POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Declaración de Confidencialidad

Este documento contiene información que es confidencial y propiedad exclusiva de la Municipalidad Provincial de Coronel Portillo. Dicha información no podrá ser divulgada fuera del entorno de la entidad, transmitida, duplicada o utilizada, total o parcialmente, para cualquier otro propósito que no sea el previsto, a menos que cuente con permiso expreso por escrito de la Municipalidad Provincial de Coronel Portillo.

Historial de Cambios

Fecha	Versión	Descripción	Autor
31/10/2014	1.00	Elaboración de Versión inicial	Ing. Teófilo Pastor Pérez Lazo
31/12/2015	1.00	Versión Revisada y Aprobada	

Índice

1. Objetivo

Establecer el marco General de Seguridad de la Información que permita lograr los niveles de seguridad que la Municipalidad Provincial de Coronel Portillo, en adelante MPCP, requiere en base a las necesidades de la entidad y a los riesgos presentes en sus procesos.

La Política General de Seguridad de la Información (PGSI) y los documentos asociados tienen los siguientes objetivos:

- Cumplir con las buenas prácticas de seguridad sobre la información (utilización, divulgación, administración y custodia), necesarias para el normal desarrollo de las actividades de la entidad.
- Minimizar la posibilidad de ocurrencia de hechos contingentes que pudieran interrumpir la operación del negocio y reducir el impacto de los daños a las instalaciones, medios de almacenamiento, equipos de procesamiento y de comunicación.
- Proteger la información, sus medios de procesamiento, conservación y transmisión, del uso no autorizado o revelaciones accidentales, errores, fraudes, sabotaje, violación de la privacidad y otras acciones que pudieran perjudicarla o ponerla en riesgo.
- Cumplir las normas legales y reglamentarias, estipuladas por la ley y los organismos reguladores correspondientes, referidas a seguridad de la información y medios que la contienen.

2. Conceptos Generales

La información utilizada por la MPCP, sea ésta de carácter público o propio de la entidad, debe ser considerada como uno de sus activos más importantes. Esta información puede existir en muchas formas, puede estar impresa o escrita en papel, almacenada electrónicamente, ser transmitida manualmente o por medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiera la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada, ya que la información lleva riesgos operativos intrínsecos los cuales no sólo están asociados a los sistemas y tecnologías de la información.

La seguridad de la información que permite mantener las características de disponibilidad, integridad y confidencialidad, es esencial para cumplir nuestra función encomendada, cumplir con las normas legales y proteger la imagen de la MPCP. Nuestra información y los sistemas que lo soportan pueden ser el objetivo de diversas amenazas como fraudes, sabotaje, espionaje industrial, vandalismo, ataques de hackers y/o de virus informáticos; amenazas en continua expansión que hacen que nuestra información y sistemas informáticos estén expuestos a riesgos cada vez mayores.

La seguridad de la información busca fundamentalmente, alcanzar los siguientes objetivos:

Confidencialidad: La información sólo debe ser conocida por el personal que la requiera para el desarrollo de sus funciones. Este principio fundamental de seguridad busca garantizar que toda la información de los ciudadanos, colaboradores y proveedores, y sus medios de procesamiento y/o conservación, estén protegidos del uso no autorizado o divulgación accidental, sabotaje, espionaje industrial, violación de la privacidad y otras acciones que pudieran poner en riesgo dicha información.

Integridad: La información no puede ser alterada ni eliminada por cambios no autorizados o accidentales. Este principio fundamental de seguridad busca garantizar la precisión, suficiencia y validez de la información, métodos de procesamiento y todas las transacciones de acuerdo con los valores y expectativas del negocio, así como evitar fraudes y/o irregularidades de cualquier índole que haga que la información no corresponda a la realidad.

Disponibilidad: La información debe estar disponible para el personal, usuarios y entidades reguladoras de manera oportuna y acorde a sus niveles de autorización. Este principio fundamental de seguridad busca garantizar que los usuarios autorizados tengan acceso a la información cuando ésta es requerida por el proceso del negocio. Para ello se debe procurar que la información y la capacidad de procesamiento sean resguardados y puedan ser recuperados en forma rápida y completa ante cualquier hecho contingente que interrumpa la operatividad o dañe las instalaciones, medios de almacenamiento y/o equipamiento de procesamiento.

En el Anexo A – Conceptos Básicos, se presentan las definiciones de los términos referidos en este documento, con el objeto de poder unificar el entendimiento de los mismos por el personal de la MPCP.

Encargado General de Seguridad de Información

Es la persona que se encargará de velar por la actualización de la Política General de Seguridad de la Información y el cumplimiento de las acciones de: mitigación de riesgos relacionados a la seguridad lógica, seguridad física y procedimientos de respaldo; verificación del normal funcionamiento, después de una remediación; y revisión de la presente política una vez al año o cuando se realice alguna modificación significativa a la infraestructura, a los servicios y al soporte de Tecnologías de Información de la MPCP.

