2023

Políticas de Seguridad TI

Actualizada a Diciembre 2023.

PUERTOS DE TALCAHUANO

Inform7ación del documento.

HISTORIA DEL DOCUMENTO			
Nombre del documento:	Políticas de seguridad TI		
Preparado Por:	Gonzalo Gacitúa V.		
Responsable del Documento	Gonzalo Gacitúa V.	**Fecha de creación**	28-10-2019
Aprobado Por		**Fecha de Aprobación**	

Control de Versiones			
Versión	**Fecha de Creación**	**Preparada Por**	**Descripción**
1.0	22-12-2017	Gonzalo Gacitúa V.	Creación del documento
2.0	25-06-2019	Gonzalo Gacitúa V.	1.- Se incorporan a la política los siguientes ítems: - Historia del documento - Control de versiones - Anexo 1: Formulario para la creación – Modificación – Eliminación de cuentas de usuario - Procedimiento para la creación – modificación – eliminación de usuarios del sistema FIN700. - Anexo 3: Matriz de perfiles por cargo sistema FIN700 2.- Se elimina el apartado “cuentas genéricas en servidor de dominio” en Política de acceso a la red. 3.- Se modifican Políticas de acceso a internet, incorporando el uso de intranet y almacenamiento en la Nube. 4.- Se incorpora Política de Gestión de Contraseñas. 5.- Se modifica el formato de las políticas de acceso a la red de datos de la empresa. 6.- Se modifica el formato y contenido de las políticas de respaldo. 7.- Se incorpora política de uso del correo electrónico corporativo.

			8.- Se incorpora política Escritorio Despejado Y Pantalla Despejada 9.- Se incorpora política Gestión ante vulnerabilidades. 10.- Se incorpora política de uso de mensajería instantánea. 11.- Se incorpora política de adquisición de hardware y software. 12.-Se incorpora plan de seguridad de la información 2019
V 3.0	28-10-2020	Gonzalo Gacitúa V.	- Uso de lenguaje inclusivo. - Cambios en textos de intranet por extranet.
V 4.0	01-12-2021	Gonzalo Gacitúa V.	incorporación de Política, directiva y procedimiento de control de cambios a sistemas
V 5.0	14-11-2023	Gonzalo Gacitúa V.	- Se incorpora las actividades de ciberseguridad que se deben realizar. Estas tareas se describen en la política de gestión ante vulnerabilidades y ciberseguridad. - Se incorporan roles y responsabilidades del comité de seguridad de la información
V 6.0	22-12-2023	Gonzalo Gacitúa V.	- Se incorpora políticas y directrices de equipos móviles y teletrabajo. - Se actualizan roles y responsabilidades del comité de seguridad de la información.

(*) La presente versión sustituye completamente a todas las precedentes, de manera que éste sea el único documento válido de entre todos los de la serie.

Contenido

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION 6
OBJETIVOS 6
ALCANCE 6
DEFINICIONES 6
a) Actualización, publicación y difusión 6
b) Comité de Seguridad 6
c) Composición del Comité, roles y responsabilidades. 7
a) Normativa de Seguridad de los Recursos Humanos 9
b) Normativa de Seguridad Física y Ambiental 9
c) Normativa de Gestión de las Comunicaciones y las Operaciones 9
d) Normativa de Control de Acceso 10
e) Normativa de Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información 10
f) Normativa de Gestión de la Continuidad del Negocio 11
g) Normativa de Gestión de Incidentes en la Seguridad de la Información 11
CUMPLIMIENTO DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN 11
POLÍTICAS ESPECIFICAS DE SEGURIDAD DE LA INFORMACIÓN 12
POL001 - Política de Acceso a Extranet, Internet y Almacenamiento en la Nube 13
POL002 - Política de Gestión de Contraseñas 14
POL003 - Política de Acceso a la Red de Datos. 14
POL004 - Política de Respaldos Institucionales 15
POL005 - Política de Uso del Correo Electrónico Corporativo. 16
POL006 - Política de Escritorio Despejado y Pantalla Despejada. 17
POL007 - Política de Gestión Ante Vulnerabilidades y Ciberseguridad 18
POL008 - Política de Mensajería Instantánea y Videoconferencias. 19
POL009 – Política de Adquisición de Hardware y Software. 20
POL010 – Política de control de cambios a sistemas 21
POL011 – Política de dispositivos móviles y teletrabajo 21
DIRECTIVAS ESPECIFICAS DE SEGURIDAD DE LA INFORMACIÓN 22

PROCEDIMIENTOS ESPECIFICOS DE SEGURIDAD DE LA INFORMACIÓN 36

ANEXOS. 45

Anexo N°1: Formulario creación – Modificación – eliminación de cuentas de usuario. 45

Anexo N°2: Avance plan de seguridad 2023. 47

Anexo N°3: Plan de seguridad 2024. 51

Anexo N°4: Matriz de perfiles por cargo sistema FIN700. 55

Anexo N°5: Plan de contingencia en caso de no acceso al sitio web. 56

Anexo N°6: Procedimiento de monitoreo y registro de visitas en sala de servidores. 57

Anexo N°7: Formulario solicitud de cambios de sistemas 59

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION

OBJETIVOS

La política de la Seguridad de la Información de Puertos de Talcahuano tiene como objetivo establecer los criterios y lineamientos sobre el manejo de la Seguridad de la Información atingentes a la función de la institución. De esta política nacen y se basan diversas políticas, procedimientos y normativas, que definen las acciones aplicadas, de acorde y en conocimiento del Directorio y la Gerencia, quienes manifiestan su compromiso para la ejecución de esta visión de seguridad de la información.

El Directorio, además, reconoce como relevantes los riesgos relacionados con la seguridad de la información, y en tal sentido emite la presente política general de seguridad de la información.

ALCANCE

Esta Política de Seguridad de la Información aplica a todo trabajador y trabajadora, proceso, sistema o entidad que interactúe con información de la Empresa, independiente su soporte o criticidad, siendo responsabilidad de toda la comunidad de Puertos de Talcahuano, sin importar su orden jerárquico, la difusión de las disposiciones aprobadas en dichas políticas, como velar por su correcto cumplimiento.

DEFINICIONES

a) Actualización, publicación y difusión

Las presentes políticas, procedimientos y normativas serán revisadas y evaluadas al menos una vez al año, o cada vez que sea necesario, por el Directorio o por quien éste designe. El Oficial de Seguridad será responsable de publicar las presentes políticas y planes en la Extranet corporativa de la Empresa y mantenerlas permanentemente actualizadas.

b) Comité de Seguridad

Este Comité es responsable de definir y establecer los lineamientos generales de seguridad, publicar y aprobar las políticas, procedimientos, normativas y nuevas definiciones en lo que respecta a

Seguridad de la Información. También son los responsables de evaluar técnicamente las propuestas, participar en procesos de evaluación de riesgos, recomendar planes de acción y atender contingencias.

Cualquier modificación sustantiva a las presentes Políticas Generales de Seguridad de la Información deberán ser aprobadas por el Directorio de la Empresa.

c) Composición del Comité, roles y responsabilidades.

Al contar con un integrante del Directorio de la empresa, este comité es denominado como Comité de Directorio.

El Comité de seguridad de la información este compuesto de la siguiente manera:

Integrante	**ROL**	**Responsabilidades claves**
Alejandro Tudela Roman.	Director	- Disponibilizar los recursos necesarios para el funcionamiento del Comité. - Nutre una cultura que promueve el comportamiento Ético en normas de seguridad de la información.
Cristian Wulf Sotomayor	Gerente General	- Organizar los recursos de la entidad. - Planeación de las actividades del Comité que se desarrollen dentro de la empresa.
Aturo Morello Fuentes	Oficial de seguridad de la información	- Brindar los servicios de seguridad en la organización, a través de la planeación, coordinación y administración de los procesos de seguridad informática - Velar por la implementación de los controles de seguridad en las plataformas tecnológicas que se utilizan para la disposición, control y manejo de la información. - Gestionar la resolución de conflictos que se generen en materia de seguridad de la información. - Monitorear el funcionamiento adecuado de las políticas de seguridad de la información. - Mantener la coordinación con otros departamentos y unidades de la

		organización para apoyar al cumplimiento de los objetivos de seguridad. - informar y reportar a dirección cualquier cuestión relacionada con la ciberseguridad. - El oficial de seguridad puede solicitar a empresas externas evaluar el cumplimiento de las políticas y controles relacionados a seguridad de la información.
Gonzalo Gacitúa Vásquez	Encargado de informática	- Alinear la estrategia de ciberseguridad con los objetivos de la empresa. - Mantener actualizadas las políticas de seguridad de la información de la empresa. - Mantener la actualización de inventario de activos de información de la organización de acuerdo con los procedimientos definidos. - Mantener informado periódicamente al comité directivo y operativo de la seguridad e información acerca del estado del sistema de seguridad de la información. - Ejecutar, aplicar e implementar las medidas de ciberseguridad que sean instruidas por la alta dirección. - Difundir la política de seguridad de la información a todo el personal.
Evelyn Domínguez Jara	Asesor interno de tecnologías y seguridad de la información.	- Proponer mejoras a las actividades relacionadas a seguridad de la información. - Recomendar mejoras técnicas y de ejecución de proyectos informáticos presentados en el comité. - Asesorar al comité en temas relacionados a infraestructura y lenguajes de desarrollo de software. - Revisar y proponer mejoras a las políticas de seguridad de la información.

NORMATIVAS

a) Normativa de Seguridad de los Recursos Humanos

El Oficial de Seguridad deberá informar, educar y concientizar a todos los trabajadores y trabajadoras relacionados con la empresa sobre lo que se espera de ellos en materias de Seguridad de la Información. Se busca minimizar los riesgos ocasionados por los trabajadores y trabajadoras de la Empresa, tales como manipulación de la información, hurto, fraudes o mal uso de las plataformas tecnológicas (sistemas, hardware), como en contra de los trabajadores y trabajadoras de la empresa, como por ejemplo filtración o pérdida de datos sensibles o estratégicos.

El objetivo es crear conciencia entre los trabajadores y trabajadoras de los riesgos que eventualmente amenazan la información con la que trabajan capacitándolos continuamente, estableciendo mecanismos de prevención, identificación y notificación de incidentes de seguridad.

b) Normativa de Seguridad Física y Ambiental

El Oficial de Seguridad identificará los riesgos asociados al acceso físico a las instalaciones y arquitectura tecnológica de la empresa por parte de trabajadores, trabajadoras y terceros (socios de negocio, proveedores, otros), con el objeto de prevenir el acceso no autorizado, daño e interferencia a las instalaciones de la empresa y a la información.

Además, se asegurará la protección física de los activos tecnológicos y de información, que afectan los procesos, las comunicaciones y la conservación de los datos de la Empresa.

c) Normativa de Gestión de las Comunicaciones y las Operaciones

Generar y definir por una parte procedimientos y responsabilidades operacionales con el objeto de asegurar la correcta operación de los medios de procesamiento de la información y por otra implementar políticas de respaldo y restauración de los datos en forma oportuna.

Si corresponde, el Oficial de Seguridad debe implementar una segregación funcional para reducir el Riesgo de negligencia o uso malicioso de los sistemas.

El Oficial de Seguridad debe asegurar la protección de la información transmitida a través de correo electrónico y la infraestructura que lo soporta.

d) Normativa de Control de Acceso

El Oficial de Seguridad debe asegurar que el acceso de los usuarios y usuarias es debidamente autorizado y evitar el acceso no autorizado a los sistemas de información, estableciendo procedimientos formales de control en la asignación de los derechos de acceso a los sistemas de información.

