la Información Pública; el Decreto Supremo N° 83, de 03 de junio de 2004, del Ministerio Secretaría General de la Presidencia, publicado en el 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 íntegra, confiable y disponible para nuestros usuarios.

1.1.- Política General de Seguridad:

La necesidad de mantener actualizada la política de seguridad de la información Institucional, así como también, entregar continuidad al proceso de gestión de 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 productos informatizados 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.

En ese sentido, se ha establecido el siguiente marco normativo del rubro, que viene a reemplazar el diseño de políticas y procedimientos desarrollado entre los años 2010 y 2012, sistematizando la información en el presente cuerpo normativo.

Los aspectos que cubre el actual marco regulatorio, da cuenta de la evolución y realidad tecnológica de la Dirección del Trabajo y su plataforma tecnológica, la que se encuentran contenidas e integradas a la presente Orden de Servicio, de acuerdo al listado adjunto, que pasa a formar parte de aquella.

I.- Manual General de Seguridad:

I.1 Política de Correo Electrónico.
I.2 Política de Cuentas de Usuario.
I.3 Política de Identificación y Autenticación.
I.4 Política de Uso de Internet.
I.5 Política de Uso de Computadores Personales.
I.6 Política de Instalación y Uso Legal del Software.
I.7 Política de Antivirus.
I.8 Política de Seguridad para la Protección de Datos en Diferentes Medios.
I.9 Política de Seguridad para Pantallas y Escritorios Limpios.
I.10 Política de Seguridad en Servicios de Archivo e Impresión.
I.11 Política de Clasificación y Manejo de la Información.
I.12 Política de Seguridad para la Protección de Información de Directivos.
I.13 Política de Respaldo de Datos.
I.14 Política de Seguridad para el Resguardo de Datos Confidenciales.
I.15 Política de Acceso Remoto.
I.16 Política Acceso Inalámbrico.
I.17 Política de Respuesta ante Incidentes de Seguridad de la Información.

I.18 Política de Seguridad Física.

I.19 Política de Control de Acceso Físico.

I.20 Política de Seguridad para Recursos Humanos.

I.21 Política de Seguridad para Capacitación y Sensibilización en Materias de Seguridad.

I.22 Política de Seguridad para la Declaración de Privacidad.

I.23 Política de Continuidad del Negocio.

I.24 Política de Recuperación ante Desastres.

I.25 Política de Control de Cambios.

I.26 Política de Seguridad en Redes y Conexiones con Terceros.

I.27 Política de Administración de Servicios WEB.

I.28 Política de Diseño y Desarrollo de Sistemas.

II.- Manual General de Operaciones de infraestructura:

II.1 Alta de Usuarios.

II.2 Baja de Usuarios.

II.3 Modificación de información de Usuarios.

II.4 Aplicación de GPOs.

II.5 Restablecimiento de Contraseña.

II.6 Creación de Base de Datos en Exchange Server.

II.7 Mover Buzón de Base de Datos en Exchange Server.

II.8 Cambiar Membresía a Libretas de Direcciones en Exchange Server.

II.9 Asignar permisos sobre buzones de otros usuarios en Exchange Server.

II.10 Modificar Límites de Tamaño de Mensajes para Envío o Recepción de Correo Electrónico.

II.11 Rastrear Correos Electrónicos en Servidores Exchange.

II.12 Conexión de Dispositivos Móviles usando Exchange Active Sync.

II.13 Borrado Remoto de Dispositivos Móviles que sincronizan con servidores Exchange.

II.14 Monitoreo de actualización de firmas desde la consola central a estaciones de trabajo y Servidores.

II.15 Actualización de Servidores.

II.16 Actualización de Controladores de Dominio.

II.17 Respaldo de Active Directory.

II.18 Respaldo de Políticas de Grupo.

II.19 Respaldo de Exchange Server.

II.20 Respaldo General y Pruebas de Recuperación.
II.21 Eliminación Segura de Información.
II.22 Eliminación de Información Digital.
II.23 Respaldo de Configuración Firewall.
II.24 Actualización de Sistema Operativo de Firewall.
II.25 Creación de Regla de NAT de Salida.
II.26 Creación de Reglas de Publicación.
II.27 Creación de túnel WEB-VPN.
II.28 Respaldo de Configuración Switch de Comunicación.
II.29 Actualización IOS Switch de Comunicación.
II.30 Creación de VLANs.
II.31 Asignación de VLAN a Puerta del Switch de comunicación.
II.32 Encendido y apagado de puerta en un Switch de Comunicación.
II.33 Búsqueda por MAC Address.
II.34 Control de Código Fuente.
II.35 Modificaciones del Modelo de Datos en las BBDD.
II.36 Paso a Producción de Nuevo Sistema.
II.37 Paso de Producción de corrección a sistema existente.
II.38 Versionado de modelo de datos.
II.39 Versionado.

1.2 .- Responsabilidades:

El equipo de Seguridad de la Información, será el encargado de analizar los riesgos asociados y desarrollar el proceso adecuado para la gestión de controles de cumplimientos técnicos como también jurídicos; así como de velar por el cumplimento de estas políticas.

1.3.- Auditoría Interna:

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

1.4.- Publicidad:

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 la Información y Oficina de Comunicaciones a que mediante los mecanismos que estimen convenientes, se difunda este nuevo marco normativo de seguridad.

1.5.- 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
30 MAR 2015
OFICINA DE PARTES

DIRECCION DEL TRABAJO
DIRECTOR
CHILE

CHRISTIAN MELIS VALENCIA
ABOGADO
DIRECTOR DEL TRABAJO

RRM/LPG/AAV/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