MUNICIPALIDAD DE CURRIDABAT
MANUAL DE PROCEDIMIENTOS Y DIRERCTRIZ PARA USO DE INTERNET Y CORREO ELECTRÓNICO

Por acuerdo Nro. 14 de las 20:34 horas del 27 de marzo de 2014, según consta en el artículo 2°, capítulo 6°, del acta de la sesión ordinaria Nro. 204-2014, el Concejo de Curridabat, en uso de su potestad normativa, dispuso la aprobación del siguiente:

Manual de procedimientos para el marco de seguridad informática MC-SOP-011, versión 1.2 así como el documento MC-PSIN-0004: Directriz para el uso del servicio de correo electrónico y acceso a Internet.

MC-SOP-011: Procedimiento Marco de Seguridad Informática

1 Introducción

1.1 Objetivo

Actualmente la seguridad informática ha tomado especial relevancia, dadas las cambiantes condiciones y nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes para explorar más allá de las fronteras nacionales, situación que ha llevado la aparición de nuevas amenazas en las tecnologías de información.

Esto ha provocado que muchas organizaciones gubernamentales y no gubernamentales, alrededor del mundo, hayan desarrollado documentos y directrices que orientan a sus usuarios en el uso adecuado de herramientas tecnológicas y recomendaciones para obtener el mayor provecho de estas y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas en los bienes y servicios que prestan las instituciones.

Las políticas institucionales de seguridad informática, surgen como un lineamiento organizacional para concientizar a cada uno de sus miembros sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la entidad.

Las políticas institucionales de seguridad informática de la Municipalidad de Curridabat están basadas en lo establecido en la "Normas ISO/IEC 17799:2000, ISO 27001:2005 y 27002:2005 las cuales son un Código de Buenas Prácticas para la Gestión de la Seguridad de la Información, dichas normas ofrecen recomendaciones en la gestión de la seguridad de la información, y define la Seguridad de la Información como la preservación de la confidencialidad, integridad y disponibilidad. A continuación se definen dichos conceptos:

- **Confidencialidad:** aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso.

- **Integridad:** garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.

- **Disponibilidad:** aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

  Este documento contiene una serie de políticas que deberán ser acatadas por los funcionarios de la Municipalidad de Curridabat, usuarios de las tecnologías de Información, dichas políticas se verán apoyadas en un conjunto de normas que brindan mayor detalle de como cumplir lo estipulado en las políticas, y están contenidas en el documento "Normas Institucionales de

Seguridad Informática", estas hacen referencia a normativa legal y diferentes guías. Por último los procedimientos y manuales, deberán estar alineados con las políticas y normas.

1.2 Objetivos Específicos de los procedimientos de seguridad informática.

- Promover el uso de las mejores prácticas de seguridad informática en el trabajo, para que los usuarios colaboren con la protección de la información y recursos institucionales.

- Proponer los mecanismos de seguridad lógica, en el ambiente informático de modo que se contribuya con la confidencialidad, integridad y disponibilidad de la información.

- Servir de guía para el comportamiento profesional y personal de los funcionarios de la institución, en procura de minimizar los incidentes de seguridad internos, como hurto de información o vandalismo.

- Promover las mejores prácticas de seguridad física, mediante la implementación de ambientes adecuados que permitan la correcta custodia de los datos y equipos administrados por los diferentes Centros de Gestión, utilización eficiente de los recursos de tecnologías de información.

- Regular el cumplimiento de aspectos legales y técnicos en materia de seguridad informática.

- Homologar la forma de trabajo de personas de diferentes unidades y situaciones que tengan responsabilidades y tareas similares.

1.3 Revisión

El documento Directrices sobre seguridad y utilización de las tecnologías de información y comunicaciones debe ser revisado al menos dos veces al año, considerando dentro de esto lo siguiente:

- Una correcta aplicabilidad de las directrices que están operando: Se refiere al hecho de determinar si las directrices que se hayan establecido son aplicables para la Institución, o si deben ser modificadas o eliminadas.

- Incorporación de nuevas directrices de acuerdo a requerimientos en seguridad que puedan surgir producto de cambios en el ambiente o de nuevas tecnologías o servicios incorporados dentro de la Contraloría.

- Requerimientos específicos de la Administración Superior.

1.4 **Beneficios de los Procedimientos de Seguridad Informática**

Las políticas de seguridad, constituyen la base a partir de la cual la Institución diseña su sistema de seguridad, para garantizar que la inversión que se realice sea la adecuada, que los productos y soluciones adquiridos cumplan con los objetivos de la institución y que éstos sean configurados correctamente. Por lo tanto, los beneficios derivados de la buena gestión de políticas de seguridad informática son:

- Existencia de procedimientos de seguridad informática regulados, uniformes y coherentes en toda la organización.

- Fomentan la cultura organizacional en materia de seguridad informática.

- Minimizar la pérdida de la información y recursos a través de la seguridad informática, mediante su aplicación.

- Proporcionan la confianza necesaria a clientes y usuarios, demostrando que la seguridad es un factor que es importante dentro de la municipalidad y que la misma se aborda correctamente.

1.5 Alcance

Las políticas aquí documentados deben ser de implementación obligatoria para todos aquellos funcionarios de la Municipalidad de Curridabat que estén involucrados directa o indirectamente con el uso de tecnologías de información y comunicaciones.

Cabe responsabilidad administrativa e incluso civil o penal para aquel funcionario que incumpla las políticas de Seguridad Informática establecidas en este documento, de conformidad con el régimen jurídico vigente.

1.6 Definiciones, Acrónimos, y Abreviaciones

1.7 Referencias

- La norma de referencia ISO 27001.

- Las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE).

- Políticas y normas de Seguridad de Informática V_octubre 2007, V1.0 Ministerio de Hacienda

- Marco de Seguridad en tecnologías de información, **Contraloría General de la República**, informe 1.0 Julio 2009 **"NORMAS TÉCNICAS DE INFORMACION Y COMUNICACIÓN "**

1.8 Autoridades y Responsabilidades

Comisión de Informática

- Brindar Asesoría para en el cumplimiento del Marco de Seguridad establecido.

Direcciones y Jefaturas de la Municipalidad de Curridabat

- Seguir y respetar los procedimientos mínimos establecidos en el presente documento, para regular el uso de las tecnologías de información en la institución.

2. Procedimiento de Concientización seguridad informática.

Concientizar a todos los funcionarios de la Institución, sobre su obligación de conocer y aplicar la normativa en materia de seguridad informática para lograr un cambio favorable en la cultura organizacional.

La institución junto con el departamento de informática, deberán establecer diferentes formas de concientización mediante boletines, charlas, afiches. Podrá visitarse diferentes sedes previa coordinación con Informática, para impartir charlas o capacitaciones. Se dará prioridad a la concientización de los administradores de tecnologías de información, para que estos a su vez transfieran el conocimiento a sus respectivos usuarios.

