Política de Seguridad de la Información Empresa Portuaria Chacabuco

ELABORADO POR:	REVISADO POR:	APROBADO POR
Empresa Portuaria Chacabuco	Filadelfo Cárcamo	Felipe Candia Araya

PLSI-001
"PLAN DE SEGURIDAD DE LA INFORMACION"
INDICE

1. Introducción

En este documento se incluyen las normas, lineamientos y servicios para la administración y buen funcionamiento de los recursos informáticos de la empresa, constituyendo la base normativa general para el personal que la integra. Asimismo, representa una fuente de consulta de fácil acceso para el personal encargado del área informática y está estructurado de acuerdo a Normas Generales, Normas Específicas, Lineamientos Generales y Requisitos para los servicios.

El presente documento proporciona la metodología que permitirá la presentación escrita, ordenada y uniforme de los principios técnico-normativos y muestra los procesos que en el contexto informático se realizan, además de los requisitos que deben cumplir y la periodicidad con que deberán realizarse.

El Plan de Seguridad Informático estandarizará el desarrollo tecnológico, mediante la promulgación de un conjunto de reglas obligatorias, que deben cumplir los responsables de todas las áreas de la empresa, siendo responsabilidad del Encargado de Informática, controlar su estricto cumplimiento en el ámbito de su competencia, tomando las medidas preventivas y correctivas para que se cumplan.

El hecho de que Empresa Portuaria Chacabuco cuente con un Plan de Seguridad Informática, significa que es una empresa previsiva orientada a minimizar al máximo los riesgos y vulnerabilidades (internas como externas), tanto en sus sistemas de información como en los demás contextos de TI.

2. Objetivo General y Específico

Objetivo General

- Contribuir a mantener la confiabilidad, disponibilidad e integridad de la información, así como a un mayor aprovechamiento de los recursos informáticos y de comunicaciones que son propiedad o que se encuentran al servicio de la Empresa, en apoyo a la gestión de la empresa.

Objetivos Específicos

- Utilizar los recursos tecnológicos de información al servicio de la empresa, en forma responsable y apropiada, de conformidad con las normas contempladas en el presente documento y otras de carácter organizacional.

- Minimizar las interrupciones en la disponibilidad de los servicios asociados a los sistemas informáticos y de comunicaciones, ocasionados por uso inapropiado o por daños causados de manera accidental o intencional.

- Informar y difundir a los usuarios de las distintas dependencias de la empresa, acerca de las normas, procedimientos y estándares que Empresa Portuaria Chacabuco, en su papel de ente rector en el ámbito de Seguridad Informática, ha establecido con el propósito de apoyar y asesorar en el mejor cumplimiento de las metas que cada área dentro de la empresa se ha trazado.

3. Campo de aplicación

Esta metodología está orientada a mantener un Plan de Seguridad Informática para todos los recursos informáticos y la infraestructura tecnológica de Empresa Portuaria Chacabuco, como también todas las actividades propias de la empresa, donde exista información digital y elementos de transferencia de los mismos por medio de dispositivos magnéticos, electrónicos o sistemas.

Las normas contempladas se aplican a todos los usuarios de datos, recursos y servicios informáticos, sean o no, propiedad de esta empresa, ya sea en forma compartida o controlados individualmente, que estén aislados o interconectados a redes.

4. Documentación de referencias

N°	Código	Descripción
1	**PLCI-001**	PLAN DE CONTINGENCIA INFORMÁTICO
2	**PRRD-001**	PLAN DE RESPALDO Y RECUPERACIÓN DE DATOS
3	**ANEXO - 01**	VALORIZACIÓN ACTIVOS TECNOLÓGICOS
4	**ANEXO - 02**	BITÁCORA DE SUCESOS PROCESO DE RESPALDO
5	**ANEXO - 03**	PLAN EVACUACIÓN RECINTO EMPORCHA
6	**ANEXO - 05**	PLAN CONTRA INCENDIOS

5. Responsabilidades:

5.1 Departamento de informática Empresa Portuaria Chacabuco

a. Elaborar las Normas Generales de Seguridad Informática.

b. Definir los controles y procedimientos de seguridad.