Todas las etapas en el ciclo de vida del acceso del usuario deben estar contempladas en estos procedimientos, esto es, desde el registro inicial de nuevos usuarios y usuarias hasta la baja de los mismos porque que ya no requieren acceso a los sistemas de información.

Poner especial atención en la asignación de derechos de acceso con privilegios que puedan permitir a los usuarios y usuarias superar los controles del sistema.

Implementar una política de escritorio y pantalla limpios de manera que por una parte reducir el riesgo de acceso no autorizado y por otra, robo o daño a los papeles u otros medios de almacenamiento de la información.

e) Normativa de Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

En los Sistemas de Información están incluidos sistemas operativos, infraestructura, aplicaciones para el negocio, servicios y aplicaciones desarrolladas internamente por la Empresa. El diseño e implementación del sistema de información que soporta el proceso de negocio puede ser crucial para la seguridad. Se deben identificar y acordar todos los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información en la fase de requerimientos de un proyecto; y deben ser justificados, acordados y documentados como parte de las formalidades para un sistema de información.

Las empresas que desarrollan el software internamente o bien, contraten el desarrollo a una empresa externa, deben garantizar que la seguridad sea parte de los sistemas de información desarrollados e incluirlos en la etapa de las especificaciones del software.

f) Normativa de Gestión de la Continuidad del Negocio

El Oficial de Seguridad debe considerar los aspectos de la seguridad de la información de la gestión de la continuidad operativa de manera de hacer frente a las interrupciones de las actividades institucionales y proteger los procesos críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

El Oficial de Seguridad debe implementar el proceso de gestión de la continuidad del negocio para minimizar el impacto sobre la compañía y lograr recuperarse de la pérdida de activos de información (lo cual puede ser resultado de, por ejemplo, ausencia del oficial de seguridad y/o encargado o encargada de informática, desastres naturales, accidentes, fallas del equipo y acciones deliberadas) hasta un nivel aceptable a través de una combinación de controles preventivos y de recuperación.

g) Normativa de Gestión de Incidentes en la Seguridad de la Información

El Oficial de Seguridad se debe asegurar que las debilidades, problemas y eventos de seguridad de la información asociados a los sistemas de información sean comunicados en forma oportuna de modo de permitir tomar acciones correctivas a tiempo.

Para lo anterior se deben seguir los siguientes pasos:

- El Oficial de Seguridad será el responsable de comunicar inmediatamente por cualquier medio disponible de la ocurrencia de un incidente de seguridad de la información al Comité de Seguridad y propondrá una solución.
- Una vez evaluada la solución por el Comité de Seguridad serán tomadas las medidas correctivas que permitan subsanar el incidente.
- El Comité de seguridad informará al Directorio en la sesión más próxima de la ocurrencia de incidentes relevantes y las medidas adoptadas para su solución.

CUMPLIMIENTO DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La presente Política será incluida en los planes anuales de Auditoría Interna para su revisión, sin embargo y ante los dinámicos cambios o acciones que se deban realizar ante eventualidades o normativas a nivel país, estas pueden ser mejoradas continuamente en cualquier momento, siendo

responsabilidad de la alta dirección, o quien corresponda, la difusión de las modificaciones realizadas.

POLÍTICAS ESPECIFICAS DE SEGURIDAD DE LA INFORMACIÓN

Para cumplir con una correcta ejecución de los procesos que involucran el flujo de información de la compañía, se han definido políticas específicas que apoyan y aseguran una segura forma de trabajar con Tecnologías de Información dentro de la compañía.

Se han generado varias formas de documentos, que ayudan a una mejor evaluación y mejora continua de los distintos procesos de Tecnologías de Información dentro de la compañía. Los tipos de documentos son los siguientes:

- Políticas
- Directivas
- Procedimientos

Estos documentos aseguran el principio básico establecido en la Política General de Seguridad de la Información.

Tipo de Documento	Política		
Nombre	*POL001 - Política de Acceso a Extranet, Internet y Almacenamiento en la Nube*	Versión 6	Diciembre 2023
Descripción	Puertos de Talcahuano establece las directrices para la utilización de los servicios de Extranet, internet y almacenamiento en la Nube. Todos los usuarios y usuarias de estos servicios son completamente responsables por la aplicación de estas directrices y de igual manera deben velar por la correcta aplicación de las diferentes políticas, procedimientos, controles, normas y buenas prácticas definidas para garantizar la integridad, confidencialidad y disponibilidad de la información.		
Objetivos	Establecer las directrices para todos los usuarios y usuarias de Puertos de Talcahuano para la adecuada utilización de los servicios de Internet, Extranet y Almacenamiento en la Nube.		
Alcance	Todos los trabajadores y trabajadoras de Puertos de Talcahuano. Proveedores y Terceros que accedan a Extranet, Internet y Almacenamiento en la Nube.		
Directrices Asociadas	DIR001 - Uso de Extranet DIR002 - Uso de Internet DIR003 - Almacenamiento en la Nube		
Responsable de su revisión	Encargado de Seguridad de la Información		
Responsable de su Aprobación	Comité de Seguridad de la Información Directorio Puertos de Talcahuano		

Tipo de Documento	Política		
Nombre	*POL002 - Política de Gestión de Contraseñas*	Versión 6	Diciembre 2023
Descripción	Las contraseñas son un medio común de verificación de la identidad de un usuario antes de darle acceso a un sistema o servicio de información.		
Objetivos	El propósito de esta política es establecer los lineamientos para el uso, manejo de cambios y elaboración de contraseñas seguras.		
Alcance	Todos los trabajadores y trabajadoras de Puertos de Talcahuano.		
Directrices Asociadas	DIR004 – Criterios de Selección de Contraseñas Seguras		
Responsable de su revisión	Encargado de Seguridad de la Información		
Responsable de su Aprobación	Comité de Seguridad de la Información Directorio Puertos de Talcahuano		

Tipo de Documento	Política		
Nombre	*POL003 - Política de Acceso a la Red de Datos.*	Versión 6	Diciembre 2023
Descripción	Las Bases de Datos, archivos almacenados en discos duros o medios extraíbles que contengan o relacione información de la empresa son de carácter privado y requieren de un manejo confidencial de las mismas.		
Objetivos	El propósito de esta política es establecer los lineamientos para el acceso a la red de datos de Puertos de Talcahuano.		
Alcance	Todos los trabajadores y trabajadoras de Puertos de Talcahuano.		
Directrices Asociadas	DIR005 – Acceso General a la Red de Datos DIR006 – Acciones a cumplir para acceder a la Red de Datos PRO001 – Creación de usuarios en la Red de Datos Puertos de Talcahuano PRO002 – Creación de usuarios en la Base de Datos Puertos de Talcahuano PRO003 – Creación de usuarios en el Sistema FIN700 de Puertos de Talcahuano PRO004 – Eliminación de usuarios en la Red de Datos Puertos de Talcahuano PRO005 – Eliminación de usuarios en la Base de Datos Puertos de Talcahuano PRO006 – Eliminación de usuarios en el Sistema FIN700 de Puertos de Talcahuano		
Responsable de su revisión	Encargado de Seguridad de la Información		
Responsable de su Aprobación	Comité de Seguridad de la Información Directorio Puertos de Talcahuano		

Tipo de Documento	Política		
Nombre	*POL004 - Política de Respaldos Institucionales*	Versión 6	Diciembre 2023
Descripción	Puertos de Talcahuano implementa la presente política con el propósito de contrarrestar las interrupciones que se puedan presentar en los sistemas de información de la compañía, protegiendo sus procesos críticos contra los efectos de fallas importantes y desastres, asegurando su recuperación oportuna, manteniendo la confidencialidad, integridad y disponibilidad de la información de la empresa		
Objetivos	Proteger, garantizar y asegurar la disponibilidad de la información digital almacenada en los diferentes dispositivos suministrados por la compañía, con el objetivo de que se mantenga respaldada y sea fácilmente recuperable en el momento que sea requerido.		
Alcance	Todos los trabajadores y trabajadoras de Talcahuano.		
Directrices Asociadas	DIR007 – Consideraciones Generales de Respaldo. PRO007 – Respaldo de Bases de Datos PRO008 – Respaldo de Datos de Usuarios PRO009 – Respaldo de Software y Sistemas Operativos PRO010 – Almacén de respaldos realizados PRO011 – Recuperación de un respaldo de la Base de Datos PRO012 – Recuperación de un respaldo de Datos de Usuarios		
Responsable de su revisión	Encargado de Seguridad de la Información		
Responsable de su Aprobación	Comité de Seguridad de la Información Directorio Puertos de Talcahuano		

Tipo de Documento	Política		
Nombre	*POL005 - Política de Uso del Correo Electrónico Corporativo.*	Versión 6	Diciembre 2023
Descripción	Es una de las herramientas más utilizadas al interior de la compañía para establecer comunicación con los trabajadores, trabajadoras y proveedores, debido a su nivel de utilización lo convierte en uno de los medios más utilizados de difusión de software malicioso y de contenidos no solicitados que atentan contra la seguridad de la información que se transmite por este medio de comunicación.		
Objetivos	Establecer los lineamentos para el buen uso del correo electrónico corporativo permitiendo garantizar la seguridad de la información que se intercambia por medio de este servicio. Garantizar la implementación de las mejores prácticas en la utilización del servicio de correo electrónico.		
Alcance	Todos los trabajadores y trabajadoras de Puertos de Talcahuano		
Directrices Asociadas	DIR008 – Consideraciones Generales en el uso del correo electrónico corporativo.		
Responsable de su revisión	Encargado de Seguridad de la Información		
Responsable de su Aprobación	Comité de Seguridad de la Información Directorio Puertos de Talcahuano		

Tipo de Documento	Política		
Nombre	*POL006 - Política de Escritorio Despejado y Pantalla Despejada.*	Versión 6	Diciembre 2023
Descripción	Esta política sirve para reducir los riesgos de acceso no autorizado, pérdida o daño a la información durante y fuera de las horas normales de trabajo. Archivadores, cajoneras u otras formas de almacenamiento seguro pueden también proteger la información almacenada dentro de ellas contra desastres tales como incendios, terremotos, inundaciones o explosiones.		
Objetivos	Establecer las directrices que los trabajadores y trabajadoras de Puertos de Talcahuano deben seguir para mantener la integridad, disponibilidad y confidencialidad de la información.		
Alcance	Todos los trabajadores y trabajadoras de Puertos de Talcahuano		
Directrices Asociadas	DIR009 – Actividades de Limpieza del Escritorio DIR010 – Actividades de Limpieza de Pantalla		
Responsable de su revisión	Encargado de Seguridad de la Información		
Responsable de su Aprobación	Comité de Seguridad de la Información Directorio Puertos de Talcahuano		

Tipo de Documento	Política		
Nombre	*POL007 - Política de Gestión Ante Vulnerabilidades y Ciberseguridad*	Versión 6	Diciembre 2023
Descripción	Esta política de Puertos de Talcahuano define las directrices para llevar a cabo la gestión de vulnerabilidades técnicas como proceso continuo para asegurar el adecuado funcionamiento de cada uno de los dispositivos que forman parte de la plataforma tecnológica con el propósito de asegurar el adecuado funcionamiento y gestión de las operaciones del negocio, así como también registrar los riegos apreciables que pueden ser incorporados mediante el análisis de vulnerabilidades sobre los activos.		
Objetivos	Definir las directrices para llevar a cabo la identificación, seguimiento, control y atención de las vulnerabilidades técnicas identificadas mediante la realización de pruebas de Ethical Hacking y Análisis de Vulnerabilidades internas y externas ejecutados en los diferentes sistemas de información, dispositivos conectados a la red y plataformas tecnológicas, con el propósito de mantener un aseguramiento adecuado de la plataforma tecnológica, mitigando siempre que sea posible los diferentes riesgos asociados a las vulnerabilidades identificadas.		
Alcance	Todos los trabajadores y trabajadoras de Puertos de Talcahuano.		
Directrices Asociadas	DIR011 – Gestión de Vulnerabilidades Técnicas DIR012 – Test o Pruebas de Vulnerabilidad DIR013 – Test de Penetración Internos y Externos DIR014 – Escaneo de puntos de acceso inalámbrico no autorizados		
Responsable de su revisión	Encargado de Seguridad de la Información		
Responsable de su Aprobación	Comité de Seguridad de la Información Directorio Puertos de Talcahuano		