Se deberán implementar mecanismos para velar por el cumplimiento de las políticas y normas institucionales, por parte de todos los usuarios de las tecnologías de información.

Los directores y jefes de la Institución, deberán proveer los mecanismos a los funcionarios para familiarizarse con las políticas, normas y procedimientos de seguridad, así como velar porque el personal a su cargo reciba las actividades de capacitación, implementación y evaluación, necesarias para permitirles proteger adecuadamente los recursos tecnológicos de la Institución y cumplir con las disposiciones vigentes en materia de Seguridad Informática.

3. Procedimiento Control de Acceso a los Recursos Institucionales

Se debe asegurar la integridad, confidencialidad y disponibilidad de los datos, información y los recursos asociados a ésta, razón por la cual el control de acceso a la información y los recursos, ya sea de la infraestructura técnica o de las aplicaciones, debe establecerse con el principio de la "necesidad de conocer lo funcional, el cual pretende que cada funcionario únicamente tenga acceso a la información y recursos estrictamente necesarios para el desarrollo adecuado de su función.

Se establecen las siguientes Políticas que regulan el acceso a los diferentes recursos institucionales.

4. Procedimiento Uso Correcto de las contraseñas por parte de los usuarios de la red y aplicaciones.

El uso de contraseñas es el pilar fundamental para el acceso a la información y recursos institucionales, razón por la cual su uso correcto son de vital importancia en la seguridad de la información institucional. Situación que implica cumplir con las directrices básicas de seguridad que serán de acatamiento obligatorio por parte de todos los usuarios de la red y aplicaciones, el objetivo fundamental se centra en obtener contraseñas más "robustas" y sean fáciles de recordar por parte de los usuarios de la institución.

Todo funcionario de la red institucional y de aplicaciones, que posea una o varias cuentas creadas a su nombre, deberá cumplir con las siguientes normas, que constituyen las mejores prácticas para la manipulación de las contraseñas personales y lo protegerán del hurto y modificación de la información institucional que administra.

1. Queda estrictamente prohibido a los funcionarios de la Institución utilizar sus cuentas de usuario para obtener cualquier clase de beneficio propio y/o para terceros.

2. La contraseña no deberá compartirse, sin excepción con ninguna otra persona (aunque se trate de la jefatura, un soportista, o compañeros de trabajo), ya que el dueño de la cuenta será el responsable por el uso que se le dé a la misma.

3. El usuario no debe dejar contraseñas escritas en medios o lugares donde puedan ser accesados por terceros (por ejemplo, en una carpeta del escritorio, en la pantalla del equipo, debajo del teclado u otros).

4. El usuario estará enterado que después de ejecutar tres intentos fallidos de "blogueo" en su cuenta de red y o de aplicaciones, la misma será bloqueada, esto para proteger sus datos e identidad, en caso de olvidar definitivamente la contraseña, deberá solicitar la activación de la misma ante su respectivo administrador, autorizado por el jefe o director del departamento, siguiendo el procedimiento establecido por la institución para tales efectos.

5. Todo usuario deberá hacer el cambio periódico de sus contraseñas cada (tres) 3 meses como mínimo.

6. Las contraseñas generadas por los usuarios para su uso en los servicios de red y aplicaciones, deben contener caracteres de al menos (tres) 3 de las siguientes (cuatro) 4 clases:

Clase	Descripción de la Clase
Letras mayúsculas	A,B,C,D…..Z
Letras minúsculas	a,b,c,d…….z
Números	0,1,2,3…9
Caracteres especiales	Por ejemplo: símbolo puntuación ú otros como %,&,@,[],%

7. Todo usuario deberá tomar en cuenta las siguientes restricciones, que han sido configuradas para que las contraseñas sean más seguras:

    - La longitud de toda contraseña a utilizar deberá ser igual o mayor a ocho caracteres.
    - La contraseña a adoptar no podrá ser igual o similar a su respectivo nombre de usuario.
    - No podrá repetir ninguna de las últimas tres contraseñas utilizadas.
    - No se podrá dejar contraseñas en blanco.

Recomendaciones:

1. Adicionalmente se le recomienda a los usuarios de la red de datos institucional, tomen en cuenta los siguientes pasos, para que las contraseñas a utilizar sean más robustas y más fáciles de recordar.

Paso 1: Seleccione la estrategia a utilizar

1.1. Primeras letras
Utilice las primeras letras de un conjunto de palabras.
Expresión: Quiero que mi contraseña sea fácil de recordar
Contraseña: Qqmcsfdr

1.2. Técnicas de transformación:
1.2.1. Técnica: Transliteración.

Expresión ilustrativa: fotográfico
Contraseña: foTOgrafiko

1.2.2. Técnica: Entrecruzar caracteres en palabras sucesivas.

Expresión ilustrativa: todo BieN
Contraseña: tBoideoN
Expresión ilustrativa: Carro nuevO
Contraseña: CnaurervoO

1.2.3. Técnica: Substitución de sinónimos.

Expresión ilustrativa: una hora del almuerzo
Contraseña: 60minDalimen

1.2.4 Técnica: Substitución de antónimos.

Expresión ilustrativa: tragaluz
Contraseña: TiraSombra

Paso 2: Longitud.

Generalmente se recomienda que las contraseñas contengan entre seis y nueve caracteres. Longitudes mayores son aceptables, tan largas como el sistema operativo lo permita y el usuario pueda recordar. Se deben evitar contraseñas de menos de 6 caracteres, porque por lo general son más fáciles de descifrar. La recomendación específica para este punto es que use por lo menos ocho caracteres.

Paso 3: Profundidad (Utilice Frases)

Deténgase a pensar en términos de contraseñas y comience a pensar en términos de frases. "Una buena contraseña es fácil recordar, pero difícil de adivinar." (Armstrong) El propósito de una frase mnemónica es permitir la creación de una compleja contraseña que no necesitará escribir. Ejemplos de una frase mnemónica incluirían una frase deletreada fonéticamente, tal como “me100to:)” (en lugar de me ciento feliz) o las primeras letras de una frase o algún proverbio tal como “amce+fdr” = "ahora mi contraseña es más fácil de recordar"

Lo que es más efectivo para los usuarios es escoger una frase que tenga significado personal (fácil de recordar), tomar las iniciales de cada una de las palabras en esa frase y convertir algunas de esas letras en otros caracteres (sustituir el número “3” por la letra “e” es un ejemplo común).

Haga su contraseña fácil de recordar para usted pero difícil de suponer para otro. Como se dijo anteriormente, recoger letras de una frase que tiene

significado para usted puede ser una fuente para una buena contraseña. De esta forma su contraseña es verdaderamente una "frase de paso".

3.1. Use alguna pregunta:

Pregunta: ¿Usted sabe cuál es la ruta a San José?
Contraseña: uscelrasj

3.2. Expresiones inspiradas por el nombre de una ciudad:

Expresión: Las fiestas de Palmares son en enero
Contraseña: LfdPse1

Expresión: Alajuela es la ciudad de los mangos
Contraseña: Aelcdlm!