Encargado de Seguridad en las Unidades Orgánicas de la MPCP

Es la persona que se encargará de canalizar y sensibilizar los riesgos tecnológicos en cada una de las áreas a las cuales pertenecen; de coordinar permanentemente con el EGSI las actividades o procesos de seguridad; de detectar e informar oportunamente

cualquier situación o evento que pueda originar alguna pérdida a la MPCP; y, de proponer, en caso lo considere necesario, controles y procedimientos que permitan mejorar los niveles de seguridad existentes en sus respectivas áreas.

Usuario de la Información

Es todo colaborador de la MPCP que tiene acceso a la información a la que está autorizado a consultar y procesar. Las autorizaciones otorgadas limitarán su capacidad en los entornos informáticos de forma tal que no pueda realizar actividades diferentes a las autorizadas. Es la persona que se encargará de informar en forma inmediata, al Encargado de Seguridad del área correspondiente, de cualquier situación o evento que pueda constituir un incidente de seguridad.

3. Alcance

Este documento establece la PGSI para el personal de la MPCP, que deberá ser de su conocimiento y cumplimiento obligatorio.

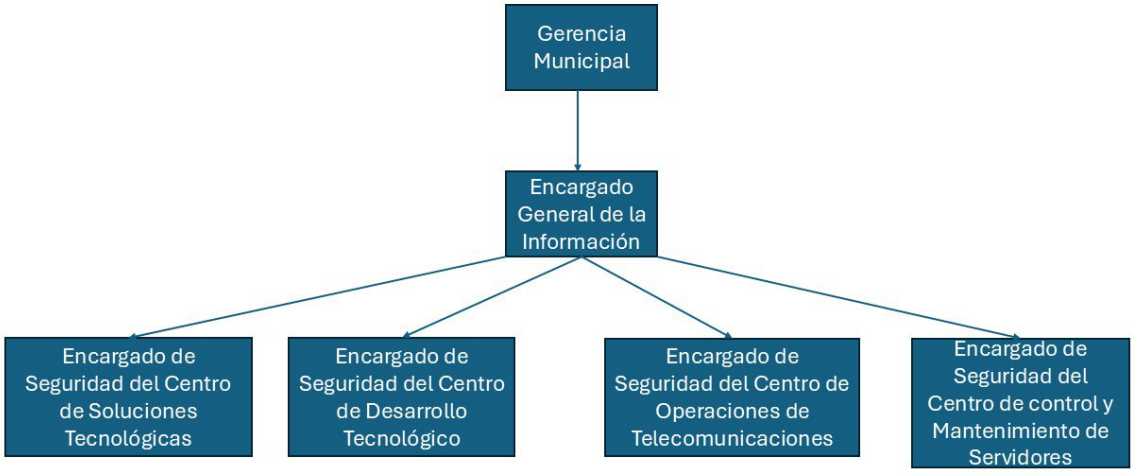
Este documento cubre los siguientes temas:

- Política de Seguridad.
- Organización para la administración de Seguridad de Información.
- Clasificación de activos de Información.
- Seguridad del personal.
- Seguridad física y ambiental.
- Administración de las operaciones y comunicaciones.
- Control de acceso.
- Cumplimiento.

4. Organización para la administración de la Seguridad de la Información

La MPCP deberá contar con una estructura que soporte los aspectos de seguridad de información al interior de la organización, la cual considera principalmente los roles y responsabilidades para garantizar una adecuada administración.

Como parte de la estructura de la Oficina de Seguridad de Información, se ha definido la siguiente organización:



4.1. Encargado General de Seguridad de la Información

Es la persona que tendrá como principales responsabilidades:

- Hacer de nexo con el Comité de Seguridad de Información.
- Coordinar activamente con los Encargados de Seguridad de las principales áreas de la MPCP para definir controles y procedimientos que mitiguen los posibles riesgos existentes y que puedan afectar los procesos críticos de la institución.
- Monitorear y revisar la adecuada implementación de los controles y procedimientos de seguridad definidos como parte de la ejecución de los procesos críticos de la empresa.
- Asegurar, a través de la Gerencia Municipal, que los aspectos de seguridad, sean considerados dentro del planeamiento estratégico de la MPCP.
- Apoyar en la definición, implementación, validación y mantenimiento del Plan de Seguridad de la Información, previa evaluación de los riesgos asociados, verificando que éste considere aspectos tales como activos de información que deben ser protegidos, alcance y descripción de los objetivos a tener en cuenta.
- Verificar el cumplimiento y efectividad de las medidas de administración de riesgos relacionados a: Seguridad Lógica, Seguridad Física, Seguridad del Recursos Humanos, Administración de Operaciones, Clasificación de Seguridad y Procedimientos de Respaldo.
- Verificar que se mantengan las características de seguridad de la información definidas por el Comité de Seguridad de la Información, cuando los procesos críticos sean objeto de una subcontratación. Así como, verificar que el proveedor del servicio sea capaz de aislar el procesamiento y la información objeto de la subcontratación, en todo momento y bajo cualquier circunstancia.
- Verificar que en el inventario periódico que realiza la institución, los activos asociados a la Tecnología de Información sean clasificados según el nivel de seguridad requerido por dichos activos.
- Verificar que los cargos existentes en la organización tengan asociados perfiles de acceso acordes al principio “necesidad-de-conocer” (“need-to-know”), es decir, el usuario sólo debe tener acceso a la información y recursos que necesita para completar o desarrollar las tareas que están asociadas al rol que el usuario tiene dentro de la MPCP.
- Verificar el cumplimiento y efectividad de los procedimientos de control y actualización de versiones y para la MPCP a producción.
- Verificar que el proceso para la aprobación de propuestas de desarrollo y/o adquisición de sistemas cuente con una descripción general de los riesgos identificados, requerimientos de seguridad y las acciones a tomar para controlar dichos riesgos.
- Garantizar la correcta implementación del Plan de Seguridad de Información, definido para la MPCP.