Tipo de Documento	Política		
Nombre	*POL008 - Política de Mensajería Instantánea y Videoconferencias.*	Versión 6	Diciembre 2023
Descripción	Puertos de Talcahuano, restringe el uso de programas de Mensajería Instantánea, para estos efectos los programas seleccionados por la empresa para uso de mensajería instantánea y videoconferencias son Microsoft Team, Zoom y Meet.		
Objetivos	Establecer los lineamentos para la correcta utilización del servicio de mensajería instantánea por parte de los trabajadores y trabajadoras de Puertos de Talcahuano. Garantizar la seguridad de la información mediante la implementación de buenas prácticas al hacer uso de programas de mensajería instantánea minimizando los riesgos que se puedan presentar.		
Alcance	Todos los trabajadores y trabajadoras de Puertos de Talcahuano.		
Directrices Asociadas	DIR015 – Uso de Mensajería Instantánea y Videoconferencias.		
Responsable de su revisión	Encargado de Seguridad de la Información		
Responsable de su Aprobación	Comité de Seguridad de la Información Directorio Puertos de Talcahuano		

Tipo de Documento	Política		
Nombre	*POL009 – Política de Adquisición de Hardware y Software.*	Versión 6	Diciembre 2023
Descripción	Puertos de Talcahuano norma la forma de adquirir nuevos activos de Hardware y Software para la compañía.		
Objetivos	• Definir las directrices que se deben tener en cuenta para la selección y adquisición de Hardware y Software con el fin de propender por un crecimiento organizado y estructurado de la arquitectura Tecnológica de la empresa. • Se entiende como Hardware cualquier elemento activo que forme parte de la Infraestructura de Comunicación y Sistemas de Información existentes, tales como Equipos de Cómputo, Servidores, Switches, Routers, Access Point, Firewalls, Dispositivos de Almacenamiento como SAN y NAS, Equipos de Videoconferencia, Plantas Telefónicas, y demás relacionados. • La política proporciona además los lineamientos a tener en cuenta al momento de adquirir algún software de propósito específico para la compañía, garantizando siempre que se cumpla con la normatividad legal vigente respecto de los temas de Licenciamiento. • Cuando un Software se vuelve crítico para los Procesos de Operación del negocio y contiene parametrizaciones y/o desarrollos a la medida, se convierte en un Sistema de Información, el cual debe tener tratamiento diferente.		
Alcance	Todos los trabajadores y trabajadoras de Puertos de Talcahuano.		
Documentos Asociados	DIR016 – Aspectos Generales a considerar para la correcta adquisición y asignación de equipamiento tecnológico. DIR017 – Consideraciones a seguir para la correcta adquisición y asignación de Hardware. DIR018 – Consideraciones a seguir para la correcta adquisición y utilización de Software y Sistemas de Información.		
Responsable de su revisión	Encargado de Seguridad de la Información		
Responsable de su Aprobación	Comité de Seguridad de la Información Directorio Puertos de Talcahuano		

Tipo de Documento	Política		
Nombre	*POL010 – Política de control de cambios a sistemas*	Versión 6	Diciembre 2023
Descripción	Puertos de Talcahuano norma la forma de controlar los camios asociados a sus sistemas informáticos tanto internos como externos.		
Objetivos	Definir cómo se controlan los cambios en los sistemas de información.		
Alcance	Todos los sistemas internos o externos de Puertos de Talcahuano.		
Documentos Asociados	DIR018 – Consideraciones a seguir para la correcta adquisición y utilización de Software y Sistemas de Información. DIR019 – Cambios o actualizaciones de sistemas de información		
Responsable de su revisión	Encargado de Seguridad de la Información		
Responsable de su Aprobación	Comité de Seguridad de la Información Directorio Puertos de Talcahuano		

Tipo de Documento	Política		
Nombre	*POL011 – Política de dispositivos móviles y teletrabajo*	Versión 6	Diciembre 2023
Descripción	Esta política tiene la finalidad de reglamentar el uso de los dispositivos móviles y medios removibles disponibles a los trabajadores y trabajadoras de Puertos de Talcahuano, a fin de minimizar los riesgos asociados a estos.		
Objetivos	Definir cómo se controlan los riesgos de seguridad de la información implícitos en el uso de dispositivos móviles. Específicamente, se pretende restringir el uso de dispositivos móviles y medios removibles a sólo aquellos de propiedad o en modalidad de arriendo de Puertos de Talcahuano, evitando la utilización de dispositivos particulares que pudieren afectar la confidencialidad de la información.		
Alcance	Todos los activos de información y funcionarios que tienen signado equipos móviles en Puertos de Talcahuano.		
Documentos Asociados	DIR020 – Directivas de uso de dispositivos móviles y teletrabjo		
Responsable de su revisión	Encargado de Seguridad de la Información		
Responsable de su Aprobación	Comité de Seguridad de la Información Directorio Puertos de Talcahuano		

DIRECTIVAS ESPECIFICAS DE SEGURIDAD DE LA INFORMACIÓN

Tipo de Documento	**Directiva**		
Nombre	DIR001 - Uso de Extranet	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL001 - Política de Acceso a Extranet, Internet y Almacenamiento en la Nube.		
Objetivos	Definir el correcto uso del servicio de Extranet dentro de Puertos Talcahuano.		

- La aprobación de los contenidos, así como la vigencia de la información y contenidos de las publicaciones oficiales que la Extranet presenta es de responsabilidad de la Gerencia de Administración y Finanzas.
- La información disponible en la Extranet es para uso interno y no puede ser reproducida o retransmitida a terceros. Es responsabilidad de cada usuario del servicio el correcto manejo de la información mostrada en el servicio de Intranet.

Tipo de Documento	**Directiva**		
Nombre	DIR002 - Uso de Internet	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL001 - Política de Acceso a Intranet, Extranet y Almacenamiento en la Nube.		
Objetivos	Definir el correcto uso del servicio de Internet dentro de Puertos Talcahuano.		

- Todos los Usuarios y usuarias de la Empresa (trabajador y trabajadora de la Empresa, o quién esté autorizado, según políticas de acceso) tienen acceso a internet para potenciar su trabajo, en beneficio de la Compañía.
- El servicio de Internet esta designado para el uso en la investigación y búsqueda de información relacionada a las funciones de su cargo.
- Con el propósito de garantizar la seguridad de la información y de la infraestructura tecnológica de la compañía, Puertos de Talcahuano se reserva el derecho de filtrar el contenido al que el usuario puede acceder a través de internet desde los recursos y servicios propiedad de la compañía, así como a monitorizar y registrar los accesos realizados desde los mismos.
- De ser necesario que un usuario o usuaria requiera acceder a un sitio restringido debe informar vía correo electrónico al Encargado o Encargada de Informática (manteniendo en copia el Gerente o Gerenta de Administración y Finanzas) quien deberá revisar la solicitud para su posterior aprobación o denegación.
- Por motivos de seguridad y para evitar la infección de virus, se prohíbe la descarga de software desde Internet.

- De ser necesaria la descargar de información desde internet los usuarios y usuarias deberán respetar y dar cumplimiento a las disposiciones legales de derechos de autor, marcas registradas y derechos de propiedad intelectual.
- Está prohibido la descarga de material gráfico que contenga actividad sexual, nudismo, violencia o cualquier otra actividad que vaya en contra de los valores corporativos de la compañía.
- Es responsabilidad de los trabajadores y trabajadoras de Puertos de Talcahuano, proveedores, y terceras partes a quienes se les otorgue acceso al servicio de internet hacer buen uso de los recursos informáticos que la compañía le suministra para el desarrollo de sus actividades.
- Es responsabilidad de los trabajadores y trabajadoras de Puertos de Talcahuano, proveedores, y terceras partes a quienes se les otorgue acceso al servicio de internet no gestionar inscripciones a boletines y/o notificaciones vía correo electrónico que no se encuentren asociadas estrictamente a temas laborales.

Tipo de Documento	**Directiva**		
Nombre	DIR003 - Uso de Almacenamiento en la Nube.	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL001 - Política de Acceso a Extranet, Internet y Almacenamiento en la Nube.		
Objetivos	Definir el correcto uso del servicio de Almacenamiento en Nube provisto por Puertos de Talcahuano.		

- No se permite almacenar en el sitio corporativo (OneDrive para la Empresa) información personal que no corresponda a asuntos propios de la actividad laboral realizada en la compañía.
- Es responsabilidad del usuario al que se asignó la cuenta dar un adecuado manejo a la información almacenada en (OneDrive para la Empresa) así como asignar y gestionar los permisos que asignen a otras personas para acceder a la información almacenada.
- Se define Onedrive como el espacio y la herramienta de almacenamiento de información corporativo, ya que dentro de las características del servicio es contar con los respaldos adecuados de los datos.
- Toda la información relacionada al negocio de la empresa debe ser almacenada en Onedrive
- Si la cuenta debe ser eliminada, es responsabilidad del usuario al que se asignó la cuenta, facilitar la custodia de la información entregando copia de esta a su jefe inmediato.

Tipo de Documento	Directiva		
Nombre	DIR004 – Criterios de Selección de Contraseñas Seguras	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL002 - Política de Gestión de Contraseñas.		
Objetivos	Definir criterios a utilizar en las contraseñas de acceso a los sistemas de información provistos por Puertos de Talcahuano.		

- La longitud de la contraseña debe ser mínima de 6 caracteres.
- Las aplicaciones en las cuales la tecnología utilizada no contemple una longitud mínima de seis caracteres, la longitud mínima deberá ser la máxima contemplado por el sistema.
- La contraseña debe estar compuesta por una combinación de letras Mayúsculas, minúsculas, caracteres numéricos y símbolos especiales como los siguientes: ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [] \ : " ; ' < > ? , . /
- La contraseña asignada no debe ser igual a 10 contraseñas utilizadas anteriormente.
- La contraseña se debe cambiar obligatoriamente cada 90 días del último cambio registrado.
- Nunca debe compartirse la contraseña con otras personas, por ejemplo, amigos, parientes o compañeros y compañeras de trabajo. Él hacerlo expone a las consecuencias por las acciones que los otros hagan con esa contraseña. Esto apoya a la correcta gestión de credenciales.
- No se debe utilizar una única contraseña para todos los propósitos.
- La autenticación de la contraseña deberá implementarse para todos los usuarios y usuarias que accedan a los sistemas, redes internas y externas.
- Cuando se utilicen contraseñas para autenticación, las mismas deberán ser cambiadas al menos cada 90 días.
- Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarse inmediatamente.
- No deben usarse contraseñas que sean idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.
- Es responsabilidad del administrador o administradora del sistema comunicar la contraseña asignada al usuario o usuaria de la manera más confidencial que sea posible.
- No se debe escribir la contraseña en papeles y dejarla en sitios donde pueda ser encontrada.
- El usuario o usuaria debe cerrar su sesión de forma manual cada vez que se ausente del puesto de trabajo.
- Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número consecutivo de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada debe quedar bloqueada o suspendida y se debe alertar al administrador del sistema para realizar su debida gestión.
- Las contraseñas deben cambiarse cuando una persona que tiene acceso a cuentas privilegiadas compartidas ha sido relevada de sus deberes a causa de alguna actividad sospechosa o se ausenta por un periodo extenso (permiso, licencia o vacaciones).
- Los usuarios deberán recibir un aviso por parte de la aplicación de por lo menos 5 días antes que expire la contraseña.