1.3. Comidas que no le gustaban durante su infancia:

Comida: sopa de espinacas y atún con vegetales
Contraseña: sdeYacv

Paso 4: Inicie la transformación.

Tomando en cuenta la estrategia, longitud y frase elegida para su contraseña inicie la transformación de su contraseña

Paso 5: Anchura (Símbolos especiales).

No considere sólo el alfabeto. También hay números y caracteres especiales como "%", y en la mayoría de los sistemas operativos, las letras mayúsculas y minúsculas son reconocidas como letras diferentes.

Sin embargo, en algunas versiones de sistemas operativos Windows, principalmente aquellas que utilizan LAN Manager como método de autenticación, no siempre son sensibles a la diferencia entre letras mayúsculas y minúsculas. (Esto significa que no sabe la diferencia entre la "A" y la "a".)

Algunos sistemas operativos también permiten caracteres de control, caracteres "alt" y espacios para ser usados en contraseñas.

Como regla general el siguiente conjunto de caracteres debe ser incluido en cada contraseña:

- letras mayúsculas como A, B, C;}
- letras minúsculas como a, b, c;
- numerales como 1, 2, 3;
- caracteres especiales como $, ?, &; y
- caracteres alt como µ, £, Æ. (Cliff)

Intercale (o reemplace algunas letras con) signos de puntuación o símbolos como #, $, %, etc. No use espacios en blanco.

Paso 6: Mayúsculas y minúsculas.

Siempre use una mezcla de letras mayúsculas y minúsculas.

Paso 7: No Utilice Palabras de Diccionarios, Nombres propios o Palabras Extranjeras.

Como ya se ha mencionado, las herramientas de craqueo de contraseñas son muy efectivas procesando grandes cantidades de letras y combinaciones de números hasta que se halla una contraseña que corresponde, por lo que los usuarios deben evitar usar palabras convencionales como contraseñas. Por la misma razón, también deben evitar palabras regulares con números en el final y palabras convencionales que simplemente son escritas al revés, tal como "nimda", en lugar de "admin". Aunque éstos resultarían difíciles de resolver para las personas, no son ningún reto para las herramientas de ataque de fuerza bruta.

Paso 8: No Utilice Ninguna Información Personal.

Uno de las cosas más frustrantes acerca de las contraseñas es que necesitan ser fáciles de recordar para los usuarios. Naturalmente, esto lleva a muchos usuarios a incorporar información personal en sus contraseñas. Sin embargo, es preocupante la facilidad que tienen los "hackers" para obtener información personal acerca de probables objetivos. Por lo que se recomienda fuertemente que los usuarios no incluyan tal información en sus contraseñas. Esto significa que la contraseña no debe incluir nada remotamente relacionado al nombre del usuario, apodo, o el nombre de un familiar o mascota. También, la contraseña no debe contener cualquier número fácilmente reconocible como números de teléfono o direcciones u otra información que alguien podría suponer viendo su correo.

Paso 9: No escriba la contraseña.

Nunca apunte su contraseña; alguien más podría verla.

Paso 10: Una contraseña para cada sistema.

Seleccione una contraseña única. No use una contraseña que utiliza con otro propósito, tal como su PIN del cajero automático o alguna otra contraseña de un sistema.

5. **Procedimiento para la administración de contraseñas por parte de los administradores del directorio Activo (Active Directory) y administradores de aplicaciones.**

   La correcta administración de las contraseñas generadas para los usuarios de la red y aplicaciones de la municipalidad, es de vital importancia en la seguridad de toda la información institucional, por lo tanto deben cumplirse lineamientos básicos de configuración de la seguridad que deberán ser aplicados por los administradores de red y de aplicaciones. La administración correcta de las contraseñas incluye entre otros aspectos, velar porque los usuarios usen contraseñas seguras, configurar el plazo de vencimiento de las mismas, así como requerimientos de identificación y robustez.

   Los administradores de las cuentas de usuario del directorio activo (active directory), desarrolladores y administradores de aplicaciones, deberán configurar y aplicar las siguientes normas, ajustables a todas las contraseñas de red y/o aplicaciones. En el mediano plazo se buscará la forma de utilizar

una única cuenta, y el cumplimiento de lo normado en el presente documento será la base para el éxito de dicha implementación.

Sobre la seguridad de las contraseñas:

- Se debe incluir la respectiva configuración, en las aplicaciones y/o políticas del directorio activo, para que se guarde un histórico de al menos las últimas tres contraseñas usadas por el usuario, para prevenir su reutilización.

  El usuario administrador no realizará cambios a las cuentas o contraseñas que sean solicitados vía telefónica, estos deben ser solicitados por el usuario por la herramienta correspondiente, contando con autorización por el jefe o director del departamento.

Sobre la duración de la contraseña:

Toda contraseña tendrá una duración máxima de tres meses, terminado dicho período el usuario de la cuenta deberá renovarla, conforme las restricciones y recomendaciones indicadas.

Sobre la longitud de la contraseña:

La longitud de toda contraseña deberá ser igual o mayor a ocho caracteres.

Sobre la robustez de la contraseña:

- Ninguna contraseña podrá ser igual o similar a su respectivo nombre de usuario ni podrá quedar en blanco.
- Las contraseñas deben contener caracteres de al menos 3 de las siguientes 4 clases.

Clase:	**Descripción de la clase**
Letras mayúsculas	A,B,C,D…Z
Letras minúsculas	a,b,c,d…z
Números	0,1,2,3…9
Caracteres especiales	Por ejemplo: Símbolo puntuación u otros, como %,&,@,(),%

Sobre los requerimientos de "logueo"

- ✓ Requerir automáticamente el cambio de contraseña la primera vez que el usuario solicita su ingreso a la red o aplicación.

- ✓ Se debe incluir la respectiva configuración para que después de 3 intentos fallidos de logueo, la cuenta sea bloqueada y se requiera intervención del administrador para desbloquearla.

- ✓ El equipo de trabajo debe ser configurado para solicitar nuevamente contraseña de ingreso después de 10 minutos de inactividad.

6. Procedimiento para la gestión de contraseñas de administrador de las estaciones de trabajo propiedad de la Municipalidad de Curridabat

Con el fin de prevenir el acceso no autorizado a los datos de las estaciones de trabajo propiedad de la Municipalidad de Curridabat, la cuenta de administrador local de cada una de las estaciones de trabajo propiedad de la institución, debe administrarse y configurarse de manera segura, ya que de ello depende minimizar el riesgo de que terceros puedan accesar la información almacenada en las mismas.