4.2. Encargados de Seguridad en las áreas de la MPCP

Es la persona designada que tendrá como principales responsabilidades:

- Canalizar y sensibilizar los riesgos tecnológicos de cada una de las áreas a las cuales pertenecen.
- Implementar las políticas y medidas aprobadas como resultado de la administración de riesgos inherentes a las funciones encomendadas.
- Evaluar permanentemente en coordinación con el Encargado General de Seguridad, las actividades o procesos que se realicen para detectar e informar oportunamente cualquier situación o evento que pueda originar alguna pérdida a la MPCP.
- Participar del Comité de Seguridad de Información, proponiendo controles y procedimientos que permitan mejorar los niveles de seguridad existentes en sus respectivas Unidades Orgánicas.

4.3. Propietario de la Información

Es el Coordinador o encargado de la Unidad Organizacional, o apoyo correspondiente, responsable de la protección y uso de la información. El propietario de la información define la clasificación de la misma y es responsable del mantenimiento y actualización de dicha clasificación. Dicha responsabilidad no puede ser delegada a terceros, sólo se podrá delegar la protección o custodia de la información en un colaborador, que apoyará en las tareas operativas de administración y control de seguridad correspondientes a la información.

4.4. Usuario de la Información

Es el conjunto de personas internas y/o externas que, con la debida autorización del propietario de la información, puede consultar, ingresar, modificar o borrar la información almacenada en los sistemas informáticos u otros medios de almacenamiento. Los usuarios sólo deben tener acceso a la información a la que están autorizados a consultar y procesar. Las autorizaciones que se otorguen limitarán su capacidad en los entornos informáticos de forma que no puedan realizar actividades diferentes a las autorizadas. Las principales responsabilidades de los usuarios de la información son las siguientes:

- Utilizar la información sólo para el propósito para el que recibió autorización de uso.
- Cumplir con los controles establecidos en las normativas impuestas por la MPCP.
- Tomar las medidas adecuadas para evitar que la información se divulgue o use sin autorización.

5. Marco Normativo de Seguridad

5.1. Marco Normativo de Seguridad de la Información

La documentación del Marco Normativo de Seguridad de la Información de la MPCP contempla los siguientes documentos:

- PGSI (el presente documento).
- Políticas de Seguridad.

5.2. Elaboración y Aprobación

Las normas y procedimientos a ser desarrollados en lo sucesivo, serán propuestos por las diferentes áreas, elaborados en conjunto con los Encargados de Seguridad de las áreas y el Encargado General de Seguridad de Información. Dichas normas serán aprobadas por la Gerencia Municipal.

6. Clasificación y manejo de activos de información

6.1.1. Aspectos Generales

Los niveles de clasificación de los activos de información, permiten definir e implementar mecanismos de seguridad y protección acordes a su nivel de clasificación, los cuales reflejan el nivel de sensibilidad, valor y criticidad del activo de información, para la MPCP.

El propietario de la información en cada área, debe identificar aquella que se encuentra bajo su control, clasificarla y efectuar una revisión periódica de dicha clasificación. En caso de ser una información recibida de terceros, será responsabilidad de quien recepcione la misma, clasificarla y rotularla en forma adecuada.

6.1.2. Nivel y Clasificación de la Información

- **Información pública:** Toda aquella información que es de libre acceso y difusión no genera ningún riesgo.

- **Información interna:** Toda aquella información de uso interno de la MPCP y cuyo acceso puede ser permitido a cualquier colaborador de la MPCP.

- **Información confidencial:** Toda aquella información cuya divulgación o conocimiento puede presentar riesgos para la MPCP, y que sólo debe ser utilizada por el propietario de la información y las personas que expresa y directamente hayan sido autorizadas por él.

6.2. Seguridad del Personal

Todo colaborador de la MPCP debe conocer sus responsabilidades respecto a la seguridad de la información.

Aquellos colaboradores que deban efectuar tareas críticas para la organización, definidas por cada área, deben pasar por un proceso de selección riguroso en el que se le indique claramente las responsabilidades que están asociadas a su función dentro de la organización.

Un requisito fundamental para obtener niveles apropiados de seguridad de información en la MPCP es la contribución de todos los colaboradores.