c. Autorizar la habilitación de conexión desde redes externas.

d. Autorizar los usuarios de la Red.

e. Autorizar los permisos a los recursos e información.

f. Autorizar las plataformas de hardware y software en uso.

g. Definir un sistema de monitoreo de incidentes de seguridad y llevar un registro en el “Libro de Incidentes Informáticos.

h. Definir la metodología de “Evaluación de Riesgos” informáticos y sobre ellos, basar los procedimientos y planes de contingencias.

i. Realizar reuniones semestrales con la alta gerencia, para informar modificaciones al Plan o Incidentes ocurridos.

j. Administrar y mantener actualizada la información administrativa y técnica del inventario informático.

k. Administrar la Red de Área Local, las aplicaciones y estaciones conectadas a la LAN.

l. Efectuar la capacitación a los usuarios, de las aplicaciones que tienen acceso por su grado y cargo.

m. Implementar, mantener y evaluar periódicamente los procedimientos y controles de seguridad definidos.

n. Llevar el registro de fallas y problemas de la red y estaciones de trabajo, en un “Libro de Incidentes Informáticos.

o. Investigar y proponer nuevas tecnologías para proteger los recursos e información.

p. Mantenerse informado de las vulnerabilidades en las aplicaciones y servicios y actualizar las versiones vulnerables.

q. Ejecutar la asignación de acceso a recursos de la LAN.

r. Mantener al día los antivirus, tanto en servidores como en las estaciones de trabajo de la LAN.

s. Considerará que la dependencia de los Administradores es exclusivamente para el trabajo de dicho personal, por lo cual, no se autoriza el acceso de personal ajeno el área TI, salvo actividades específicas relacionadas con dicho trabajo. Cumplimiento que debe ser controlado por el Encargado de Informática o quien designe la empresa.

t. Deberá realizar controles periódicos, a fin de auditar y avaluar los procedimientos y controles de seguridad definidos, actividad que deben estar respaldadas, documentadas e informadas, en las reuniones con la Gerencia.

u. Autorizarán bajo firma la salida de los equipos computacionales en caso de que estos deban ser utilizados en exposiciones o reuniones fuera de la empresa, coordinarán con la gerencia de la empresa, si el traslado de estos equipos es por motivos de cambio, reparación o uso de garantía.

v. Elaborar el calendario de mantenimiento de los PC.

w. Mantener una alta disponibilidad del sitio Intranet e Internet, como también de los accesos, seguridad y compartimentaje de la información en el publicado.

x. Administrar la información de "log" de Monitoreo de Acceso web, Base de Datos, etc.

y. Auditar y evaluar periódicamente los procedimientos y controles de seguridad definidos.

z. Realizar controles periódicos, a fin de verificar que los permisos de los usuarios, estén de acuerdo a lo dispuesto en Normativa de Administración y definición de Cuentas, conforme a lo descrito en el Anexo-04".

aa. Controlarán y revistarán el cargo de elementos magnéticos y documentación contenida dentro de los respectivos departamentos y secciones.

bb. Procederá a informar a Encargado de Informática, en lo referido a caducar las cuentas de todo funcionario que se encuentre en condición de retiro y cambio de desempeño, una vez que se protocolice su egreso.

cc. Controlarán que el cambio de las password se realice cada 30 días, según lo definido en la Normativa de Administración y Definición de Cuentas.

dd. Controlará que exista un sello indicativo en cada PC., a fin de detectar cualquier intento de manipulación del hardware del PC.

ee. Ejercerán un control permanente sobre los elementos magnéticos extraíbles (Pendrives y CD-ROM).

ff. Controlará que no existan computadores particulares en la Empresa.