Tipo de Documento	Directiva		
Nombre	DIR005 – Acceso General a la Red de Datos	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL003 - Política de Acceso a la Red de Datos.		
Objetivos	Definir el correcto uso de acceso general para unirse a la Red de Datos de Puertos de Talcahuano.		

- Los equipos computacionales de tipo desktop asignados por la empresa deben estar conectados a la red LAN o WIFI privada corporativa. La conexión a cualquier otra red de información o dispositivo que permita el acceso a internet está prohibida.
- Para los tipos de usuarios y usuarias del Directorio Activo y FIN 700 se establece como control la revisión de cuentas con una periodicidad de dos veces al año.
- La red inalámbrica se encuentra segmentada para usuarios o usuarias de la empresa y usuarios o usuarias invitados e invitadas:

- Red inalámbrica Portuaria: Red de carácter privada de uso exclusivo para laptop de la empresa. La contraseña de esta red es de carácter privado.
- Red inalámbrica Portuaria INVITADOS: Red de carácter público para uso de visitas. La contraseña de conexión estará disponible en la recepción.

- Los equipos computacionales de tipo laptop asignados por la empresa deben estar conectados a la red LAN corporativa o a la red inalámbrica privada PORTUARIA. Los usuarios y usuarias que requieran hacer uso de internet estando fuera de las oficinas deben conectarse en modo de anclaje de red al celular o router asignado por la empresa. La conexión a cualquier otra red de información o dispositivo que permita el acceso a internet está prohibido.

Tipo de Documento	Directiva		
Nombre	DIR006 – Acciones a Cumplir para acceder a la red de Datos	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL003 - Política de Acceso a la Red de Datos		
Objetivos	Definir las acciones para unirse correctamente a la Red de Datos de Puertos de Talcahuano.		

- Asignar un nombre que identifique cada Pc que utilice la red de datos.
- Disponer de un listado de software y su categoría que utiliza la Empresa.
- La nomenclatura para identificar al usuario o usuaria en la red de datos que utilizas sus recursos es: Xnn..n, donde x es la primera letra del primer nombre (o segundo nombre; y n es el apellido paterno (o materno).
- Existen dos niveles de acceso a una red de datos: Una es usar los recursos de la red y la otra es el acceso a los sistemas de información de la empresa. Cada uno de esos niveles necesita de una palabra clave denominada PASSWORD para ingresar, es decir, solo pueden acceder personas autorizadas para ello.

Tipo de Documento	Directiva		
Nombre	DIR007 – Consideraciones Generales de Respaldo	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL004 - Política de Respaldos Institucionales.		
Objetivos	Definir los aspectos generales asociados a la realización de Respaldos de Información dentro de Puertos de Talcahuano.		

- El sistema ERP FIN 700 se respaldará de forma diaria. Esta tarea será ejecutada por la empresa SONDA.
- Se solicitará a la empresa SONDA verificar que los respaldos del ERP se estén realizando de manera optima y en los plazos establecidos. Para esto, el encargado de informática solicitará evidencia mediante correo electrónico a al empresa prestadora del servicio.
- Los Respaldos de datos en forma externa, denominada DATACENTER, se harán en un lugar apropiado para ello, servicio que es provisto por terceros, quienes cuentan y tienen implementados los procedimientos de seguridad para transportar, almacenar y recuperar datos.
- Es responsabilidad del Encargado de Informática garantizar que se cuente con la disponibilidad de la plataforma requerida para llevar a cabo el almacenamiento y copia de respaldo de la información contenida en los servidores de archivos de la compañía.

Tipo de Documento	Directiva		
Nombre	DIR008 – Consideraciones Generales en el uso del correo electrónico corporativo.	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL005 - Política de Uso del Correo Electrónico Corporativo.		
Objetivos	Definir las consideraciones generales y el correcto uso del servicio de Correo Electrónico de Puertos de Talcahuano.		

- Los trabajadores y trabajadoras de Puertos de Talcahuano son completamente responsables de todas las actividades realizadas con sus cuentas de correo electrónico asociadas al dominio @puertotalcahuano.cl.
- Se debe ser respetuoso y utilizar un vocabulario adecuado al momento de redactar un correo electrónico.
- La cuenta de correo electrónico que proporciona Puertos de Talcahuano es personal e intransferible, por lo que no debe proporcionarse a otras personas.
- No está permitido distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para la compañía o correos SPAM de cualquier índole. Se consideran correos SPAM aquellos no relacionados con las funciones específicas a los procesos de trabajo.
- Para efectos de esta política, se entenderá por correo masivo aquellos envíos que cumplan con las siguientes características:
  - Que tengan como destinatarios toda una empresa.
  - Envíos a listados personalizados que contengan más de 100 destinatarios.
- No se deben enviar o reenviar mensajes con contenido difamatorio, ofensivo, racista u obsceno.
- No se deben usar seudónimos y enviar mensajes anónimos, así como aquellos que consignen títulos, cargos o funciones no oficiales.
- No se permite utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del emisor de correo.
- Si se recibe un correo de origen desconocido, se debe informar al Encargado o Encargada de Informática, bajo ningún aspecto se debe abrir o ejecutar archivos adjuntos de correos dudosos, ya que podrían contener códigos maliciosos (virus, troyanos, keyloogers, gusanos, etc.).
- No abra los mensajes que le ofrezcan dudas en cuanto a su origen o posible contenido sin asegurarse que han sido analizados por el software antivirus de la compañía.
- No proporcione su dirección de correo electrónico si no está seguro de las intenciones de aquél que se la requiere.
- Evite difundir cuando no sea necesario las direcciones de correo electrónico de otras personas.
- Es responsabilidad de los trabajadores y trabajadoras hacer un adecuado uso, consulta o transmisión del correo electrónico el cual debe ser utilizado exclusivamente para las actividades relacionadas con el trabajo y funciones a cargo.

- Es responsabilidad de los Gerentes o Gerentas de Área ante un retiro de un trabajador o trabajador a su cargo, solicitar la entrega formal de la información de la compañía, previa a la fecha de retiro de la empresa por parte del colaborador.
- Es responsabilidad de los Gerentes o Gerentas de Área ante el incumplimiento del punto anterior, tramitar previo al retiro del trabajador o trabajadora, la autorización firmada por el trabajador o trabajadora para acceso a la cuenta del correo electrónico e información que se encuentre a su cargo de no contar con esta autorización no se podrá autorizar el acceso a la información.
- Todo trabajador y trabajadora que por error reciba un mensaje correo electrónico dirigido a otro destinatario, debe devolverlo al remitente de inmediato, protegiendo la información contenida y sin hacer uso indebido de la misma.
- No está permitido el direccionamiento automático, envió o almacenamiento de correos de la empresa en cuentas de correo personales no corporativas.

Tipo de Documento	**Directiva**		
Nombre	DIR009 – Actividades de Limpieza del Escritorio	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL006 - Política de Escritorio Despejado y Pantalla Despejada.		
Objetivos	Definir las actividades a realizar para una correcta mantención del Escritorio.		

- Almacenar de manera segura (con llave u otro control) medios de almacenamiento como (CD/DVD, dispositivos de almacenamiento masivo (memorias USB, discos extraíbles)), papelería y otros elementos que puedan contener información sensible; mientras no estén en uso, en ausencia del responsable o cuando se termine la jornada laboral.
- Los documentos que contengan información sensible se deberían retirar inmediatamente de las impresoras, una vez estos sean impresos.
- No ingresar ni ingerir alimentos en el puesto de trabajo.
- Al finalizar la jornada laboral o al ausentarse del puesto de trabajo se deben asegurar con llave los cajones, gabinetes y/o archivadores.

Tipo de Documento	**Directiva**		
Nombre	DIR010 – Actividades de Limpieza de Pantalla	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL006 - Política de Escritorio Despejado y Pantalla Despejada.		
Objetivos	Definir las actividades a realizar para una correcta mantención de la Pantalla de Trabajo.		

- Ejecutar el bloqueo de pantalla siempre que el trabajador o trabajadora del equipo se ausente de la terminal, ejecutando la combinación de teclas CTRL + ALT + SUPR y seleccionar bloquear equipo.
- Configurar el bloqueo de equipo de manera automática utilizando para ello las propiedades de pantalla, protector de pantalla, seleccionar inicio de sesión o el equivalente.
- Ejecutar el procedimiento de clasificación, etiquetado y manejo de la información de forma segura y ordenada en rutas de acceso recordables.
- Para el trabajador y trabajadora operativo en la pantalla solo deben permanecer los iconos de acceso directo a las diferentes herramientas de gestión de la campaña, no deben permanecer archivos digitales de ningún tipo.

Tipo de Documento	**Directiva**		
Nombre	DIR011 – Gestión de Vulnerabilidades Técnicas	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL007 - Política de Gestión Ante Vulnerabilidades.		
Objetivos	Definir actividades a realizar para gestionar de forma correcta la identificación de Vulnerabilidades Técnicas.		

- Es responsabilidad del Encargado o Encargada de Informática, crear y mantener una actividad regular para identificar las vulnerabilidades técnicas en todos los activos de información de Puertos de Talcahuano.
- Como resultado del procedimiento operativo las normas de configuración de seguridad se deben actualizar, según sea necesario, para reflejar la identificación de nuevas vulnerabilidades.

Tipo de Documento	**Directiva**		
Nombre	DIR012 – Test o Pruebas de Vulnerabilidad	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL007 - Política de Gestión Ante Vulnerabilidades.		
Objetivos	Definir actividades a realizar para gestionar pruebas que permitan identificar nuevas vulnerabilidades.		

- El Encargado o Encargada de Informática es responsable de realizar y/o gestionar la realización del escaneo de las redes internas y externas al menos una vez al año y después de cualquier

cambio significativo en la red (por ejemplo. La instalación de nuevos componentes, los cambios en la topología de la red, las reglas de firewall, actualizaciones de producto).

- Los análisis de vulnerabilidad externa deben ser realizados por un proveedor externo. Los escaneos externos de vulnerabilidad realizados después de cambios en la red y todos los escaneos de vulnerabilidades internas deben ser llevados a cabo por personal interno calificado, a condición de que dicho personal sea independiente organizativamente.

Tipo de Documento	**Directiva**		
Nombre	DIR013 – Test de Penetración Internos y Externos	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL007 - Política de Gestión Ante Vulnerabilidades.		
Objetivos	Definir actividades a realizar para gestionar pruebas que permitan realizar efectivamente test de penetración internos y externos.		

- Las Pruebas de penetración interna y externa a nivel de red y aplicación se deben realizar una vez al año o después de cualquier cambio significativo (como, por ejemplo, la instalación de nuevos componentes del sistema, cambios en la topología de la red, modificaciones en las normas de firewall, actualizaciones de productos).
- El Encargado o Encargada de Informática coordinará la realización de las pruebas de penetración externas e internas usando una empresa de seguridad calificada o una fuente interna calificada que tenga conocimientos en la realización de pruebas de penetración y hacking ético. Si se elige el personal interno para llevar a cabo una prueba de penetración, dicho personal debe estar separado de la administración del entorno a evaluar, así mismo no debe tener responsabilidad alguna sobre el ambiente que se está probando.
- Todas las vulnerabilidades explotables identificadas deben corregirse en el menor tiempo posible, así mismo una vez se confirme su corrección debe repetirse la prueba con el objetivo de validar la remediación de la vulnerabilidad identificada.