El incumplimiento de las políticas de seguridad de la información conducirá a acciones disciplinarias establecidas en el Reglamento Interno del Trabajo de la MPCP.

Cuando un colaborador haga uso de su período vacacional, él o los usuarios de acceso a los distintos sistemas que utiliza, deberán ser temporalmente deshabilitados para evitar que personal no autorizado intente utilizar dichas cuentas para efectuar alguna acción no autorizada.

Cuando un colaborador culmine su relación laboral con la MPCP se deberá tener en cuenta que:

- El órgano de Gestión del Capital Humano, deberá notificar al Área de Infraestructura, Servicios y Soporte de Tecnologías de Información para que ésta cancele todas las cuentas y accesos a los sistemas de información que tenía asignado el colaborador, esto debe ser efectuado en el momento de haberse producido el cese de dicho colaborador.
- El órgano de Gestión del Capital Humano recibirá del colaborador todos los elementos que la organización le suministró para su labor.

El conocimiento de las actividades de cualquier área de la MPCP es importante para la entidad, deben estar en el dominio de dos o más personas, de forma que se puedan cubrir situaciones inesperadas sin interrumpir el servicio. El velar por esta política es responsabilidad del Coordinador o Supervisor directo del área que efectúa procesos críticos para la organización.

Los encargados de la seguridad de las diferentes áreas de la MPCP están en la obligación de reportar los diferentes incidentes de seguridad de información, tales como fallos en seguridad, amenazas, debilidades de los sistemas o mal funcionamiento, de acuerdo a los procedimientos establecidos.

Todos los colaboradores internos o temporales deben cumplir con los requerimientos de control y seguridad de información especificados en estas

políticas y deberán firmar un documento de conocimiento y aceptación del PGSI de la MPCP, el que se detalla en el Anexo B – Compromiso de Aceptación y cumplimiento de Políticas de Seguridad de Información.

La Gestión del Capital Humano, debe realizar verificaciones en el proceso de selección de personal orientadas a validar la información presentada por el candidato.

6.3. Seguridad Física y Ambiental

6.3.1. Áreas críticas

Definimos como áreas críticas, a los lugares protegidos bajo un perímetro de seguridad con adecuados controles de entrada. Estas áreas deben de estar físicamente protegidas contra accesos no autorizados, daños e interferencias.

Los lugares donde se albergan los activos en los cuales se procesa y almacena la información crítica de la entidad es considerada un área crítica que debe contar con los controles antes mencionados.

La infraestructura eléctrica y el cableado en general deberán estar controlados y convenientemente ordenados a fin de prevenir cortocircuitos y fallos en los equipos. Así mismo, en el área de comunicaciones, los circuitos y redes informáticas deberán estar identificados y rotulados.

El acceso a las áreas críticas sólo estará permitido al personal autorizado y a los contratistas que realizan mantenimiento a las instalaciones de éstas, los que deberán estar permanentemente supervisados por personal de del área de Centro de control y Mantenimiento de Servidores de la MPCP.

6.3.2. Seguridad de los Equipos Informáticos

Todos los equipos informáticos de la MPCP deberán estar tanto física como lógicamente protegidos.

Se deben de establecer contraseñas de acceso a las estaciones de trabajo (PC) o portátiles y protectores de pantalla por periodos de inactividad. En el caso de las portátiles, se deberá implementar los mecanismos de seguridad que correspondan al nivel de criticidad de la información, que se maneja en éstas.

6.4. Administración de las operaciones y comunicaciones

6.4.1. Controles preventivos: detección de virus, correo no deseado (spam) y otros ataques

Todas las estaciones de trabajo de LA MPCP y demás que se conecten a las redes internas de la MPCP y deben cumplir con el uso del software antivirus aprobado en la organización.

En caso de ocurrir una infección por virus, existencia de software malicioso u otro tipo de ataque sobre una estación de trabajo, el Usuario de Información deberá manejarlo como un incidente de seguridad de información, reportándolo a través del Encargado de Seguridad del Área a la que pertenece, para que sea derivado a través del Sistema de Incidencias a fin de proceder a gestionar la solución el incidente.

Los usuarios no deben usar ningún software que no haya sido aprobado; el software especializado deberá ser probado, para evitar la infección por virus o ataques de cualquier tipo. Sólo se podrá manejar como excepción el software que haya sido probado y aprobado por los responsables en dichas áreas.

Toda estación de trabajo debe bloquearse cuando el usuario deje la misma desatendida. Para volver a utilizar la estación se deberán ingresar las credenciales correspondientes.

6.4.2. Seguridad sobre las redes

Toda conexión externa a la red de la MPCP deberá ser autorizada por el Área de Centro de control y Mantenimiento de Centro de Soluciones Tecnológicas, y estar acorde a la norma administrativa interna de conexiones externas, así mismo toda la información que se transmita deberá contar con el nivel de seguridad requerido.

Las comunicaciones se pueden realizar por líneas propias como por redes públicas. Si bien ambos procedimientos pueden ser utilizados, el nivel de seguridad de las redes públicas es inferior, por lo tanto, en ese caso se deberá utilizar procedimientos de seguridad adicionales.