5.2 Operadores de equipos computacionales

a. Dar estricto cumplimiento a las normas y procedimientos, descritos en el presente documento

b. Velar por la privacidad de su contraseña para ingresar a la red y a los diferentes sistemas de la Empresa

6. Método

6.1 NORMAS GENERALES

6.1.1 Empresa del Archivo Computacional

a. La totalidad de los equipos computacionales deberán estar conectados a la red de la empresa, por lo tanto, todos los trabajos que desarrollan los Departamentos, Secciones y/o Oficinas, deberán quedar archivados en los respectivos directorios de los discos de red según corresponda y en los respaldos respectivos, en elementos magnéticos extraíbles debidamente foliados conforme a lo indicado en el documento “PLAN DE RESPALDO Y RECUPERACIÓN DE DATOS”.

b. Se prohíbe mantener información reservada o de carácter organizacional en el disco local del PC (C:), para ello el usuario deberá almacenar la documentación de trabajo en los discos de Red asignados.

c. Los usuarios no pueden almacenar información de carácter personal en los discos de la Red.

d. Cada Departamento o Unidad de la empresa, dispondrá, de un sistema de archivo computacional, conforme a las materias que desarrollan:

- Por Ejemplo:
  - Minutas
  - Memorando
  - Etc.

e. Todo acceso a visualizar o compartir información de los discos de Red, deberán ser solicitadas por documento al Encargado de Informática de la

empresa, a fin de mantener el aseguramiento y compartimentaje de la información, permitiendo además la identificación del responsable de ella.

f. Será de responsabilidad de los Departamentos, Secciones y/o Oficinas cuando exista un cambio de usuario, verificar la información que reside en los discos, a fin de liberar espacio físico en el servidor central y no mantener información desfasada.

6.1.2 Claves de acceso a la red y Equipamiento computacional

- Tendrán una duración de 30 días, para lo cual el usuario deberá efectuar el cambio antes de su vencimiento.
- El sistema avisará con 5 días de anticipación el vencimiento de la clave de acceso.
- Se debe considerar que el sistema recordará y no permitirá el uso de las últimas claves asignadas al usuario.
- El largo mínimo permitido para la creación de nuevas claves será de 6 caracteres.
- La cuenta se bloqueará después de 3 intentos fallidos, para lo cual deberá solicitar ENCARGADO DE INFORMÁTICA, su habilitación.
- Queda estrictamente prohibido divulgar la clave de acceso a la cuenta que maneja el usuario, siendo esta de su exclusiva responsabilidad.
- Se llevará un registro de claves de Hardware y Software crítico en el Libro de Claves en poder ENCARGADO DE INFORMÁTICA (Caja Fuerte).
- Todos los PCs. deberán mantener activa la password de setup (única para la empresa, dispuesta por ENCARGADO DE INFORMÁTICA, y registrada en el Libro de Claves.

6.1.3 Norma de cuentas de usuarios de la red.

La estructura de cuentas de usuarios en el dominio se realizará por nombre, conforme a lo siguiente:

Nombre	User
Claudio Escobar	cescobar

- Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las Normas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.
- La cuenta de usuario debe ser coincidente con el nombre de la máquina, a objeto de facilitar el control y monitoreo por parte de ENCARGADO DE INFORMÁTICA
- La solicitud de una nueva cuenta (intranet y/o correo) o el cambio de privilegios deben ser hechos por escrito a ENCARGADO DE INFORMÁTICA y debe ser debidamente aprobada por la alta Gerencia.
- No debe concederse una cuenta a personas ajena a la empresa.
- Se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad.
- Toda cuenta quedará activa y no caducará, mientras la función que se desarrolle no sea suspendida.
- Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El ENCARGADO DE INFORMÁTICA debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de la GERENCIA GENERAL, y en particular cuando un empleado cesa en sus funciones.
- El inicio de sesión de usuario será restringido y accesado sólo en su estación de trabajo, para lo cual, el administrador de red aplicará la política en el Servidor de Dominio.
- Cuando un empleado es despedido o renuncia a la empresa, debe desactivarse su cuenta antes de que deje el cargo.

6.1.4 Fondo y protector de pantalla

a. Como una forma de uniformar la visualización de los PCs., el fondo de pantalla estará definido en el servidor central, siendo este de carácter obligatorio, al igual que el protector de pantalla.

b. El sistema cada 15 minutos por motivos de seguridad bloqueará el PC, pudiendo el usuario desbloquear el equipo con su password y de esta forma continuar su trabajo en forma normal.