La cuenta de administrador local de las estaciones de trabajo, tiene que ser creada y administrada, considerando características de seguridad y robustez iguales a las que se configuran para las cuentas de red y aplicaciones. Los administradores y soportistas de red, deben ser colaboradores activos con los usuarios en el cumplimiento de esta política

1. De cumplimiento por parte del encargado de soporte de las estaciones de trabajo:

   - ✓ Cada estación de trabajo será configurada de la siguiente manera: La cuenta del usuario de red se incluirá como un normal o limitado. En el caso de los desarrolladores que requieren permisos especiales, relacionados con sus funciones de programación, su cuenta de red podrá ser configurada como administrador de la estación de trabajo.

   - ✓ Todas las contraseñas deben ser configuradas tomando en cuenta lo normado en este documento para el "Uso de contraseñas robustas".

   - ✓ El administrador o soportista de las tecnologías de información, no tiene necesidad de conocer ninguna contraseña de usuario para brindar.

2. De cumplimiento por parte del usuario de la estación de trabajo:

   - ✓ No deberá bajo ninguna circunstancia cambiar la contraseña de administrador local de la máquina.

   - ✓ No deberá modificar el acceso a los archivos, de modo que el usuario administrador local siempre tenga acceso total en la estación.

   - ✓ No deberá compartir con ningún usuario o persona, incluso ni con el administrador o soportista de las tecnologías de información, la contraseñas correspondientes a sus cuentas.

3. De cumplimiento de la jefatura o Dirección.

   En caso de ausencia del usuario dueño de la estación de trabajo y de presentarse la necesidad de accesar la información contenida en ella, la jefatura del usuario deberá solicitar por escrito al administrador de cuentas del departamento de Informática respectivo, que realice las acciones tendientes para poder acceder la información, ya sea ingresando a la estación con una cuenta de administrador de dominio o procediendo a restablecer la contraseña de administrador de la estación de trabajo. Se sugiere que este tipo de acceso a la información de la estación de trabajo de un funcionario, se realice únicamente si no existe otro medio para obtener los datos requeridos, de realizarse, deberá garantizársele al usuario dueño de la estación de trabajo que no se accesarán documentos personales ni su correo

electrónico, se propone que al momento de obtener la información se cuente con la presencia de al menos un testigo.

Deberá recordar a los funcionarios sobre la necesidad del cambio periódico de dichas contraseñas, al menos cada tres meses.

7. **Procedimiento sobre la confidencialidad de la información institucional y trato con terceros.**

Cada funcionario contratado por la institución, para cumplir con las tareas propias de su cargo, tiene acceso a información institucional en diferentes formatos (escrita, digital o verbal).

Ejemplos de este tipo de información son las notas, circulares, minutas, acuerdos, bases de datos, reportes, consultas a los sistemas de información, equipos médicos que interaccionan con componentes y aplicaciones informáticas entre otros.

Toda la información confidencial a la cual cada funcionario tiene acceso en cumplimiento de sus funciones, debe ser administrada de modo que no sea divulgada a personas que podrían utilizarla en beneficio propio, en contra de terceros o de la propia institución. Ningún funcionario podrá modificar, borrar, esconder o divulgar información en beneficio propio o de terceros.

En la norma asociada con esta política, se hace referencia a la normativa y base legal que sustenta el principio de confidencialidad de la información.

Este conjunto de lineamientos son de acatamiento obligatorio para todos los funcionarios de la Institución, tanto en propiedad como interinos, así como las personas contratadas por servicios profesionales a nombre propio o de un tercero, así como a estudiantes que realizan tesis de graduación, prácticas supervisadas, trabajos comunitarios, investigaciones y cualquier otra modalidad aceptada a nivel institucional, en cualquiera de las dependencias de la Municipalidad de Curridabat, que en cumplimiento de sus funciones, tengan acceso a la información institucional.

Información confidencial. Se define como cualquier información ya sea en forma electrónica, escrita o verbal, relacionada con el cumplimiento de las funciones, los asuntos u operaciones de la Institución, que puedan ser comunicados o revelados a terceros, directa o indirectamente, incluyendo pero no limitándose a: contratos, informes, memorandos, documentación legal, datos financieros, planes o estrategias presentes o futuros, datos de clientes, tecnología, diseño y técnicas o cualquier información relacionada con la prestación de servicios. La información confidencial, cuenta con las siguientes excepciones:

a) Sea de dominio público por publicación u otros medios, excepto por omisión o acto no autorizado por parte de la Institución.

b) Sea obtenida legalmente por la municipalidad de un tercero independiente de la entidad, quien en el conocimiento de la institución, no tiene ninguna restricción u obligación de confidencialidad con la entidad.

c) Sea ordenada y requerida por autoridades judiciales, gubernamentales o regulatorias.

Por lo anterior, ningún funcionario de la Institución, no podrá: publicar, hurtar, vender, modificar, borrar, ocultar, analizar o destruir información institucional, mucho menos información de carácter confidencial, en beneficio propio, de un tercero.

El manejo de la información de la Institución es uno de los aspectos en donde debemos aplicar mayores controles para mantener un adecuado nivel de seguridad, especialmente cuando la información debe de proporcionarse a terceros, cuando por las labores que se estén realizando así sea requerido.

Esta norma contempla el uso que se le debe dar a toda información que se le entregue a terceros, principalmente en aquellos casos en donde por las labores que estén ejecutando se debe de utilizar información de uso confidencial de la municipalidad.

- **Velar por el cumplimiento de las cláusulas de confidencialidad, por parte de terceros.**
-

  Los funcionarios de la Institución que en determinado momento funjan como contraparte de un proyecto, deberán velar por el cumplimiento por parte de terceros, de lo estipulado en las cláusulas de confidencialidad indicadas en los respectivos contratos, en caso de notar alguna anomalía o incumplimiento deberá informarlo a su jefatura inmediata.

- **Información de modelos de seguridad.**

  Ningún funcionario de la Institución, podrá brindar a terceros información de los modelos de seguridad implementados en la Municipalidad de Curridabat.

- **Informar sobre la pérdida o hurto de información de la Municipalidad de Curridabat.**

  En caso de pérdida o robo de información mientras está siendo utilizada por terceros, el funcionario de la institución que funja como responsable del proyecto en la municipalidad, deberá comunicar directamente a la jefatura inmediata.

- **Información para tesis de graduación.**

  En el caso que la realización de un proyecto de tesis de graduación requiera información de la Municipalidad de Curridabat, la dirección donde se aplicará la tesis o proyecto, deberá nombrar un personero de la institución quien será el encargado de brindarle información al estudiante para la ejecución del proyecto, dicho representante designado por la jefatura correspondiente, deberá: 1) valorar que la información suministrada para efectos de realización de tesis no sea información que comprometa a la Institución o los usuarios. 2) Asimismo, como el documento de tesis se convierte en un documento público, el representante , debe velar porque dicho documento no contenga información confidencial que no debe ser expuesta a conocimiento público, 3) en caso de determinar que el documento contiene información confidencial o que no convenga someterla a conocimiento público, el representante deberá solicitar al estudiante que realiza la tesis la

exclusión de dicha información en el documento y dejar constancia de dicha solicitud.