Con el fin de garantizar un funcionamiento y mantenimiento adecuados, el responsable del mantenimiento de las redes, deberá documentar y mantener actualizado el esquema de la red de la MPCP. Dicha documentación deberá estar a disposición del personal autorizado, cada vez que éste la requiera.

6.4.3. Copias de respaldo

La disponibilidad de los sistemas operativos, aplicaciones en producción y la información de los usuarios (datos) son la parte medular de la seguridad de información, por lo que es necesario asegurar que se contará con la disponibilidad de dicha información mediante un adecuado procedimiento de respaldo en base a copias de seguridad periódicas, locales y externas, de software base de datos (motor de base de datos, archivos críticos en disco y cinta).

Las copias de respaldo realizadas deberán almacenarse adicionalmente en una ubicación diferente a los sistemas respaldados, que cuente con fácil acceso y niveles de seguridad adecuados, evitando su pérdida en caso de siniestro de gran magnitud y asegurando el acceso adecuado en caso de contingencia.

Todo registro físico o lógico considerado importante debe ser resguardado en un lugar adecuado fuera de la organización.

6.4.4. Seguridad en el correo electrónico

El correo electrónico se pone a disposición de los colaboradores de la MPCP para el desarrollo exclusivo de sus funciones laborales, el servicio de correo puede ser proporcionado tanto a nivel interno como externo según el rol que cumpla cada colaborador en la organización.

Se debe tener en cuenta que en la mayoría de los casos, el almacenamiento de los mensajes se realiza en las estaciones de trabajo de los usuarios, por lo cual estarían disponibles a cualquier persona que logre acceder a dicha estación. Por lo tanto, se deberán tomar las medidas adecuadas para proteger el acceso a sus estaciones de trabajo.

Todo correo electrónico contiene información confidencial y para los casos donde no cumple esta categoría deberá tener en el Asunto la palabra NO CONFIDENCIAL, a modo de rotulación.

Sólo el personal debidamente autorizado tendrá la potestad de enviar mensajes de correos en representación de la MPCP hacia ámbitos fuera del mismo.

6.4.5. Seguridad en Internet

El acceso a Internet se provee como una herramienta para el desarrollo exclusivo de la actividad laboral de los colaboradores de la MPCP. El

acceso deberá ser aprobado el responsable de la unidad organizacional respectiva.

El acceso a Internet, por parte de los usuarios internos, requerirá que éstos estén debidamente identificados y autenticados en los sistemas administradores de red.

Todas las conexiones a Internet deberán estar controladas mediante la instalación de mecanismos de control de acceso a la red de la MPCP y servidores que soportan los servicios de Internet que entrega la empresa. Los programas que se usen para estos servicios deberán de ser aprobados y ser permanentemente actualizados, evaluados e instalados los parches de seguridad que se generen por parte de los fabricantes, en caso que la evaluación defina que se deben instalar.

6.5. Control de Acceso

La autorización de acceso a la información por parte de los usuarios, debe ser realizada de acuerdo con sus atribuciones, funciones y/o tareas a desarrollar. Estas deben ser asignadas por el responsable de la unidad organizacional correspondiente. Será responsabilidad del superior directo definir el perfil de acceso de sus subordinados.

El acceso realizado por el personal de backup, deberá ser efectuado utilizando su cuenta personal, es decir, no se deberá utilizar la cuenta de la persona a quien reemplaza.

Queda estrictamente prohibido el acceso a la información confidencial o restringida por vías no autorizadas, esto incluye la utilización de software no definido en el perfil del usuario, o cualquier tipo de utilitario no provisto por la MPCP para esa función.

El acceso a los recursos de información de la MPCP es a través de usuarios y contraseñas. El personal encargado del Centro de control y Mantenimiento de Servidores, es responsable de la creación, administración y eliminación de los usuarios. Cada copia de información confidencial en papel o en algún medio magnético deberá ser autorizada por el propietario de esa información.

El acceso a las aplicaciones deberá estar adecuadamente restringido sólo para usuarios con autorización, así mismo las aplicaciones deben contar con una adecuada estructura de perfiles de usuario que restrinja los accesos de acuerdo a las funciones y responsabilidades de los colaboradores de la MPCP.

La asignación de contraseñas es realizada de manera personal y confidencial,

siendo el usuario final responsable del uso de las credenciales y las consecuencias que pueda tener su uso inadecuado.

Se deberá evitar, bajo cualquier circunstancia, la escritura de dichas contraseñas en papeles, notas recordatorias o archivos compartidos, asumiendo el usuario la responsabilidad, en caso personal no autorizado tenga acceso a estas credenciales por los motivos descritos anteriormente.

El uso de las contraseñas de acceso es personal, confidencial e intransferible. Bajo ninguna circunstancia las credenciales de accesos deben compartirse entre los colaboradores de la MPCP.