6.1.5 Cambios de configuración

La Gerencia deberá informar por escrito, el cambio de usuarios al ENCARGADO DE INFORMÁTICA, lo que permitirá adecuar el Correo electrónico al nuevo usuario, su estructura de archivos y perfiles en el dominio

6.1.6 Horario de trabajo de las Redes

La Red mantendrá un horario de trabajo para los usuarios desde las 08.00 a 18.00 Hrs. con excepción de aquellos usuarios con privilegios especiales definidos por los jefes de Departamentos. Para alterar el horario de trabajo, por motivos del servicio, se deberá solicitar por documento al ENCARGADO DE INFORMÁTICA.

6.1.7 Directorios compartidos

a. Se mantendrá un Directorio compartido para cada departamento a fin de facilitar el trabajo colaborativo, el que radicará en el Servidor de Archivo.

b. No existirá ningún otro directorio particular con privilegios compartidos para uso específico o general que no esté contemplado en la Normativa de Administración y Definición de Cuentas.

c. Los usuarios definidos se limitarán a usar sólo los recursos definidos en la Normativa de Administración y Definición de Cuentas.

6.1.7 Empleo del correo electrónico

a. Correo

- Se autoriza la tramitación de información clasificada por correo electrónico, que requieran urgencia en su transmisión, debiéndose contar con el respectivo respaldo escrito con la firma del Gerente General o autoridad que corresponda. Lo anterior describe la autorización previa a la creación de las cuentas de correo.

- Se prohíbe estrictamente ocupar el correo electrónico interno de Empresa Portuaria Chacabuco, para la transmisión de cualquier otro tipo información que no sean de carácter profesional.

- El tamaño máximo de los archivos Adjuntos al Correo, no podrá exceder los 10 Mb, si así fuese el sistema lo rechazará.

- Los buzones de correo, no deberán usarse como medios de almacenamiento o respaldo de archivos de trabajo o de carácter personal, debiendo éstos proceder a su eliminación (considerar también la carpeta elementos eliminados).

6.1.8 La configuración base de las estaciones de trabajo es:

1.- Sistema Operativo y Upgrade.
2.- Software de Oficina.
3.- Antivirus.
4.- Software Utilitarios

6.1.9 Software

a. Queda absolutamente prohibido la instalación de cualquier software ajeno a los licenciados para la empresa.

b. Todo software necesario de implantar en las estaciones de trabajo, deberá poseer su correspondiente licencia y esta quedará en custodia de ENCARGADO DE INFORMÁTICA.

6.2 SEGURIDAD DE DOCUMENTACIÓN E INFORMACIÓN

a. El primer nivel de seguridad comprenderá el control del acceso al computador al momento de encender el equipo, mediante la activación de la clave de acceso a través del setup de cada computador, esta clave debe ser definida en la BIOS por el ENCARGADO DE INFORMÁTICA y debe ser entregada al usuario al momento de asignar el equipamiento (la confidencialidad de esta clave será de exclusiva responsabilidad del usuario y su cambio deberá ser solicitado directamente al ENCARGADO DE INFORMÁTICA.

b. El segundo nivel de seguridad comprenderá el control del acceso de la función usuarios de la red, mediante la activación de las claves respectivas creadas en el Active Directory y la perfilación definida para cada una de las

cuentas, (Nombre identificatorio usuario) USERNAME, (clave de acceso) PASSWORD, y su administración estará a cargo de ENCARGADO DE INFORMÁTICA.

c. Ambos niveles de seguridad serán fiscalizados por ENCARGADO DE INFORMÁTICA.

d. Las claves de acceso serán administradas ENCARGADO DE INFORMÁTICA y serán custodiadas en un lugar estratégico dentro del la empresa, éstas solo serán divulgadas a terceros mediante solicitud exclusiva de los respectivos Gerentes de Área o ante una emergencia solamente por el Gerente General o quien lo subrogue.

e. La administración comprenderá lo siguiente:

1) Control de acceso a los directorios de trabajo.
2) Restricciones dentro de cada grupo de trabajo.
3) Restricciones por grupo de trabajo.
4) Restricciones horarias.
5) Chequeo automático de virus computacionales.
6) Sistema de auditoría de red.
7) Control de acceso a los archivos.
8) Control de ambientes de trabajo dentro de la red.