- **Uso de la información de los sistemas de la Municipalidad de Curridabat.**

  La información contenida en las bases de datos, medios de almacenamiento y sistemas, es propiedad de la Municipalidad de Curridabat, en los casos que la Institución autorice su uso para un proyecto o actividad específico deben ser utilizados únicamente para los fines previamente establecidos por las partes, una vez terminada la ejecución del proyecto.

- **Personal responsable del manejo de la información en proyectos con terceros.**

  Se deberán establecer las personas responsables por ambas partes para el manejo de la información que se envíe y se reciba, no se deberá suministrar ninguna información a personas que no estén previamente autorizadas por la institución.

- **Información de cuentas de usuario.**

  Al administrador le queda estrictamente prohibido revelar información relativa a cuentas de usuarios a terceros, en caso de necesitar efectuar procesos de pruebas o algún otro se deberán de definir cuentas específicas para dicho proceso.

- **Uso de datos personales.**

  Los datos personales de los usuarios no deben ser entregados por la Municipalidad a terceros, esto debido a la confidencialidad que estos esperan de la institución de la información que esta administra. En caso de que sea necesario para la ejecución de pruebas o alguna otra razón se deberá mantener la confidencialidad de la información suministrada.

- **Procedimiento sobre uso adecuado de las estaciones de trabajo.**

  La Institución, asigna a los funcionarios en apoyo al cumplimiento de sus labores, cuando así se requiere una estación de trabajo. Estos equipos son parte del patrimonio institucional y por lo tanto, debemos buscar la mejor forma de utilizarlos, tomando en cuenta aspectos de seguridad físicos y lógicos para su protección. Las normas asociadas a esta política incluyen entre otras, las mejores prácticas de uso de las estaciones para proteger el equipo y la información contenida en él.

  Será responsabilidad de todos los usuarios a los cuales se les haya asignado una estación de trabajo y de sus respectivas jefaturas, acatar las normas que se detallan más adelante.

  De cumplimiento por parte de los usuarios de las estaciones de trabajo:

  1. Darle un uso adecuado donde el mismo no deberá recibir más que el deterioro normal, derivado de su uso normal. Se indican como buenas prácticas:

     - No ingerir alimentos cerca del equipo de cómputo, de modo que no se vea dañado por regarle líquidos o residuos de comida.

- Velar porque no esté ubicado debajo de goteras y/o ventanas, si es así deberá movilizarlo cuanto antes, de modo que el equipo no se vea afectado.

- No utilizarlo sobre ningún tipo de base inestable, como cajas, o mesas en mal estado, de modo que la probabilidad de caer al suelo sea alta.

- Reportar al encargado de soporte mediante las herramientas del sistema de solicitudes cualquier anomalía que se esté presentando durante su uso.

- Llevar un control de las partes que le cambien a la estación de trabajo asignada, para su respectiva comunicación al funcionario encargado de activos en su unidad de trabajo.

- Cuando el equipo presente problemas de funcionamiento no golpearlo porque podría empeorar el problema, preferiblemente comunicar el incidente a soporte técnico, utilizando la herramienta de solicitudes de informática, pudiendo accesarla desde cualquier terminal o bien el jefe del área puede realizar la solicitud.

- Si no cuenta con experiencia suficiente en mantenimiento de equipos no debe tratar usted de arreglarlo, debe contactar al responsable de soporte técnico

- Acatar las instrucciones que con respecto al uso de la estación de trabajo, le dé el encargado de soporte técnico.

- En caso de tener que movilizar el equipo, debe desconectar todos los dispositivos conectados al CPU y la corriente eléctrica. En la medida de lo posible empacarlo de modo que el movimiento o vibraciones que sufra durante su traslado, no produzca ningún daño en el equipo.

- Al finalizar las labores y siempre que el equipo no esté en uso, utilizar en la medida de lo posible cobertores apropiados para el equipo.

- No colocarle adornos excesivos o con imanes que podrían afectar el desempeño del equipo.

- Mantener una ventilación adecuada para evitar el sobrecalentamiento de los equipos, no colocar objetos que impidan el ingreso o salida de aire, al equipo.

2. En cuanto a la información almacenada en la estación de trabajo, se tiene que:

   ✓ Los equipos facilitados por la Institución para que el funcionario desarrolle sus labores son propiedad de la Municipalidad de curridabat, por lo que para efectos de la institución la información contenida en las mismas, se puede catalogar desde el punto de vista de derecho de acceso como:

- De interés institucional (es decir pertenece a la Institución, y ha sido generada en cumplimiento de las labores para las cuales el funcionario ha sido contratado).

- De carácter privado-personal (es decir la información que el funcionario considere como íntima, confidencial o personal).

Se sugiere que toda esa información que el usuario considere como personal, sea almacenada en una carpeta específica y se identifique como tal, nombrando dicha carpeta con algún calificativo que haga referencia a su carácter personal, íntimo, confidencial u otro similar.

En caso de requerir acceso a la información contenida en la estación de trabajo, salvo voluntad expresa del interesado, ninguna otra persona que no sea la dueña de la información podrá accesar la información confidencial del interesado. Todo acceso a la información contenida en las estaciones de trabajo, será realizado en presencia del interesado.

- ✓ Ningún usuario de estación de trabajo está autorizado para almacenar material pornográfico, u ofensivo en ningún medio de almacenamiento de la estación de trabajo o dispositivo periférico, o en ningún otro medio de almacenamiento disponible en la red institucional, y mucho menos propagarlo distribuirlo a otras personas.

- ✓ De darse el caso que la estación de trabajo presenta problemas de rendimiento debido a poco espacio en el disco duro, será responsabilidad del usuario que tiene asignada la estación de trabajo eliminar todos aquellos archivos que puedan borrarse dando prioridad a eliminar los archivos que no sean indispensables para el cumplimiento de sus funciones. Podrá buscar la asesoría con informática en caso necesario, para cumplir con este punto.

- ✓ El usuario deberá buscar colaboración con el departamento de Informática, para la realización de los respaldos, contando con dicha colaboración el usuario será el responsable de hacer respaldos actualizados de la información que se considera critica, para realizar esta labor deberá coordinar con el personal informático del área y realizar la coordinación respectiva para evitar posibles pérdidas de información considera crítica para la organización.

- ✓ En los respaldos de información que se realicen no se admite incluir ningún tipo de información personal, mucho menos videos o imágenes que no correspondan a las tareas asignadas y al quehacer del departamento.

De cumplimiento por parte de los administradores del departamento de Informática.

Los soportistas del departamento de informática, deberán velar porque los equipos de cómputo, cuenten con:

- Cada Centro de Gestión Informática, en coordinación con el respectivo encargado de activos, deberá contar con un inventario actualizado de las estaciones de trabajo, correspondiente a todas las estaciones de

trabajo adscritas al Centro de Gestión Informática, dicho inventario debe incluir el nombre del funcionario responsable del equipo, así como el listado de las características técnicas del hardware, donde al menos se conozca:

- La capacidad del disco duro, la cantidad de memoria RAM, el tipo de procesador y su velocidad, el tipo de tarjeta madre y sus características, de ser posible contar también los números de serie de los dispositivos que la contengan.