6.5.1. Monitoreo y uso de los sistemas de acceso

En la medida que el software del sistema lo permita, los sistemas de comunicaciones y servidores que contengan información sensible, valiosa o crítica de la MPCP deberán contar con un registro de eventos de seguridad de la información relevante, para detectar como mínimo lo siguiente:

- Intentos de adivinar contraseñas.
- Intentos de usar privilegios no autorizados.
- Cambios a privilegios de usuarios.
- Modificaciones a software de sistemas.

6.5.2. Control del cumplimiento de la PGSI

Dado que la MPCP pone a disposición de los colaboradores internos o externos los recursos de información con el objeto de que éstos desarrollen su trabajo y funciones asignadas y que estas facilidades sean sólo entregadas para el propósito del negocio, se considera que los colaboradores no almacenen ni manejen información personal dentro de estos recursos.

Para controlar estas actividades se asignan las siguientes responsabilidades.

Los Coordinadores o Supervisores de las áreas organizacionales, o quien éstos deleguen se reservan el derecho de examinar todos los archivos guardados o transmitidos en sus sistemas, correo electrónico, directorios de archivos personales, disco duro, y cualquier otra información mantenida o transmitida en los sistemas de la MPCP.

La MPCP se reserva el derecho de supervisar, acceder, recuperar, leer y/o descubrir comunicaciones del colaborador cuando:

- Exista una verdadera necesidad que no pueda ser satisfecha a través de otros medios.
- El funcionario involucrado no está disponible y el tiempo sea crítico para la realización de una actividad.
- Exista una causa razonable para sospechar de una actividad delictiva o violación a las políticas de seguridad.
- Sea requerida por alguna ley o regulación, para una supervisión.

6.6. Cumplimiento

6.6.1. Cumplimiento con los requerimientos legales

La MPCP operará siempre dentro del marco legal al que se encuentra sometido, manteniendo siempre como premisa, asegurar el cumplimiento de los objetivos de la organización, actuar de acuerdo con las políticas generales de la MPCP y mantener siempre un comportamiento profesional y de compromiso con la calidad.

La información almacenada en los archivos informáticos de la MPCP es básica para el funcionamiento del negocio y estará adaptada a lo que las leyes en vigor dictaminan. Nunca podrá ser usada sin autorización previa, ni con fines distintos a los requeridos por el trabajo encomendado en cada momento.

Tanto el software adquirido por la MPCP, como los programas desarrollados en forma interna están sujetos a la normativa sobre propiedad intelectual.

6.6.2. Acuerdo de confidencialidad

Toda vez que se confíe información crítica a un tercero, debe procurarse contar con un acuerdo por escrito de confidencialidad, no divulgación y uso apropiado de la información entregada por la MPCP. Este acuerdo debe incluir instrucciones precisas para el manejo de los datos y la eliminación o borrado de los mismos cumplido el periodo circunstancial que llevo a confiar en el tercero.

En el caso que se requiera que la MPCP firme un acuerdo de confidencialidad con terceros, como el que se detalla en el Anexo C – "Acuerdo de Confidencialidad", éste sólo podrá ser firmado por el Gerente Municipal o quien él designe en su defecto.

6.6.3. Legalidad y seguridad de software

El Área OTI centralizará la administración y supervisión de las licencias de software de las estaciones de trabajo de los usuarios de la MPCP. Asimismo, el Área EUS debe efectuar inventarios periódicos del software instalado en los equipos del personal de la MPCP. En aquellos casos en que se detecten anomalías o licencias sin regularizar, se informará al Encargado de Seguridad del área correspondiente y al Encargado General de Seguridad, quienes coordinarán con el área de Recursos Humanos la aplicación de medidas correctivas según reglamento interno de la MPCP.

La instalación de software en los ambientes de procesamiento y/o estación de trabajo, sólo puede ser llevada a cabo por personal autorizado o por los mecanismos automáticos destinados a dicho fin.

6.6.4. Derechos de propiedad intelectual

Se debe asegurar que el software de la MPCP (adquirido o desarrollado internamente) cumpla con la normativa legal vigente, correspondiente a decreto legislativo 822, Ley de Derecho de Autor.

Los productos de software desarrollados o modificados por personal de la MPCP, son de propiedad exclusiva de la MPCP.

El software desarrollado por personal de la MPCP, deberá inscribirse a nombre de la MPCP en el registro de propiedad intelectual respectivo, con el objeto de acogerse a los resguardos que estipula la ley de propiedad intelectual.

No se podrá prestar ni copiar software adquirido o desarrollado por la MPCP a no ser que exista una autorización a nivel de la Gerencia Municipal.

Es recomendable que todo el software y la documentación que posea la MPCP incluyan avisos de los derechos de autor y propiedad.

La MPCP tiene propiedad legal sobre el contenido de todos los archivos almacenados en los equipos de cómputo y sistemas en red, así como de todos los mensajes que viajan a través de su Infraestructura, Servicios y Soporte de Tecnologías de Información. La MPCP se reserva el derecho de permitir el acceso a esta información a terceras personas.