6.2.1 Manejo de la información y documentación

a. La transferencia de datos a un CD-ROM o DVD-ROM (Grabación), será de responsabilidad de ENCARGADO DE INFORMÁTICA, único lugar para reproducir y almacenar información digital en este medio magnético. Para lo cual cada usuario deberá llevar el respectivo CD o DVD para esta tarea y la debida autorización de la Alta Gerencia.

b. Toda documentación que tenga un carácter de reservada debe ser visada por la Alta Gerencia, para su traslado fuera de la Empresa.

c. Todo integrante de la empresa que trabaje o custodie material informático y computacional, deberá tener conocimiento de las responsabilidades penales en caso de no dar cumplimiento a la legislación vigente en estas materias.

6.3 SEGURIDAD FÍSICA Y DEL MATERIAL

6.3.1 Fallas de Hardware (Equipos computacionales físicos) e Instalaciones.

a. Solo el ENCARGADO DE INFORMÁTICA será el responsable de configurar los equipos computacionales, como de resolver posibles anomalías presentadas en estos, como también de instalación de software.

b. La totalidad de los equipos de computación deben estar conectados a la red de energía eléctrica de computación dedicada. En consecuencia, queda prohibido que cualquier otro artefacto eléctrico (que no sea de computación), se conecte a esta red de energía de los computadores, como asimismo equipos que estén fuera de esta red eléctrica.

c. Con la finalidad de evitar la pérdida de información ante una falla del o los equipos y/o de la instalación de la red de energía, los usuarios del sistema computacional darán cumplimiento al almacenamiento de datos, en el sentido de mantener los respaldos respectivos en los discos de la red en forma periódica.

d. Toda vez que un usuario detecte un desperfecto y requiera la reparación o cambio de un componente informático, deberá dar aviso a ENCARGADO DE INFORMÁTICA, a fin de coordinar la entrega del equipo computacional, al departamento informático de la empresa, el cual será entregado bajo firma del responsable y mediante la “ficha de recepción de CPU o Portátil para reparación”, posteriormente será chequeado por personal especialista quien deberá verificar que las características técnicas del equipo recepcionado son las que corresponden al cargo respectivo.

d. Una vez detectado el desperfecto y aprobado el presupuesto se procederá a su reparación.

f. Si es necesario trasladar y transportar equipos computacionales fuera de la instalación, para ser reparados y revisados por organismos externos a la empresa o hacer uso de su garantía, se deberán respaldar todos los programas y sistemas contenidos en el disco duro. Realizado lo anterior se procederá a formatear el disco de forma segura y preparar el equipo en

conformidad a las exigencias técnicas de éste para su traslado.

g. En caso de ser posible, y previa coordinación con las empresas externas se podrán enviar los equipos para su reparación sin su disco duro, exceptuando aquellos que se encuentren dentro del período de garantía, razón por la cual se estaría impedido de extraer el disco (por rompimiento del sello de garantía), lo anterior sin perjuicio de las autorizaciones pertinentes y trámites administrativos que corresponda realizar.

6.3.2 Prevención en el uso de los computadores.

a. Antes de encender los equipos, se deberá verificar que todos sus componentes se encuentren debidamente conectados en la red de energía dedicada habilitada para tal efecto.

b. El no estar los equipos conectados a la red antes indicada, puede provocar una diferencia en la carga de energía eléctrica, con el consiguiente daño en los computadores.

c. Una vez verificado lo anterior, el usuario deberá realizar el siguiente chequeo secuencial, antes de iniciar las actividades diarias:
   - Encender el computador.
   - Encender la impresora.
   - El operador del computador debe digitar en forma moderada el teclado, sin golpear las teclas.