Tipo de Documento	**Directiva**		
Nombre	DIR014 – Escaneo de puntos de acceso inalámbrico no autorizados	Versión 6	DIciembre 2023
Política(s) Asociada(s)	POL007 - Política de Gestión Ante Vulnerabilidades.		
Objetivos	Definir actividades a realizar para gestionar pruebas que permitan realizar escanear puntos de acceso inalámbricos no autorizados.		

- Cada cierto tiempo, sin previo aviso, el Encargado o Encargada de Informática debe ejecutar una búsqueda de presencia de puntos de acceso inalámbrico no autorizados en todas las instalaciones de la compañía en las cuales se procesen, almacenen y/o transmitan datos, utilizando una combinación de análisis de redes inalámbricas, inspecciones físicas y lógicas de los componentes del sistema y la infraestructura.

Tipo de Documento	**Directiva**		
Nombre	DIR015 – Uso de Mensajería Instantánea y Videoconferencias.	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL008 - Política de Mensajería Instantánea y Videoconferencias.		
Objetivos	Definir obligaciones en el correcto uso de comunicaciones con mensajería instantánea y videoconferencia.		

- No se pueden enviar o recibir ningún tipo de archivos con usuarios o usuarias externos, solo se intercambiarán mensajes de texto.
- Los trabajadores y trabajadoras solo deben usar la cuenta asignada por licencia de office con nombre de dominio @puertotalcahuano.cl
- Los programas de mensajería instantánea son de uso laboral; se deben utilizar solo para contactar a colaboradores, proveedores o comunicaciones internas del proceso.
- Se prohíbe el uso de vocabulario grotesco, vulgar, intimidación, difamación en los mensajes enviados, se debe ser respetuoso y cordial al escribir para recibir el mismo trato.
- No aceptar invitaciones o link de conexión a páginas desconocidas, muchas de estas invitaciones las utilizan los hackers para descargar Virus, Malware, Spyware (gusanos, troyanos, etc.).
- Es responsabilidad del usuario al cual se le aprobó la utilización del programa de mensajería instantánea garantizar su correcta utilización.
- El programa de mensajería instantánea únicamente podrá ser utilizado por la persona a la que se autorizó su uso y solo deberá ser empleado para actividades laborales.
- No está permitido el ingreso a los programas de mensajería instantánea de las páginas de redes sociales como (hi5, Sonico, MySpace, Orkut, Tuenti, o cualquiera clasificada de este tipo.).

Tipo de Documento	Directiva		
Nombre	DIR016 – Aspectos Generales a considerar para la correcta adquisición y asignación de equipamiento tecnológico.	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL009 - Política de Adquisición de Hardware y Software.		
Objetivos	Definir actividades necesarias para adquirir equipamiento tecnológico en general.		

- Toda solicitud de asignación de Hardware y Software debe realizarla el Gerente o Gerenta de área correspondiente vía correo electrónico dirigido al Gerente o Gerenta de Administración y Finanzas quien debe dar el visto y bueno e informar al Encargado o Encargada de informática de la compra. Esta solicitud se debe informar con al menos dos semanas de anticipación a la fecha requerida de entrega.
- Cada asignación de un equipo de cómputo debe estar soportada con un documento o acta de entrega en la cual se especifica las características del equipo entregado, así como las obligaciones y responsabilidades que el usuario asume al recibir dicha asignación. Este proceso debe ser realizado por el encargado de informática.
- Cuando un trabajador o trabajadora se retira de la compañía debe hacer devolución del equipo que le fue asignado la última vez (de conformidad con el acta de entrega), con los programas y toda la información generada durante el desarrollo de su labor.
- En caso de que un trabajador o trabajadora se retira de la compañía pretenda devolver un equipo de cómputo diferente al que le fue asignado, la empresa se reserva el derecho de cobrarle el valor correspondiente al equipo que le fue entregado según acta. Este proceso será adelantado por parte del área de Recursos Humanos de la compañía.
- Los equipos de cómputo serán asignados a un único usuario o usuaria. En caso que un computador esté configurado para el acceso de más de un usuario o usuaria, los trabajadores y trabajadoras que trabajen en este equipo son igualmente responsables por el cumplimiento de las políticas y directrices definidas por la empresa en cuanto al correcto uso de hardware y software.
- El hardware, software, sistemas de información y los datos, son propiedad de la empresa. Su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la compañía, será sancionado de acuerdo con las normas y reglamento interno de la empresa.

Tipo de Documento	Directiva		
Nombre	DIR017 – Consideraciones a seguir para la correcta adquisición y asignación de Hardware.	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL009 - Política de Adquisición de Hardware y Software.		
Objetivos	Definir actividades necesarias para adquirir y asignar equipamiento tecnológico de tipo Hardware.		

- El Encargado o Encargada de informática debe asegurarse que los equipos adquiridos cuenten con la garantía y licenciamiento solicitado que certifique la legalidad del equipo y el software preinstalado.
- Los equipos que conforman la Infraestructura de Comunicaciones y que a su vez atienden la demanda de acceso a los distintos Sistemas de Información, deben tener una arquitectura tecnológica escalable a nivel de sus componentes de Hardware. Se debe preferir la compra marcas mundialmente conocidas en el mercado y que cuenten con múltiples canales de representación a nivel nacional de tal manera que se pueda garantizar su soporte y mantenimiento a largo plazo.
- Otros requerimientos de Hardware de Redes y Comunicaciones, como Switches, Router´s, Access Point, Dispositivos de almacenamiento NAS / SAN, equipos de Videoconferencia, plantas telefónicas, etc, deben ser solicitados directamente a la Gerencia de Administración y Finanzas.

Tipo de Documento	Directiva		
Nombre	DIR018 – Consideraciones a seguir para la correcta adquisición y utilización de Software y Sistemas de Información.	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL009 - Política de Adquisición de Hardware y Software.		
Objetivos	Definir actividades necesarias para adquirir y utilizar correctamente software y sistemas de información.		

- El uso legal de software es una directriz obligatoria, de estricta adopción y cumplimiento por parte de todos los trabajadores y trabajadoras de la compañía. Es una política de alto impacto para la organización dadas las implicaciones legales que tiene y el compromiso organizacional de hacer uso exclusivo de programas de computador de procedencia segura, debidamente adquiridos e instalados.
- Todo programa de computador antes de ser instalado debe tener la licencia legal de uso debidamente registrada según corresponda de acuerdo con las exigencias del licenciamiento adquirido y las políticas específicas de la casa de software a la que pertenece.
- No toda licencia de software legalmente comprada a nivel personal, es libre de ser utilizada con fines empresariales, ni puede ser empleada para desarrollar trabajos en redes empresariales. Su uso en redes empresariales puede acarrear sanciones o multas para la empresa que permita su utilización.
- Está prohibida la instalación o uso de programas de computador que no estén debidamente autorizados.
- La Gerencia de administración y finanzas es la única autorizada para la evaluación y compra de licencias de programas para computador o Sistemas de Información, siendo la encargada de evaluar el tipo de licenciamiento y las condiciones en que se le puede dar uso a un programa solicitado.
- El Uso de cualquier Software sin Licencia es Ilegal y puede exponer a la Compañía a una Responsabilidad Civil e incluso Penal, por lo que la instalación por parte de un funcionario de cualquier programa no autorizado es una falta grave.
- Toda contratación de desarrollo o implementación un Software o Sistema de Información debe contar con la aprobación de la Gerencia de Administración y Finanzas. En caso que el proyecto sea aprobado debe contar con el liderazgo o direccionamiento del proyecto por parte de un funcionario del departamento acordado con la Dirección.
- Todo “desarrollo de software a la medida” bien sea contratado con terceros o desarrollado por personal de la compañía es considerado “Propiedad Intelectual” de la empresa, por tanto, los derechos de autor, las licencias de uso, el código fuente y demás documentación relacionada con el sistema es propiedad de la organización.

Tipo de Documento	Directiva		
Nombre	DIR019 – Cambios o actualizaciones de sistemas de información	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL010 – Política de control de cambios a sistemas		
Objetivos	Definir actividades necesarias para el control de cambio de software.		

- Cada vez que un sistema requiera modificaciones se deberá notificar al Gerente o Gerenta de Administración y Finanzas y Encargo o Encargada de informática los cambios requeridos a algún sistema en particular. La notificación deberá ser enviada por correo electrónico, adjuntando el anexo numero 5 adjunto en este documento. Una vez autorizados los cambios, se procesadora a realizar las gestiones del cambio del software.

Tipo de Documento	Directiva		
Nombre	DIR020 – Directivas de uso de dispositivos móviles y teletrabajo	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL011 – Política de dispositivos móviles y teletrabajo		
Objetivos	Definir actividades necesarias para el control en el uso de dispositivos móviles.		

- Los dispositivos móviles utilizados son Laptop y Smartphones.
- Los dispositivos móviles serán activos de procesamiento de información, y por tanto deberán incorporarse al registro de inventario de activos.
- El responsable de cada dispositivo móvil, deberá encargarse de la seguridad física de estos, protegiéndolo contra golpes, humedad, u otro factor que pudiere dañarlo.
- El responsable de cada dispositivo móvil, deberá encargarse de no instalar softwares y aplicaciones que no apunten a las tareas para la cual fue asignado el dispositivo móvil.
- Todo dispositivo móvil deberá poseer una contraseña, acorde a lo establecido en el Procedimiento de gestión de contraseñas. En caso de Smartphone, deberán contar con algún método que restrinja el acceso sólo al responsable del dispositivo.
- En caso de pérdida o robo de algún dispositivo móvil, se debe dar aviso inmediato al encargado de seguridad de la información, quien tratará el hecho como un incidente.
- A cada trabajador o trabajadora que tenga asignado un laptop, se le asignara un candado de seguridad para que sea anclado al escritorio, siendo responsabilidad de cada persona su uso.
- Todos los trabajadores y trabajdoras deben dar uso corporativo al computador asignado, incluyendo si ejerce sus labores en modalidad teletrabajo.
- Los equipos móviles deben estar conectados a redes seguras que soliciten contraseña de conexión.

PROCEDIMIENTOS ESPECIFICOS DE SEGURIDAD DE LA INFORMACIÓN

Tipo de Documento	**Procedimiento**		
Nombre	PRO001 – Creación de usuarios y usuarias en la Red de Datos Puertos de Talcahuano	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL003 - Política de Acceso a la Red de Datos		
Objetivos	Agregar nuevos usuarios y usuarias a la Red de Datos de Puertos de Talcahuano para acceder a los diversos servicios en red de la compañía.		

1. Los responsables de solicitar la creación de usuarios y usuarias de red son los Gerentes o Gerentas de área correspondiente utilizando el Anexo 1: Formulario para la creación – Modificación – Eliminación de cuentas de usuario.
2. El Gerente o Gerente del Área solicitará a través de e-mail dirigido al Gerente o Gerenta de Administración y Finanzas la creación de la cuenta de usuario usuaria, identificando al usuario o usuaria con nombre completo, área de trabajo, que Pc va a utilizar y qué restricciones tendrá (ej: No usar internet, etc), si hay uso de correo.
3. El Gerente o Gerenta de administración y finanzas será el encargado de Autorizar la creación del usuario, notificando al Encargado o Encargada de Informática vía correo electrónico.
4. El Encargado o Encargada de Informática con la información del e-mail crea el perfil del usuario o usuaria.
5. El Encargado o Encargada de Informática crea la userid y password de acceso a la red de datos, de acuerdo con las reglas establecidas.
6. Para las cuentas de red se establece como perfil predeterminado el tipo de usuario sin privilegios de administración.
7. El Encargado o Encargada de Informática por instrucción del Gerente o Gerenta de Administración y Finanzas, a través de contacto personal informa al usuario de la userid y password, y le informa de la privacidad de esos datos y su responsabilidad del manejo de datos de la red.