- Software autorizado por la Institución o bien licencias adquiridas por la Institución.

- Actualización de los antivirus y parches necesarios para asegurar el buen funcionamiento del equipo.

- Asegurar el buen funcionamiento de la conexión del equipo de cómputo a la red institucional

- Elaborar las recomendaciones técnicas o informes que le permitan al usuario detectar los problemas técnicos que a meriten cambio de repuestos o dispositivos.

- Es obligación de usuario y su respectivo Centro de Gestión Informática, asegurarse que el antivirus de su equipo se encuentre actualizado y ejecutarlo regularmente para prevenir la aparición de virus y se propague por la red.

9. Procedimiento sobre uso adecuado de la red de datos institucional.

La Institución asigna a cada funcionario en apoyo al cumplimiento de sus labores, una cuenta de acceso a la red de datos institucional, con la cual el dueño puede accesar diferentes elementos que la componen como: servidores de archivos, servidores de bases de datos, impresoras, archivos compartidos en otras estaciones de trabajo, sistemas y aplicaciones Institucionales, entre otros. Dicha cuenta es otorgada para facilitar las labores de los funcionarios mediante el uso de tecnología informática. Por lo anterior, los usuarios deben hacer uso de la red y de los servicios relacionados con esta, estrictamente en cumplimiento de las labores institucionales, tomando en consideración la privacidad de otros usuarios y la no saturación de la red por uso indebido del ancho de banda, entre otros argumentos.

Será responsabilidad de todos los usuarios a los cuales se les haya asignado cuenta de acceso a la red institucional, acatar las normas que se detallan más adelante.

El usuario con una cuenta de red tendrá las siguientes responsabilidades:

1. Cambio periódico de la contraseña de la cuenta de red, para lo cual debe acatar lo estipulado en lo estipulado en este documento, del correcto uso de contraseñas de parte de los usuarios de red y aplicaciones".

2. No compartir archivos o carpetas en su estación de trabajo, sin restricción de usuarios o atributos. Esta situación puede poner en peligro

la información que está almacenada en su estación de trabajo y que es propiedad de la Institución. De tener la necesidad de compartir archivos, deberá asesorarse con su el departamento de informática.

3. No saturar el ancho de banda de la red, copiando y/o accesando archivos de índole personal utilizando infraestructura de la red, no importa cuál sea su formato y de igual manera haciendo mal uso del internet.

4. En caso de traslado de datos de interés de la administración, cuyo traslado por la red pueda causar saturación en los servicios de red, deberá coordinarse con los administradores del respectivo departamento de Informática, para que se determine el mejor medio y horario para el traslado de la información.

5. No accesar equipos, o servicios a los cuales no se ha brindado el permiso específico para su utilización.

De cumplimiento por parte de los administradores

1. Realizar labores de trasiego de información por la red institucional, en horarios en los cuales el tráfico no interfiera con los servicios de la red institucional.

2. Realizar labores de mantenimiento de los equipos de comunicaciones y servidores, en horarios que no interfieran con las labores diarias de las unidades.

3. Realizar monitoreos en busca de optimizar el uso de la Red de Datos y desempeño de los equipos.

10. Procedimiento sobre uso de equipos portátiles.

La institución asigna equipos tipo portátil tales como: laptops, table pc, o computadoras de bolsillo tipo "hand help, palm, pocket pc" entre otros, a sus funcionarios, para facilitarles el cumplimiento de sus labores. Los funcionarios que tengan asignado cualquier equipo tipo portátil, deben hacer correcto uso de los mismos y de la información que contienen, porque dadas las características de ese tipo de tecnología, se presentan más vulnerabilidades de seguridad, por las facilidades de conectarse diferentes ambientes informáticos, en los cuales la institución no tiene control, y adicionalmente son más susceptibles a robo o pérdida.

Será responsabilidad de todo funcionario de la Municipalidad, al que se le haya autorizado o asignado la utilización de un computador portátil, u otro tipo de equipo portátil, donde deberá velar por la protección, uso adecuado y buen funcionamiento del mismo tal y cual lo establecen las siguientes regulaciones.

Responsabilidades del funcionario a quien se le asigna el equipo portátil:

- Asegúrese de tener la autorización respectiva para el uso del equipo, para portarlo dentro o fuera de las instalaciones de la Municipalidad.

- Mantener el equipo en el estuche de protección adecuado.

- Asegurar que siempre pueda identificarse la localización física de la portátil, así como conocer la sensibilidad de los datos en el equipo y el nivel de seguridad.

- Utilizar el antivirus y el analizador de código malicioso regularmente en la portátil, pida ayuda al Area de Soporte Técnico al respecto de este punto.

- Llevar a cabo los procedimientos de seguridad adecuados contra el robo. Considere el uso cables, candados u otros dispositivos de seguridad en las oficinas.

- En caso de robo de la computadora portátil, se debe de reportar inmediatamente al encargado del inventario y a la autoridad policial respectiva, indicando el número de placa y serie respectiva.

- No dejar nunca el equipo portátil desatendido, ya sea en la oficina y especialmente cuando esté de viaje, hoteles, sitios de atención al cliente, vehículos.

- Asegurar que estén disponibles las facilidades de protección física del equipo, las cuales deben de aplicarse mientras el equipo no esté en uso, como por ejemplo los controles biométricos en caso que estén disponibles.

- Asegurar que exista la protección física adecuada para aplicarse si el equipo es utilizado en el hogar del usuario u otras instalaciones que no sean de la institución.

- Aplicar la normativa en el uso de Internet, Intranet y Extranet.

- Uso apropiado del servicio de correo electrónico institucional.

- Únicamente el usuario custodio del equipo debe de hacer uso del mismo, no se autoriza el uso por parte de amigos, miembros de la familia u otros para la manipulación del equipo.

- Antes de apagar su computadora cierre todas las aplicaciones en uso para evitar fallas de funcionamiento al volver a encenderla.

- No forzar el apagado del equipo durante los procesos de actualización del mismo pues podrían afectar negativamente la estabilidad del sistema operativo.

- No coloque una computadora portátil en posiciones que obstruyan la entrada de aire del ventilador y salida de calor del sistema.

- Procure no tocar la superficie de la pantalla con los uñas o la punta de un lápiz o un bolígrafo. Al limpiarla, use telas antiestáticas secas y líquidos especiales para este tipo de pantallas (sin alcohol, sin jabón y sin agentes abrasivos), y hágalo sólo cuando la computadora esté apagada.

- Hacer respaldos de la información contenida en el equipo portátil regularmente.

- Utilice siempre una contraseña al encender el equipo como un simple bloqueo para usos oportunistas.