Los usuarios finales no deberán copiar software proporcionado por la MPCP en ningún medio de almacenamiento magnético o divulgar software sin la autorización escrita correspondiente.

6.6.5. Faltas a la política

La seguridad de la información en todos sus ámbitos, debe ser considerada como un ítem dentro de la evaluación de desempeño del personal.

El incumplimiento de las obligaciones y prohibiciones mencionadas en este documento y otros documentos complementarios, facultan a la MPCP a aplicar medidas disciplinarias de acuerdo al Reglamento Interno de Trabajo de la MPCP.

6.6.6. Responsabilidades

Una adecuada implementación del PGSI en la MPCP sólo podrá lograrse con la cooperación y ayuda de todos los colaboradores, por lo tanto, es necesario que todo el personal lo conozca y se comprometa con los requerimientos de seguridad de información identificados, dado que éstos son responsables del cumplimiento de esta Política.

Será responsabilidad del trabajador que detecte un incumplimiento de las obligaciones o prohibiciones indicadas en este documento, dar a conocer en forma inmediata al Encargado de Seguridad de su Área, todos los eventos de seguridad; quien gestionará la investigación del hecho y reportará al Encargado General de Seguridad de Información el resultado de dicha investigación. En caso de comprobarse una conducta no apropiada, el Encargado General de Seguridad de Información dará aviso a la Gerencia de Recursos Humano para que tome las acciones pertinentes.

Es responsabilidad de la Gerencia Municipal de la MCPC asegurar que el personal reciba una adecuada capacitación relacionada a seguridad de información y se comprometa a cumplir con dichos procedimientos. Los encargados de cada una de las Unidades Organizacionales son responsables de asegurar que sus colaboradores o el personal externo que trabaja en su área, conozcan y cumplan dichas políticas.

La MPCP podrá supervisar violaciones a las políticas mediante controles en base a los cuales se podrán tomar las medidas disciplinarias del caso.

7. Anexos

Se presentan a continuación los documentos anexos a la Política General de Seguridad de Información:

- Anexo A – Conceptos Básicos
- Anexo B – Compromiso de aceptación y cumplimiento de Políticas de Seguridad de la Información
- Anexo C – Acuerdo de Confidencialidad.

7.1. Anexo A – Conceptos Básicos

Activo de Información, es todo recurso de información, software, hardware o servicio que contenga y/o manipule información de la MPCP. Ejemplos de activos asociados a sistemas de información son los siguientes:

- Recursos de información: bala MPCP de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, disposiciones relativas a sistemas de emergencia para la reposición de información perdida ("fallback"), información archivada.
- Recursos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios.
- Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles), equipos de comunicaciones (routers, PBXs, contestadores), medios magnéticos (cintas y discos), otros equipos técnicos (suministro de electricidad, unidades de aire acondicionado), mobiliario, lugares de emplazamiento.
- Servicios: servicios informáticos, de comunicaciones y control ambiental.

El Marco Normativo de Seguridad de la Información, es un conjunto de documentos formales, que se aplican de manera funcional y genérica a cualquier tarea o actividad y que ayudan a la gerencia en la dirección y guía de los colaboradores en la terminación efectiva de sus deberes.
Bajo esta definición el marco normativo de la MPCP, es un conjunto de políticas, y guías de procedimientos usados para comunicar sus estrategias al resto de la organización.

Las Políticas, son las reglas a las que se deben ajustar las tareas y actividades relacionadas con la protección de la información; estas son independientes del ambiente de procesamiento.

Los Procedimientos, son documentos que permiten darle dinamismo y eficiencia a los procesos, regulando las disposiciones internas emanadas por la Gerencia Municipal de la Entidad en el ámbito administrativo y permitiendo establecer pautas orientadas a un ordenamiento y control de la gestión interna.

Recursos de Hardware, equipamiento tecnológico constituido por equipos portátiles, equipos de escritorio, dispositivos de almacenamiento, equipos de comunicación, servidores de aplicación, servidores de protección, etc.

Software, conjunto de programas o aplicaciones desarrollados o adquiridos.

Usuarios, son las personas tanto internas como externas a la MPCP, que hacen uso de los recursos informáticos y de la información de la MPCP con el objeto de poder cumplir con sus correspondientes funciones.

7.2. Anexo B – Compromiso de aceptación y Cumplimiento de Políticas de Seguridad de la Información

COMPROMISO DE ACEPTACIÓN Y CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Este documento deberá ser entregado al colaborador con otros documentos que debe firmar al momento de ser contratado

Como Trabajador, en carácter de colaborador(a) de la MPCP, con fecha _____ declaro conocer y aceptar en todo su contenido el documento denominado, "Política General de Seguridad de la Información".

En dicho documento se indican conductas no aceptadas al interior de la MPCP y responsabilidades que asumo como colaborador de la Empresa.

A continuación, se enumeran aquellas conductas no aceptadas y responsabilidades consideradas más importantes, sin que, por esto, éstas deban ser consideradas como las únicas exigidas por la MPCP:

Responsabilidades

Me comprometo a conocer y cumplir con la Política General de Seguridad de la Información y toda otra Política o Procedimiento que la MPCP considere necesario implantar para cumplir con los requisitos legales y/o salvaguardar la integridad, disponibilidad y confidencialidad de la información.