Tipo de Documento	Procedimiento		
Nombre	PRO002 – Creación de usuarios en la Base de Datos Puertos de Talcahuano	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL003 - Política de Acceso a la Red de Datos		
Objetivos	Agregar nuevos usuarios a la Base de Datos de Puertos de Talcahuano para acceder a trabajar con los datos de la compañía.		

1. El Gerente o Gerenta del Área solicitará la creación de usuario(s) a través de correo electrónico dirigido al Gerente o Gerenta de Administración y Finanzas, identificando al usuario o usuaria con nombre completo, área de trabajo, indicando que sistema va a utilizar.
2. El Encargado o Encargada de Informática con la información del e-mail creará una cuenta de usuario en el sistema solicitado.
3. El Encargado o Encargada de Informática por instrucción del Gerente o Gerenta de Administración y Finanzas, deberá completar el perfil del usuario en el mismo sistema a explotar; para ello le informará la userid y su password.
4. El Encargado o Encargada de Informática por instrucción del Gerente o Gerenta de Administración y Finanzas, a través de correo electrónico informa al usuario de la userid y password, y le informa de la privacidad de esos datos y su responsabilidad del manejo de la base de datos.
5. La privacidad y la confiabilidad de la base de datos, entendiendo por ello que el acceso a los datos que se almacenan en ellos solo debe ser manipulados por los usuarios autorizados vía sistema de información, está garantizada por el software propio del sistema del motor de base de datos que esta utiliza y que solo el administrador de la base de datos, en este caso el encargado o encargada de informática tiene el acceso para efecto de su administración técnica de ellos.

Tipo de Documento	Procedimiento		
Nombre	PRO003 – Creación de usuarios en el Sistema FIN700 de Puertos de Talcahuano	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL003 - Política de Acceso a la Red de Datos		
Objetivos	Agregar nuevos usuarios al Sistema FIN700 de Puertos de Talcahuano.		

1. Los responsables de solicitar la creación de usuarios del sistema FIN 700 son los Gerentes o Gerentas de área correspondiente.
2. El Gerente o Gerenta del Área solicitará a través de correo electrónico dirigido al Gerente o Gerenta de Administración y Finanzas la creación de la cuenta de usuario, identificando al usuario o usuaria con nombre completo, área de trabajo.
3. El Gerente o Gerenta de administración y finanzas será el encargado de Autorizar la creación del usuario, notificando al Encargado o Encargada de Informática vía correo electrónico.
4. El Encargado o Encargada de Informática con la información del e-mail crea el perfil del usuario de acuerdo a la matriz de roles y cargos del sistema FIN 700 (Anexo 3).
5. El Encargado o Encargada de Informática crea la userid y password de acceso al sistema acorde a los roles autorizados por cargo.
6. El Encargado o Encargada de Informática por instrucción del Gerente o Gerenta de Administración y Finanzas, a través de contacto personal informa al usuario de la userid y password, y le informa de la privacidad de esos datos y su responsabilidad del manejo de datos de la red.

Tipo de Documento	Procedimiento		
Nombre	PRO004 – Eliminación de usuarios en la Red de Datos Puertos de Talcahuano	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL003 - Política de Acceso a la Red de Datos		
Objetivos	Eliminar usuarios a la Red de Datos de Puertos de Talcahuano		

1. Los responsables de solicitar la eliminación de usuarios de red son los Gerentes o Gerentas de área correspondiente.
2. El Gerente o Gerenta del Área solicitará a través de e-mail dirigido al Gerente de Administración y Finanzas la eliminación de la cuenta de usuario, identificando al usuario con nombre completo.
3. El Encargado o Encargada de Informática con la información del e-mail eliminara el perfil de usuario y su cuenta de correo asociada en el caso de existir.
4. El Encargado o Encargada de Informática registrara en una bitácora la fecha de la eliminación, motivos y datos de la cuenta.
5. El Encargado o Encargada de Informática informara a la Gerencia solicitante y a la Gerencia de administración y finanzas la confirmación de la eliminación de la cuenta de usuario.

Tipo de Documento	Procedimiento		
Nombre	PRO005 – Eliminación de usuarios en la Base de Datos Puertos de Talcahuano	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL003 - Política de Acceso a la Red de Datos		
Objetivos	Eliminar usuarios de la Base de Datos de Puertos de Talcahuano		

1. Los responsables de solicitar la eliminación de usuarios de red son los Gerentes o Gerentas de área correspondiente.
2. El Gerente o Gerenta del Área solicitará a través de e-mail dirigido al Gerente o Gerenta de Administración y Finanzas la eliminación de la cuenta de usuario, identificando al usuario con nombre completo.
3. El Encargado o Encargada de Informática con la información del e-mail eliminara el perfil de usuario y su cuenta de correo asociada en el caso de existir.
4. El Encargado o Encargada de Informática registrara en una bitácora la fecha de la eliminación, motivos y datos de la cuenta.
5. El Encargado o Encargada de Informática informara a la Gerencia solicitante y a la Gerencia de administración y finanzas la confirmación de la eliminación de la cuenta de usuario.

Tipo de Documento	Procedimiento		
Nombre	PRO006 – Eliminación de usuarios en el Sistema FIN700 de Puertos de Talcahuano	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL003 - Política de Acceso a la Red de Datos		
Objetivos	Eliminar usuarios del Sistema FIN700 de Puertos de Talcahuano.		

1. Los responsables de solicitar la eliminación de usuarios del sistema FIN 700 son los Gerentes o Gerentas de área correspondiente.
2. El Gerente o Gerenta del Área solicitará a través de e-mail dirigido al Gerente o Gerenta de Administración y Finanzas la eliminación de la cuenta de usuario, identificando al usuario con nombre completo.
3. El Encargado o Encargada de Informática con la información del e-mail eliminara el perfil de usuario y su cuenta de correo asociada en el caso de existir.
4. El Encargado o Encargada de Informática registrara en una bitácora la fecha de la eliminación, motivos y datos de la cuenta.
5. El Encargado o Encargada de Informática informara a la Gerencia solicitante y a la Gerencia de administración y finanzas la confirmación de la eliminación de la cuenta de usuario.

Tipo de Documento	Procedimiento		
Nombre	PRO007 – Respaldo de Bases de Datos	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL004 - Política de Respaldos Institucionales		
Objetivos	Realizar correctamente un respaldo de la Base de Datos Institucional de Puertos de Talcahuano.		

1. Las bases de datos a respaldar son Estadisvti, estadisthno (Sistema estadístico), y cualquier otro que la Empresa determine con una periocidad trimestral.
2. La periodicidad del respaldo de las bases de datos de los sistemas internos se debe definir en la documentación del programa.
3. La nomenclatura para identificar cada base de datos respaldada es: xxxxx_db_ddmmaahhmm.BAK, donde x representan los caracteres del nombre de la base de datos, d el día, m el mes , a el año, h la hora y m los minutos.
4. Respaldar Backup de bases de datos en DATACENTER externo según periocidad definida por el sistema.
5. El respaldo del sistema ERP de la empresa lo realiza por contrato la empresa SONDA de forma diaria.

Tipo de Documento	Procedimiento		
Nombre	PRO008 – Respaldo de Datos de Usuarios	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL004 - Política de Respaldos Institucionales		
Objetivos	Realizar correctamente un respaldo a los Datos de Usuarios de Puertos de Talcahuano.		

1. Una vez al semestre se deberá realizar un simulacro de perdida de información por desastre natural u otro tipo de perdida, solicitando la restauración de los servicios y datos al proveedor del Datacenter con el fin de corroborar que el servicio de respaldo de información y servicio de réplica de servidores funcione de forma adecuada.

Tipo de Documento	Procedimiento		
Nombre	PRO009 – Respaldo de Software y Sistemas Operativos	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL004 - Política de Respaldos Institucionales		
Objetivos	Realizar correctamente un respaldo a los Software y Sistemas Operativos utilizados en Puertos de Talcahuano.		

1. Hacer copia completa de cada software y almacenarlos en el servidor de archivo o cuenta OneDrive. En la carpeta se deben almacenar las seriales e instaladores del programa.
2. El acceso a la carpeta de software está restringido y solo podrán acceder los integrantes del comité de seguridad de la información.

Tipo de Documento	Procedimiento		
Nombre	PRO010 – Almacén de respaldos realizados	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL004 - Política de Respaldos Institucionales		
Objetivos	Almacenar, resguardar y asegurar la disponibilidad eficiente de los distintos respaldos que se realizan en Puertos de Talcahuano.		

1. A contar desde 17 de Julio de 2011 los datos respaldados se hacen a través de un DATACENTER, quien posee las instalaciones adecuadas para brindar el resguardo necesario con respecto a posibles daños por pérdida producto de la acción del agua, tiempo, fuego. La información debe ser replicada en el servidor que cumple la función de réplica en el Datacenter vía internet o enlace MPLS.
2. Los Cd originales que contienen las aplicaciones y S.O se guardan en la oficina del Encargado o Encargada de informática.

Tipo de Documento	Procedimiento		
Nombre	PRO011 – Recuperación de un respaldo de la Base de Datos	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL004 - Política de Respaldos Institucionales		
Objetivos	Recuperar correctamente un respaldo realizado a la Base de Datos Institucional		

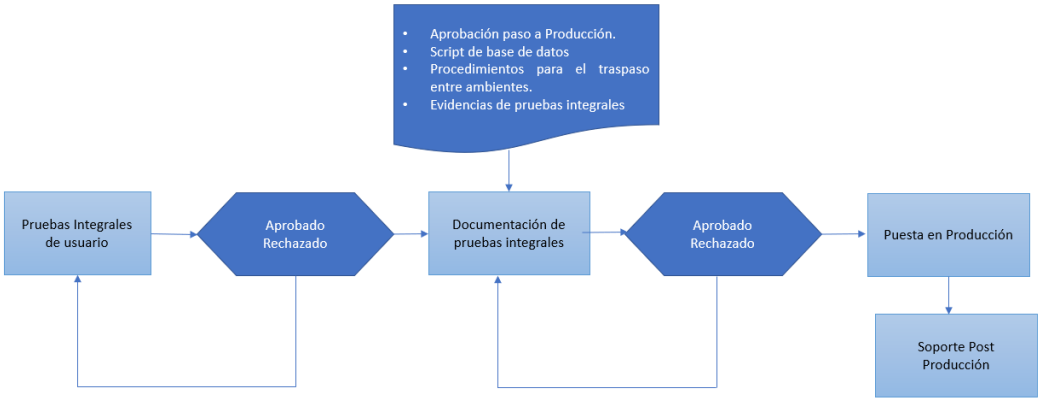
1. Por correo electrónico, enviado al Encargado o Encargada de Informática, el usuario o usuaria de la base de datos solicita recuperar base de datos, especificando el nombre sistema a recuperar y fecha de la base de datos a recuperar (ejemplo: sistema prodfact del 03/08/2018).
2. Verificar si existe espacio suficiente en el servidor de aplicaciones para recuperar el backup de la base de datos.
3. Recuperar archivo correspondiente al respaldo solicitado.
4. Respaldar la base de datos actual con SQL.
5. Restaurar la base de datos con SQL.
6. Informar por correo al usuario o usuaria solicitante que el servicio solicitado está disponible.