- Asegure la confidencialidad y seguridad de archivos de respaldo.

- Analizar los archivos antes de copiarlos a la portátil, independiente de la fuente de procedencia

Responsabilidades del Departamento de Informática:

- ✓ Deberá llevar el control de quien es el responsable de los equipos portátiles, e inventariar las características de dichos equipos.

- ✓ Darle el soporte requerido para el mantenimiento preventivo y correctivo de los equipos portátiles

11. Procedimiento sobre uso unidades de respaldo de la información.

Dada la importancia de la información que maneja la institución y la necesidad de resguardar los datos, así como emitir información a otras entidades, surge la necesidad de establecer la normativa para regular el uso de cualquier tipo de unidades de respaldo sean estas internas o externas, entre las que podemos mencionar los quemadores de discos compactos, DVD, cintas magnéticas, entre otros; con el objeto de que su uso sea para labores propias de la institución.

Por lo anterior, toda unidad que cuente con dispositivos para la realización de respaldos computadoras de escritorio, portátiles, servidores y equipos médicos) debe velar porque se haga un uso adecuado de esos recursos, utilizándolos únicamente para cumplir con los intereses de la institución, y tomando en cuenta las funcionalidades operativas del equipo.

Será responsabilidad de las jefaturas de todas las unidades de la institución y de los funcionarios designados por las jefaturas de las unidades en los cuales se cuentan con dispositivos de respaldo, acatar lo dispuesto en esta norma y velar por el uso óptimo de los equipos. Dado que los dispositivos de respaldo pueden ser internos o externos, esta norma aplica para cualquiera de los casos.

El encargado de la administración del equipo "utilizado para respaldos" debe de:

- Documentar la información que ha sido respaldada, considerando: cantidad y descripción de archivos respaldados, tamaño, fecha, y el propósito del respaldo.
- Utilizarlo para labores institucionales de acuerdo a la naturaleza del área de trabajo; lo cual tiene implícito la no reproducción de información no autorizada (información personal o de entretenimiento).

- En caso de fallas técnicas notificar de inmediato al encargado, Soporte Técnico.

- En caso de robo o extravío notificar a la instancia respectiva para iniciar el proceso administrativo respectivo.

- En el caso de utilizarse para respaldos de aplicaciones o datos de las estaciones de trabajo de los funcionarios, referirse a lo normado con respecto a la realización de respaldos, en este documento.

12. Procedimiento sobre uso dispositivos de almacenamientos externos (DVD,CD,LLAVES MAYAS, DISCOS EXTERNOS,MEMORIAS SD)

La información constituye uno de los principales activos de la institución, por tanto el manejo adecuado de la misma es responsabilidad de todos los funcionarios así como la correcta utilización de los dispositivos que el mercado ofrece para la administración y respaldo información. Por lo tanto todos los usuarios de tecnologías de información que manipulen dispositivos como: CD, DVD, llaves maya, discos duros externos, entre otros, deben utilizarlos considerando la importancia de la información que contienen, buscando mecanismos seguros para su almacenamiento o distribución.

Es responsabilidad de todos los funcionarios de la Municipalidad de Curridabat que entren en contacto con un equipo de cómputo, velar por el cumplimiento de las normas con relación al manejo de la información y la utilización de los dispositivos tecnológicos para el almacenamiento de la información.

Mantener sus dispositivos de almacenamiento, rotulados (en caso que sea posible) y en un lugar seguro, de forma tal que de requerir alguno de estos, sea de fácil localización.

- No deje los dispositivos de almacenamiento accesibles, a personas ajenas cuando no esté en uso.

- No deje los dispositivos de almacenamiento externos como llaves maya, CD’s o DVD’s en el quipo cuando usted no esté utilizándolo.

- Maneje en los dispositivos de almacenamiento únicamente la información que es requerida para el desempeño de sus funciones únicamente.

- En caso de requerir el almacenamiento de volúmenes grandes de información notificarlo a su jefatura, justificando la necesidad de la misma.

- Verifique que los archivos a copiar, estén libres de virus o software malicioso, antes de copiarlos ya sea del dispositivo a la máquina o viceversa.

- En caso de extraviar alguno de los dispositivos, notificar la pérdida.

- Siga las recomendaciones del fabricante sobre el uso y cuidados de los dispositivos de almacenamiento.

- Tome en cuenta condiciones ambientales tales como temperatura, humedad, entre otros; que pueden dañar la información almacenada.

- En el caso de tener que almacenar información sensible, realice al menos dos copias adicionales, debidamente protegidas como prevención.

- Preferiblemente almacene en gabinetes de materiales con resistencia al fuego para sus dispositivos.

13. Procedimiento del uso adecuado de las unidades de potencia interrumpida.

Las fuentes de potencia ininterrumpida (UPS por sus siglas en inglés), cumplen la función de mantener el suministro de energía estable a los equipos de cómputo, cuando este se interrumpe.

Ante el respaldo que brindan las UPS a la operativa del equipo y la ampliación de tiempo para que el usuario pueda aplicar las medidas de contingencia, se convierten en elementos importantes para el cuidado de los equipos y la información que estos contienen, razón por la cual todos los usuarios que administren o tengan asignadas para su uso UPS, deben utilizarlas cumpliendo con los lineamientos para el uso y el mantenimiento adecuados de las mismas.

Es responsabilidad de todos los funcionarios o unidades que tengan a su cargo un equipo de cómputo conectado a un dispositivo UPS.

De cumplimiento de parte del área de informática

- Tener un registro con el modelo, marca, placa, cantidad de receptáculos, dispositivos interconectados a la UPS y un listado de las comprobaciones de la estabilidad y estado de carga de la batería.

- Efectuar Inspección visual externa, comprobación de todas las conexiones, alimentación de la UPS, previa utilización del equipo.

- Comprobación visual de todos los indicadores de la UPS, tanto ópticos (luces que pueda tener como indicadores de fallas, operación, u otros) como acústicos, en caso de fallos comunicarlo inmediatamente al departamento de informática

- Deberán hacer la comprobación-calibración de valores eléctricos, si fuera necesario mediante equipos de medida externa (tester, multímetro, osciloscopio, etc); limpieza de la parte de control y electrónica, mediante soplado delicado con aire comprimido; en su caso, actualizaciones del software de control, drivers, etc. Comprobación del software de control remoto de la UPS, en caso de existir.

- Velar por que la ubicación y ambiente de trabajo de los equipos, temperatura (que la batería se mantenga fría y que el lugar de operación de la misma sea lo más frío posible), humedad, polvo, etc.

- Elaborar ficha actualizada de mantenimiento de equipo, situada en el mismo equipo UPS, que permita conocer el estado de revisión, incidencias, etc. de forma inmediata.