6.3.3 Daños por ataque de virus computacionales

a. En los computadores sólo se deberán ejecutar y operar programas que hayan sido revisados y autorizados por ENCARGADO DE INFORMÁTICA, siendo el único organismo autorizado y capacitado para instalar los programas que se requieran conforme a las necesidades de las actividades que desarrollan los diferentes Departamentos, por lo cual queda prohibida la instalación de otros programas que no cuenten con la debida licencia.

b. Queda prohibida la instalación de juegos, software, archivos etc. bajados de Internet, y propagados en la red a través de pendrive u otro medio, ya que estos son la principal causa, junto con el “pirateo”, del contagio de virus en los computadores y por ende en la red Institucional.

c. Asimismo, se deberá tener especial cuidado con los elementos de almacenamiento de datos extraíbles que lleguen de otras unidades, para lo cual se deberán tomar las medidas correspondientes de chequeo de este material con los antivirus respectivos, como también informando ENCARGADO DE INFORMÁTICA, cuando se detecte una situación de virus.

d. En atención a que no existen productos 100% efectivos a todos los virus deberán tener presentes algunos de los siguientes síntomas:
   1) Lentitud injustificada del equipo.
   2) Destrucción involuntaria de datos.
   3) Aparición de caracteres especiales en la pantalla.
   4) Mensajes en la pantalla.

e. ENCARGADO DE INFORMÁTICA deberá mantener actualizado el servidor de antivirus en forma diaria.

6.3.4 Procedimiento de adquisiciones y cambio de activos de las redes.

a. Todo cambio en el activo de las redes (Hardware y Software), deberá ser canalizado por ENCARGADO DE INFORMÁTICA, quien deberá certificar que cumpla con las normas técnicas.

b. De lo anterior se notificará a la Alta Gerencia quien deberá dar su aprobación definitiva de los movimientos de activos.

6.4 USO DE COMPUTADORES PORTÁTILES (P.C. Y/O NOTEBOOK)

a. En lo posible se deberá mantener un contacto físico permanente con los notebooks de la empresa y particulares. En ningún momento deberán quedar abandonados sobre los escritorios o la vista en oficinas sin la correspondiente custodia.

b. Se deberá considerar el empleo de fundas o maletines de traslado poco llamativos y ostentosos. Un bolso acondicionado proveerá una mejor protección visual sobre el elemento a trasladar.

c. La totalidad de los equipos notebook adquiridos por la empresa deberán contener una inscripción de identificación que deberá expresar **"**PROPIEDAD DE LA EMPRESA". Dicha inscripción deberá ser efectuada en grabado láser, maquina o grabado manual, pegada en lamina metálica o plástica sobre el chasis superior del computador.

e. Los notebooks de uso estable en una dependencia, deberán contar con el cable de fijación correspondiente.

f. Se deberá aumentar la conciencia de responsabilidad en el empleo por parte del personal a cargo en el uso, administración y custodia de los equipos portátiles, determinando de manera clara las responsabilidades disciplinarias y pecuniarias de reposición sobre una eventual pérdida de este material informático.

g. El ingreso y uso de equipos notebook particulares en la empresa, serán autorizados por el Gerente General. De la autorización de ingreso y empleo, se

dejará constancia, de acuerdo a lo siguiente:

- Nombre del responsable.
- Características del equipo (marca y número de serie).
- Lugar de empleo.
- Fecha de empleo (desde y hasta).

h. Con la finalidad de evitar extravíos o pérdidas de equipos organizacionales y/o particulares en la vía pública, se deberá evitar dejar los equipos en el interior de los vehículos particulares.

i. Durante el traslado de personal con equipos portátiles de la empresa y/o particulares, que por motivos del servicio (reuniones, delegaciones, etc.), deban permanecer por un período de tiempo en hoteles, residencias y casas particulares, se deberá adoptar el máximo de seguridad en su transporte, custodia, y principalmente en lo referido a elementos magnéticos extraíbles que mantengan materias reservadas.

6.5 USO DEL SERVICIO DE INTERNET AL INTERIOR

Las herramientas computacionales puestas a disposición de los usuarios, son para fines netamente de la empresa, para lo cual se debe dar cumplimiento a lo siguiente:

a. Uso de Chat:

- De utilizar este medio de comunicación, se prohíbe exponer o difundir cualquier tipo de materia o nombres de personas, que afecten la seguridad.
- Tener presente, que el uso de este medio de comunicación no es un pasatiempo, quedando prohibido su uso para fines particulares.
- Toda la actividad de tráfico, será monitoreado por ENCARGADO DE INFORMÁTICA.