Tipo de Documento	Procedimiento		
Nombre	PRO012 – Recuperación de un respaldo de Datos de Usuarios	Versión 6	Diciembre 2023
Política(s) Asociada(s)	POL004 - Política de Respaldos Institucionales		
Objetivos	Recuperar correctamente un respaldo realizado a los Datos de un Usuario		

1. Por correo, enviado al Encargado o Encargada de Informática, el usuario o usuaria solicita la recuperación de archivo o carpeta especificando su nombre y la fecha, a recuperar.
2. El Encargado o Encargada de informática. solicitará a la empresa que presta los servicios de Datacenter la recuperación de la carpeta a través de correo electrónico.
3. El proveedor dispondrá la carpeta en un espacio temporal en el servidor de archivos.
4. Se Restaurará la carpeta recuperada.
5. Informar por correo al usuario o usuaria solicitante que el servicio solicitado está disponible.

Tipo de Documento	Procedimiento		
Nombre	PRO013 – Cambios o actualizaciones de software	Versión 6	Diciembre 2021
Política(s) Asociada(s)	POL010 – Política de control de cambios a sistemas		
Objetivos	Control los cambios asociados a software.		

1. Por correo, enviado al Encargado o Encargada de Informática y Gerente de administración o finanzas, el usuario o usuaria solicita el cambio o actualización de software adjuntando el anexo 5 adjunto en este documento.
2. El Gerente o Gerenta de administración y finanzas y el Encargado o encargada de informática evaluaran el impacto y costos de los cambios solicitados, aprobando o rechazando lo solicitado por el usuario.
3. El Encargado o Encargada de informática. solicitará a la empresa que presta los servicios de desarrollo de software el cambio o utilizara recursos internos para llevar a cabo la tarea.
4. La empresa Portuaria Talcahuano San Vicente cuenta para la operación de sistemas de 2 ambientes de servidores para la correcta ejecución del desarrollo del sistema, pruebas integrales, corrección de errores y puestas en producción.
5. Se deben considerar los siguientes ambientes:
    a. Ambiente QAS: Ambiente para pruebas del sistema.
    b. Ambiente PRD: Ambiente de operación del sistema.
6. Las pruebas de sistema se deben efectuar en ambiente de QAS y una vez que se disponga de los vistos buenos de pruebas, la aplicación debe ser trasportada a la Plataforma PRD.
7. Para una correcta gestión en el transporte de códigos fuentes entre el ambiente de pruebas (QAS) y operación del sistema (PRD) se debe cumplir el siguiente flujo de trabajo:



ANEXOS.

Anexo N°1: Formulario creación – Modificación – eliminación de cuentas de usuario.

Datos del Usuario	Dato			
Nombre completo (2 nombres y 2 apellidos)				
Indique la acción solicitada C: Creación, M: Modificación, E: Eliminación				
En el caso de Modificación de la cuenta de usuario indique la modificación.				
En el caso de Eliminación de la cuenta de usuario indique el motivo.				
RUT (Caso de usuarios en Chile) y ID (Caso de usuarios extranjeros)				
Cargo del nuevo usuario				
Unidad				
Jefe directo				
Usuarios Interno o Externos (indicar la Empresa contratista o EST pertenece)				
RUT o NIF de Empresa Contratista o EST				
Fecha límite de validez del usuario				
Teléfono de contacto del nuevo usuario				
Indicar si requiere correo electrónico Corporativo	Si		No	
Indique si requiere acceso a Internet	Si		No	

SOLICITUD EQUIPAMIENTO

Solicitud de arriendo de equipamiento.

Equipo	Marque con una X la preferencia
Desktop	
Notebook Standard	
Notebook Ultraliviano	

Nota:

1. Toda solicitud para acceder a un equipo nuevo de computación ya sea Portables (Laptop) o de Escritorio deben ser aprobada por el Gerente o Gerenta de administración y finanzas. Dicha aprobación debe ser adjuntada a este formulario, objeto iniciar la gestión de arriendo.

2. El plazo de entrega del equipo es de 7 a 14 días, desde el momento que se cuenta con la aprobación correspondiente.

Anexo N°2: Avance plan de seguridad 2023.

II.1.- Medidas aplicadas a desastres naturales

Medida	Descripción	Fecha	Responsable	Observaciones
Revisión de la ubicación de los equipos en alturas para disminuir daños en caso de inundaciones	Al tener oficinas en un primer piso, se ubican los Pc y monitores en lugares que no llegue el agua, como también prever las inundaciones producto de falla baños y o lugar donde exista instalaciones sanitarias	Octubre 2023	Encargado de Informática	Cumplido
Revisar uso de UPS en cada equipo.	Verificar que cada usuario este utilizando UPS en su computador.	Octubre 2023	Encargado de informática.	Cumplido

II.2.- Medidas aplicadas a problemas estructurales

Medida	Descripción	Fecha	Responsable	Observaciones
Tener a la vista certificación de la instalación eléctrica.	Se debe mantener visible el certificado de instalación eléctrica de la empresa.	Marzo 2023	Encargado de informática.	Cumplido

II.3.- Medidas aplicadas a problemas de Hardware

Medida	Descripción	Fecha	Responsable	Observaciones
Revisar funcionamiento de réplica de los servidores.	Al disponer de los servidores replicados permitirá que al producirse una falla en algunos de ellos, se reemplaza. Se evalúa tener el servicio de hosting para el servidor de dominio y servidor de archivo	Octubre 2023	Encargado de informática.	Cumplido

Revisión del proceso de respaldo de los softwares de aplicación y datos en servidores externos	Evaluación de la forma de trabajo de los respaldo y su funcionamiento de los DATACENTER externo, que cuente con todas las medidas y planes de contingencia que permita contener nuestros datos y software de aplicación	Octubre 2023	Encargado de informática.	Cumplido

II.4.- Medidas aplicadas a problemas de Software

Medida	Descripción	Fecha	Responsable	Observaciones
Actualizar los softwares	Se debe preparar un catastro actualizado de los software disponible en la empresa con licencia a fin de de determinar cuales están sujetos a actualización debido a requerimiento de la empresa y cuales son de actualizaciones standard del mercado	Junio 2023	Encargado de informática.	Se cuenta con un catastro de software licenciado por la empresa
Evaluar funcionamiento antivirus centralizados	Con el objeto de estandarizar y sincronizar un antivirus para la red de datos, y correos y acceso a internet se debe buscar un antivirus de calidad y que sea actualizado en línea (via internet)	Marzo 2023	Encargado de informática.	El funcionamiento se revisa de manera diaria ejecutando análisis en busca de malware y vulnerabilidades.

II.5.- Medidas aplicadas a problemas de Red

Medida	Descripción	Fecha	Responsable	Observaciones
Revisión de la red de datos	Trabajar con servidores, estaciones de	Diciembre 2023	Encargado de informática.	Cumplido

	trabajos, swich, router y firewall			

II.6.- Medidas aplicadas a problemas de los Respaldos de Seguridad

Medida	Descripción	Fecha	Responsable	Observaciones
Revisión del proceso de respaldo de datos de nuestros servidores en Datacenter externo	Se establece realizar verificaciones de respaldos de servidor de archivos.	Octubre 2023	Encargado de informática.	Revisado
Revisión procedimiento para que cada usuario respalde los datos de su estación de trabajo (Pc)	Definir ciertas reglas claras y medible para que cada usuario sea responsable de sus datos de su Pc y que la empresa provee los medio para que este haga sus respaldos una vez a la semana	Octubre 2023	Encargado de informática.	Revisado

II.7.- Medidas aplicadas a problemas con la Información

Medida	Descripción	Fecha	Responsable	Observaciones
Comunicar los medios de respaldos con los que cuenta la empresa.	Se debe comunicar al personal todos los medios de respaldo de información con los que cuenta la empresa para evitar pérdidas de datos	Octubre 2023	Encargado de Informática	Cumplido

II.8.- Medidas aplicadas a problemas con el Personal

Medida	Descripción	Fecha	Responsable	Observaciones
Al implementar las medidas anteriores permiten solucionar los problemas identificados en este apartado	Revisión e informe medidas puntos anteriores.	Diciembre 2023	Encargado de informática.	

II.9.- Medidas aplicadas a problemas con Patrimonio

Medida	Descripción	Fecha	Responsable	Observaciones
Crear inventario de los elementos de la configuración computacional de la empresa	Crear y mantener actualizado un inventario de todos los elementos de la configuración computacional de la empresa y un plano de red de datos asociado de usuario y red de datos	Septiembre 2023	Encargado de informática.	Cumplido.

II.10.- Medidas aplicadas a problemas provocados por otros riesgos

Medida	Descripción	Fecha	Responsable	Observaciones
Al implementar las medidas anteriores permite solucionar los problemas identificados en este apartado	Revisar y emitir informe medidas puntos anteriores. El tema apunta a riesgos derivados del terrorismo o cualquier otro de baja probabilidad de ocurrencia	Diciembre 2023	Encargado de informática.	Cumplido
Charla de concientización de seguridad de la información (ciberseguridad)	Realizar charlas de ciberseguridad para generar conciencia del uso de aplicaciones o visita a sitios maliciosos que pueden causar algún daño a la información de la empresa	Octubre 2023	Encargado Informática	Cumplido
Actividades de Hacking ético (ciberseguridad)	Realizar ataques de hacking ético sobre la infraestructura de la empresa.	Diciembre 2023	Encargado Informática	Por Ejecutar

Anexo N°3: Plan de seguridad 2024.

II.1.- Medidas aplicadas a desastres naturales

Medida	Descripción	Fecha	Responsable	Observaciones
Revisión de la ubicación de los equipos en alturas para disminuir daños en caso de inundaciones	Al tener oficinas en un primer piso, se ubican los Pc y monitores en lugares que no llegue el agua, como también prever las inundaciones producto de falla baños y o lugar donde exista instalaciones sanitarias	Marzo 2024	Encargado de Informática	
Revisar uso de UPS en cada equipo.	Verificar que cada usuario este utilizando UPS en su computador.	Octubre 2024	Encargado de informática.	

II.2.- Medidas aplicadas a problemas estructurales

Medida	Descripción	Fecha	Responsable	Observaciones
Tener a la vista certificación de la instalación eléctrica.	Se debe mantener visible el certificado de instalación eléctrica de la empresa.	Marzo 2024	Encargado de informática.	

II.3.- Medidas aplicadas a problemas de Hardware

Medida	Descripción	Fecha	Responsable	Observaciones
Revisar funcionamiento de réplica de los servidores.	Al disponer de los servidores replicados permitirá que al producirse una falla en algunos de ellos, se reemplaza. Se evalúa tener el servicio de hosting para el servidor de dominio y servidor de archivo	Abril 2024	Encargado de informática.	

Revisión del proceso de respaldo de los softwares de aplicación y datos en servidores externos	Evaluación de la forma de trabajo de los respaldo y su funcionamiento de los DATACENTER externo, que cuente con todas las medidas y planes de contingencia que permita contener nuestros datos y software de aplicación	Octubre 2024	Encargado de informática.	

II.4.- Medidas aplicadas a problemas de Software

Medida	Descripción	Fecha	Responsable	Observaciones
Actualizar los softwares	Se debe preparar un catastro actualizado de los software disponible en la empresa con licencia a fin de de determinar cuales están sujetos a actualización debido a requerimiento de la empresa y cuales son de actualizaciones standard del mercado	Junio 2024	Encargado de informática.	
Evaluar funcionamiento antivirus centralizados	Con el objeto de estandarizar y sincronizar un antivirus para la red de datos, y correos y acceso a internet se debe buscar un antivirus de calidad y que sea actualizado en línea (via internet)	Abril 2024	Encargado de informática.	.