Asumo la responsabilidad sobre los sistemas y recursos puestos a mi disposición por la MPCP para el desarrollo de las funciones que se me encomendó. Me responsabilizo por la seguridad de los mismos.

Me responsabilizo por la notificación al Encargado de Seguridad y a mis Coordinadores o Supervisores inmediatos, en caso de verificar el mal uso de los recursos por parte de algún otro colaborador interno o externo a la MPCP.

Me comprometo a utilizar sólo aquel software que esté autorizado por el área competente y que me haya sido asignado para el desarrollo de las funciones encomendadas

Asumo la responsabilidad en el uso y manipulación de la información sobre la que tengo autorización, la que me comprometo a efectuar y proteger en base a los niveles de clasificación que tenga dicha información.

Me comprometo a no acceder, copiar ni transferir información para la cual no tengo la autorización adecuada.

Conductas no aceptadas

Todas aquellas indicadas en la Ley como figuras penales relativas a Informática, algunos ejemplos de éstas:

- Distribución maliciosa o inutilización de sistemas de información, sus partes o componentes, obstaculización o modificación de su funcionamiento o modificación no autorizada de los datos contenidos en el sistema.
- Acceso o intromisión en sistemas para apoderarse, usar o conocer indebidamente la información contenida en él.
- Daño, alteración o destrucción maliciosa de los datos contenidos en un sistema de información.
- Revelación o difusión maliciosa de datos contenidos en un sistema.

Conductas contrarias a la Ley, en base a lo establecido en el Decreto Legislativo 822, Ley de Derecho de Autor, acerca de la legislación de derechos de autor y propiedad intelectual, que regula la adquisición y el uso de software, o cualquier otra ley promulgada al respecto.

Copiar o distribuir software, datos, códigos y manuales sin la expresa autorización del titular de los derechos de autor.

Usar copias no autorizadas de Software (sin la debida licencia). Esto incluye la ejecución simultánea de software en dos o más computadores salvo que conste debidamente autorizado en la licencia de uso.

Fabricar, adquirir o utilizar cualquier elemento que sirva para remover o burlar, aspectos de seguridad del software legalmente adquirido.

Disposición Final

El no cumplimiento de este compromiso formal, será considerado por la MPCP como una falta grave que atenta tanto contra la legalidad vigente como contra las normas internas, y lo facultará para adoptar las medidas administrativas que estime pertinente.

Pucallpa, _____de_____ de 20__

Nombre: _____

Fecha: _____

Área: _____

Firma: _____

7.3. Anexo C – Acuerdo de Confidencialidad

ACUERDO DE CONFIDENCIALIDAD

Este Acuerdo de Confidencialidad, efectivo el día _____, es firmado entre la Municipalidad Provincial de Coronel Portillo, en adelante la MPCP, y _____, en adelante EL TERCERO, bajo los siguientes términos:

Por cuanto EL TERCERO ha recibido la solicitud para realizar los servicios de _____, para la MPCP; y en conexión con la provisión de tales Servicios, la MPCP puede proporcionar a EL TERCERO cierta información clasificada como CONFIDENCIAL, ambas partes acuerdan lo siguiente:

Toda Información clasificada como Confidencial deberá ser etiquetada con la palabra "CONFIDENCIAL", de forma escrita por la MPCP antes de ser proporcionada a EL TERCERO para propósito de este documento, siendo EL TERCERO responsable de no revelar dicha información a ningún tercero, sujeto a los términos y condiciones establecidos en este documento.

Queda entendido que la información entregada por la MPCP hacia EL TERCERO será usada en la respectiva evaluación de las áreas de su interés. Asimismo, se deja constancia que la entrega de la referida información no le da ningún derecho sobre dichas áreas.

La información, materia del presente acuerdo, tiene carácter confidencial; en consecuencia, no podrá ser suministrada o transferida a otros entes, sean éstos personas naturales o jurídicas, bajo ninguna circunstancia.

EL TERCERO está de acuerdo que la información clasificada como confidencial entregada por la MPCP debe ser utilizada solamente en conexión con la provisión de estos Servicios.

EL TERCERO debe llevar a cabo sus obligaciones bajo este acuerdo usando las mismas normas de seguridad que utiliza para proteger su propia información, o por lo menos un razonable grado de seguridad.

Las obligaciones establecidas en este documento, continuará en toda su extensión y efectos por un período de 5 años desde la fecha efectiva de este acuerdo, o un período no menor a 3 años en caso que así lo acuerden las partes.

Este acuerdo se rige por las leyes de la República de Perú.

Encontrándose las partes conformes con la ejecución de este acuerdo, los representantes autorizados de las partes firman este documento en duplicado en señal de conformidad, en la ciudad de Pucallpa, el _____de _____ de 20___.

LA MPCP	EL TERCERO
Por:	Por:
_____	_____
Título	Título
_____	_____