b. Uso de correo por Internet:

- Queda prohibido transferir información que afecte la seguridad de la empresa a través de este medio.
- No abrir correos de usuarios desconocidos, a fin de evitar el ingreso de Software espías o troyanos.
- Será de exclusiva responsabilidad del usuario y no de la empresa, los correos o información transferida o recibida.
- El ENCARGADO DE INFORMÁTICA, evaluará una herramienta computacional, que permita realizar un filtrado de contenido de los mails.

c. Uso de Internet para navegación:

- Se debe considerar, que el objetivo principal de esta herramienta es de consulta y búsqueda de antecedentes válidos que permitan mejorar procedimientos, funciones u otros, en pos de generar mejores prácticas en apoyo a la producción y gestión de la Empresa.
- Se prohíbe la navegación en sitios con contenido pornográfico.
- Se prohíbe bajar juegos y programas debido al alto índice de virus.
- El ENCARGADO DE INFORMÁTICA, realizará un monitoreo de los sitios web visitados por los usuarios.

d. Uso de blogs y herramientas similares.

- Se prohíbe el intercambio de información de cualquier tipo y/o característica por este medio de comunicación digital que promulgue información reservada o afecte directamente a la empresa.
- Por no corresponder a una política de comunicación institucional, se prohíbe a los miembros de la empresa (persona natural), el intercambio,

envío y subida de imágenes, archivos personales, instalaciones, etc., sin previa autorización de la Alta Gerencia.

e. Consideraciones referidas al PC. conectado a Internet:

- EL ENCARGADO DE INFORMÁTICA, realizará monitoreo a la totalidad de los computadores conectados a la red Internet a fin de detectar software malicioso o programas espías, como también aquellos que permitan compartir archivos en Internet, a fin de ser eliminados.

6.6 USO DE INTRANET.

a. Los equipos que se desempeñen como usuarios de la red interna de la unidad, deberán minimizar al máximo el empleo de dispositivos externos de archivo tales como, disquetes, pendrives, CDs., DVI), flash memory, grabadores externos y otros. Lo anterior mediante el bloqueo de puertos USB, disqueteras, CD-RW, etc. El empleo de estos medios, se limitará conforme a las necesidades de la unidad y autorizados por ENCARGADO DE INFORMÁTICA.

b. Los equipos computacionales de la empresa sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

c. Debe respetarse y no modificar la configuración de hardware y software establecida por ENCARGADO DE INFORMÁTICA (identificación, sellos y software base)

d. Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, agua, etc.)

e. Cualquier falla en los computadores o en la red debe reportarse inmediatamente al ENCARGADO DE INFORMÁTICA, ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

f. Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.

g. No pueden moverse los equipos o reubicarlos sin permiso. Para cambiar un equipo a otro lugar se requiere una autorización de ENCARGADO DE INFORMÁTICA.

h. La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

i. Para prevenir el acceso no autorizado, los usuarios no deben divulgar su contraseña a otras personas y evitar dejar anotada la misma en la proximidad de la estación de trabajo.

j. No está permitido llevar al sitio de trabajo computadores portátiles (laptops) y en caso de ser necesario se requiere solicitar la autorización correspondiente a ENCARGADO DE INFORMÁTICA.

k. Todas las comunicaciones de datos deben efectuarse a través de la LAN de la empresa.

l. A menos que se indique lo contrario, los usuarios deben asumir que todo el software desarrollado en la empresa está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

m. Los usuarios no pueden extraer datos fuera de la empresa sin la aprobación previa del dueño del dato y posteriormente del Gerente Gereral. Esta política es particularmente pertinente a aquellos que usan a computadoras portátiles.

n. Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al ENCARGADO DE INFORMÁTICA y poner el PC en cuarentena hasta que el problema sea resuelto.

o. No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por el ENCARGADO DE INFORMÁTICA.

p. Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el ENCARGADO DE INFORMÁTICA

q. Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro

r. Se realizará periódicamente el respaldo de los datos guardados en servidores conforme a procedimientos establecidos por el ENCARGADO DE INFORMÁTICA

s. Cada usuario deberá hacer mantenimiento de su disco de red y eliminar la información duplicada.