II.5.- Medidas aplicadas a problemas de Red

Medida	Descripción	Fecha	Responsable	Observaciones
Revisión de la red de datos	Trabajar con servidores, estaciones de	Diciembre 2024	Encargado de informática.	

	trabajos, swich, router y firewall			

II.6.- Medidas aplicadas a problemas de los Respaldos de Seguridad

Medida	Descripción	Fecha	Responsable	Observaciones
Revisión del proceso de respaldo de datos de nuestros servidores en Datacenter externo	Se establece realizar verificaciones de respaldos de servidor de archivos.	Octubre 2024	Encargado de informática.	
Revisión procedimiento para que cada usuario respalde los datos de su estación de trabajo (Pc)	Definir ciertas reglas claras y medible para que cada usuario sea responsable de sus datos de su Pc y que la empresa provee los medio para que este haga sus respaldos una vez a la semana	Octubre 2024	Encargado de informática.	

II.7.- Medidas aplicadas a problemas con la Información

Medida	Descripción	Fecha	Responsable	Observaciones
Comunicar los medios de respaldos con los que cuenta la empresa.	Se debe comunicar al personal todos los medios de respaldo de información con los que cuenta la empresa para evitar pérdidas de datos	Octubre 2024	Encargado de Informática	

II.8.- Medidas aplicadas a problemas con el Personal

Medida	Descripción	Fecha	Responsable	Observaciones
Al implementar las medidas anteriores permiten solucionar los problemas identificados en este apartado	Revisión e informe medidas puntos anteriores.	Diciembre 2024	Encargado de informática.	

II.9.- Medidas aplicadas a problemas con Patrimonio

Medida	Descripción	Fecha	Responsable	Observaciones
Crear inventario de los elementos de la configuración computacional de la empresa	Crear y mantener actualizado un inventario de todos los elementos de la configuración computacional de la empresa y un plano de red de datos asociado de usuario y red de datos	Septiembre 2024	Encargado de informática.	.

II.10.- Medidas aplicadas a problemas provocados por otros riesgos

Medida	Descripción	Fecha	Responsable	Observaciones
Al implementar las medidas anteriores permite solucionar los problemas identificados en este apartado	Revisar y emitir informe medidas puntos anteriores. El tema apunta a riesgos derivados del terrorismo o cualquier otro de baja probabilidad de ocurrencia	Diciembre 2024	Encargado de informática.	
Charla de concientización de seguridad de la información (ciberseguridad)	Realizar charlas de ciberseguridad para generar conciencia del uso de aplicaciones o visita a sitios maliciosos que pueden causar algún daño a la información de la empresa	Octubre 2024	Encargado Informática	
Actividades de Hacking ético (ciberseguridad)	Realizar ataques de hacking ético sobre la infraestructura de la empresa.	Diciembre 2024	Encargado Informática	

Anexo N°4: Matriz de perfiles por cargo sistema FIN700.

Sistema	Cargo	Roles
FIN 700	Encargado de Informática	ROLADMUSU Administrador de usuarios
	Encargada de Personal y Recursos Humanos	ADMREM Administrador de remuneraciones
	Contador General	ADMVEN Adm Ventas y Dte
		ADM ADMINISTRADOR
		ACTIVOFIJO Administrador Activo Fijo
		ADMCONFIG Administrador de configuraciones
		ADMCONTAB Administrador de contabilidad
		ADMINFORMES Administrador de informes
		ADMPRE Administrador de presupuestos
		ADMREM Administrador de remuneraciones
		ROLADMUSU Administrador de usuarios
		ADMWORKFLOW Administrador WORKFLOW
		CONF ASOC EMPR Configuracion Asociar Empresa
		CON-GEC-SOC-PER Configuracion General
		FUNCIONAL (ALU) Funcional
		INFORMES CONTAB Informes contabilidad
		INFORM.RPTGEST Informes reportes generales
		PROCMAS-APROBAR Proceso masivo de aprobacion
		PROCMAS-CONTABIL Proceso masivo contabilidad
		PROCMASLPROCLARG Proceso masivo
		TES1 TESORERIA PRINCIPAL
		USCONTABILIDAD Uusario contabilidad
	Analista Contable	ACTIVO FIJO Administrador Activo Fijo
		ADMREM Administrador de remuneraciones
		CAJERO cajero
		CONFAFI Configuracion y parametros Activos
		CONSULTAS-PROVD Consultas Proveedores
		FUNCIONAL (ALU) Funcional
		IMFORMESAFI Informes Activo Fijo
		INFORMES PROVEED Informes Proveedores
		VENTASOPERADOR Operador de ventas y finanzas
		PROVEEDORES Proveedor
		TES1 TESORERIA PRINCIPAL
		TRANS CON CONCBA Transaccion Caontabilidad
		TRANS LCO ADM Transacción libro de compras
		TRANS LCO OPE Transacción libro de compras

		TRANS LVE ADM Transacción libro de ventas
		TRANS PER OPE Transacción personal operaciones
		TRANS PROV OPE Transacción proveedores
		TRANS TES OPE Transacción Tesoreria Operaciones
		TRANSAFI Transacciones activo Fijo
		USUARIODLC Usuario lirbo de compras

Anexo N°5: Plan de contingencia en caso de no acceso al sitio web.

La Empresa Portuaria Talcahuano San Vicente, cuenta con un sitio web cuya dirección (URL) es http://www.puertotalcahuano.cl, con el objetivo de dar a conocer a los clientes, usuarios y público en general las actividades de la Empresa, así como la información que legalmente debe ser de dominio público.

A fin de disminuir la probabilidad de que dicho sitio web no esté disponible a través de internet en un momento determinado, el área de informática permanentemente deberá verificar su adecuado funcionamiento, y además será responsable del desarrollo y de incorporar las actualizaciones que entregan las gerencias en cuanto a sus contenidos, y por ende debe verificar el cumplimiento del plan de contingencia.

En caso de existir problemas para acceder al sitio web de la empresa (el cual se detecta a través de los monitoreos que hace el encargado o encargada de informática o por la recepción de queja por parte del usuario o usuaria ya sea en forma verbal o por medio de correo), será el encargado o encargada de informática quien deberá buscar solución en el menor plazo posible, de acuerdo con las siguientes opciones de acción, dependiendo de la situación que se produzca:

1.- El sitio de internet no está disponible:

- Falla externa: Debe verificar con proveedor actual de hosting web si el servicio se encuentra operativo y el correcto funcionamiento del acceso a internet.
- Falla de energía eléctrica en el edificio, dar aviso al encargado del edificio para que llegue pronto la restauración.
- Falla en los dispositivos de comunicación: Debe verificar el correcto funcionamiento de los switch, router y firewall ubicados en la oficina de informática.
- Falla interna: Debe verificar el correcto funcionamiento de la red de información y el correcto acceso a internet.

2.- Daños al contenido del sitio web vía internet (hackear la página, es decir que extraños coloquen contenidos que no corresponden):

- Verificar con proveedor de hosting Web el correcto funcionamiento del firewall y solicitar informe de posibles vías de acceso no autorizados (puerto de entrada) y reprogramar el firewall para eliminar esas vías violentadas.
- Levantar respaldo del contenido del sitio web con proveedor del desarrollo del sitio Web.

En caso de ocurrencia de cualquier anomalía descrita y que requiera el uso del plan de contingencia, el Encargado o Encargada de informática deberá informar por escrito (vía e-mail) al Gerente o Gerenta de Administración y Finanzas, describiendo la situación indicando el origen del problema y sus posibles causas, debiendo proponer las soluciones del caso, en el menor tiempo posible; se deberán arbitrar las medidas necesarias, que permitan la no recurrencia del o los hecho(s).

Anexo N°6: Procedimiento de monitoreo y registro de visitas en sala de servidores.

Este procedimiento establece la forma en que se registraran los ingresos a la sala de servidores y la forma de chequear de forma física con una frecuencia diaria la operación de los instrumentos y condiciones que el espacio físico debe cumplir.

Procedimiento de registro de ingreso a la sala de servidores.

De los ingresos:

- Se debe disponer de un libro que permita el registro de los ingresos a la sala de servidores.
- Para el ingreso de personal no autorizado se debe enviar un correo electrónico al Gerente o Gerenta de Administración y finanzas solicitando la autorización del ingreso a la sala. Previa autorización se notificará al Encargado o Encargada de informática.
- Cada ingreso debe ser registrado en el libro de ingresos.
- Los registros deben indicar:
  - Fecha
  - Personas que ingresaron a la sala
  - Motivo del ingreso

Procedimiento de chequeo físico de la sala de servidores.

Del chequeo de la sala de servidores

- El chequeo de la sala de servidores se debe realizar cada lunes al inicio de la jornada laboral.
- El encargado de realizar el chequeo es el Encargado de Informática.
- Se dispondrá de un listado de ítems, los cuales la sala de servidores debe cumplir. El no cumplimiento debe ser registrado en las observaciones y se debe dar aviso a la Gerencia de Administración y finanzas.

La lista de chequeo es la siguiente:

Checklistt Fisico sala de servidores		
Fecha:		
Hora:		
Responsable: Gonzalo Gacitúa		
Esta bitácora esta con valores por defecto. De encontrar alguna anomalía o no cumplimiento se debe ingresar como observación y ser informada a la respectiva Gerencia		
Elemento evaluado	**SI**	**No**
El área de servidores contiene solamente el equipo relacionado directamente con informática y sus sistemas de ayudas ambientales		
Tiene el área de servidores un sistema de control del ambiente apropiado		
Se mantiene el área de servidores con una temperatura adecuada		
Tiene el área de servidores una salida de emergencia identificada y despejada		
Se ha prohibido a los personas el consumo de alimentos y bebidas en el interior del área de servidores para evitar daños al equipo		
Está el área de servidores protegido de la luz solar directa		
Los servidores estan alejados de las ventanas.		
La sala de servidores cuenta con la iluminación necesaria		
Se encuentran los interruptores de iluminación en un sitio adecuado		
Está el área de servidores situado sobre el nivel del mar		
Existe una bitácora de las visitas e ingresos al área de servidores		
Existe una o varias UPS's que soporten la carga eléctrica del área de servidores		
Está el cableado de datos debidamente canalizado e identificado		
Cuentan las puertas de área de servidores con cerraduras de seguridad adecuadas		
Los equipos Switch, UPS y servidores se encuentran en funcionamiento.		
Observaciones:		

Anexo N°7: Formulario solicitud de cambios de sistemas

Nombre del Proyecto		*Objetivo del documento:* *Registrar antecedentes para gestionar la aprobación de cambios a la Línea Base (Alcance, Costos, Plazos).* *Pasos de la solicitud:* *1. Evalúe impacto de los cambios.* *2. Aprobados los cambios por parte del Comité de proyecto, realice actualización de los documentos de proyecto, formalice y Comunique a los interesados.*
Responsable del Plan		
Solicitante		
Fecha solicitud		

1. DESCRIPCIÓN DEL CAMBIO

Tipo de cambio *(Inclusión, exclusión o modificación)*	**Descripción** *(Nombre de la iniciativa/Etapa y descripción del cambio)*	**Justificación** *(porqué es necesario realizar el cambio)*	**Impacto** *(Sistemas, procesos y plazos impactados)*

2. ANEXOS

Nombre Documento	**Descripción** *(del documento)*

REGISTRO DE APROBACIONES

Revisión Jefe de proyectos TI → *(Gonzalo Gacitúa Vásquez)*	**V°B° Gerente de Administración y Finanzas →** *(Arturo Morello)*	**V°B° Sponsor Negocio** *(Nombre del Sponsor)*
Aceptada	**Aceptada**	**Aceptada**
Fecha	**Fecha**	**Fecha**
Observación	**Observación**	**Observación**
Firma Jefe de proyectos TI	**Firma Gerente de administración y finanzas**	**Firma Sponsor**