- La forma en que se le suministra carga a la batería es muy importante y afecta sensiblemente la vida útil de la misma. Una batería aumenta su vida útil si está permanentemente mantenida en estado de flotación, ya que hay procesos de envejecimiento que son atenuados si se ejecuta esta premisa. De aquí es importante que aunque el UPS se encuentre apagado, pero conectado a la red, el cargador continúe suministrando la carga de Flote.

- Cuando la UPS es conectada por primera vez, se debe permitir la carga libre de la misma por un mínimo de 24 horas, esto es sin ningún dispositivo conectado a la misma. Luego de ese lapso, se puede conectar a ella, únicamente el monitor y la CPU, ya que la carga que almacena la UPS, solo está diseñada para soportar estos dos dispositivos. No deben conectarse a este equipo, parlantes, abanicos, calculadoras, regletas, impresoras ni ningún otro dispositivo, ya que inhiben a la UPS de su carga temporal y disminuye su vida útil.

- Se debe de comprender que la carga de energía eléctrica que la UPS almacena para una situación de corte del fluido eléctrico, es de aproximadamente diez minutos. (esto puede variar significativamente dependiendo del estado de la batería y la potencia de la unidad).
- Por tal razón en este lapso de tiempo se debe salvaguardar la información que se esté procesando en ese momento para no perderla y proceder a apagar todo el equipo completo incluyendo UPS.

- Indicar al usuario respectivo de una UPS, que no deberá conectar más equipos adicionales sin la recomendación del técnicos respectivo.

- Una Vez finalizada la jornada laboral, proceder apagar el equipo, para evitar su descarga si en horas de la noche sucede un corto eléctrico y el equipo no es apagado en el tiempo requerido

14. Procedimiento sobre uso Stock de repuestos de equipo de cómputo.

La existencia de un stock de repuestos para equipo de cómputo en las unidades de la institución, es importante para la continuidad en la prestación oportuna de los servicios, por lo tanto debe contarse con los controles adecuados que permitan tener repuestos actualizados, que los mismos estén disponibles cuando se necesiten y que realmente sean utilizados en beneficio de la institución.

Se justificará la existencia de un stock de repuestos únicamente para aquellas unidades que cuenten con personal técnico capacitado en mantenimiento y reparación de equipo de cómputo. Para aquellas unidades que no cuenten con el personal técnico indicado o el mismo sea insuficiente, podrán recurrir a la contratación externa de soporte técnico, siempre y cuando cumplan con el marco normativo y legal respectivo.

Las indicaciones relacionadas con tipo de repuestos y cantidades a adquirir, se detallan a continuación:

1) Será responsabilidad del encargado de soporte de la institución, velar por tener un inventario actualizado del stock de repuestos, la adquisición de repuestos en buen estado, no descontinuados y acorde a las características de los equipos de cada unidad.

2) El responsable de la administración del stock de repuestos deberá llevar actualizados los siguientes controles, ya que él o ella deberán responder por el correcto uso de los mismos.

    a) Inventario de todos los repuestos comprados, que incluya:

        i. las características técnicas de los mismos, considerando:

            - número de serie
            - modelo
            - otras señas técnicas relevantes según el tipo de repuesto

        ii. la fecha de adquisición
        iii. el monto que se pagó por cada repuesto,
        iv. en caso de ser utilizado, registrar el número de activo del computador donde se instaló, en caso de no contar con el número de placa utilizar el número de serie del equipo.

    b) Formular la metodología de compras, donde deben considerarse las características de los equipos, tipos de ranuras para las tarjetas de video y red, configuración de memoria que aceptan los equipos, interfases utilizadas por los discos duros, para asegurarse que los repuestos adquiridos sean realmente utilizados en los equipos existentes.

    c) La cantidad de repuestos que se mantengan en stock debe tener relación directa con a cantidad de equipos que son administrados por el departamento de Informática de las unidades, y adquirir en mayor cantidad los repuestos que están más propensos a fallar, se debe considerar al menos la compra de:

        - ✓ discos duros,
        - ✓ DIMM de memoria RAM,
        - ✓ tarjetas de red,
        - ✓ tarjetas de video,
        - ✓ mouses,
        - ✓ teclados
        - ✓ Fuentes de poder internas.

Por último es importante que las unidades comprendan que el objetivo de esta política es contar con algunos repuestos que permitan la continuidad del servicio, (por medio de una reparación oportuna, que evitará reducir el tiempo de respuesta de fallas y el papeleo de rigor que debe contemplar la compra de un repuesto para los equipos de cómputo), no es que dicho papeleo se elimina, dado que el mismo debió ser realizado en el momento de hacer la compra general de repuestos. No es aceptable que se utilice este medio para

mejorar por completo equipos de cómputo (sustitución de todos los componente internos del "case" del equipo), en dicho caso lo que corresponde es darlos de baja y presupuestar la compra del o los equipos nuevos.

Documentación de los procedimientos de operación.

Los responsables de las áreas funcionales del área de informática, deben elaborar y darle mantenimiento a los procedimientos de operación, respaldo y recuperación de los recursos TIC a su cargo. Todos estos procedimientos deberán estar almacenados y accesibles a quien se disponga por parte del área de TI.

Los procedimientos deben estar registrados electrónicamente y contar con un respaldo físico que pueda ser accedido fácilmente sin necesidad de contar con un acceso a la red de comunicación institucional.

Trimestralmente cada responsable de recursos, deberá proceder a validar la información contenida en los procedimientos bajo su responsabilidad.
Se debe llevar dentro de cada procedimiento un registro para control de cambios efectuados al mismo, contemplando la fecha de la modificación del procedimiento, el responsable de la modificación y un detalle de la modificación efectuada.

15. Procedimiento sobre Separación de ambientes de trabajo.

El ambiente utilizado para el desarrollo de aplicaciones debe estar separado del ambiente de producción. Para esto se deberá considerar una separación física o virtual, garantizando la independencia de estos ambientes. Los desarrolladores de sistemas no deben tener acceso a los sistemas y datos en producción, y las pruebas que se efectúen sobre sistemas en desarrollo se deben hacer sobre una plataforma independiente a la de producción, con un ambiente totalmente controlado.

16. Procedimiento sobre realización de respaldos.

"La posesión más valiosa en la mayoría de las organizaciones es la información". Bajo esa premisa el departamento de Informática deberá velar por la existencia de metodologías y herramientas para la creación de respaldos de la información municipal.

Estas metodologías y herramientas deberán cumplir con las siguientes características:

- Los respaldos deberán incluir toda la información relevante de cada funcionario municipal que permita la continuidad de las operaciones en caso de falla en cualquier equipo que sea propiedad de la municipalidad.

- Se debe respaldar toda información almacenada en los servidores de la municipalidad que sea importante para garantizar la continuidad de las operaciones de la institución.

- Estos respaldos deberán ser realizados de manera automática, evitando en la medida de lo posible la participación de cada funcionario.

- No se deberá incluir dentro de la información a respaldar información de carácter personal o no relacionado con las operaciones y labores dentro de la municipalidad.

- Se deben garantizar medios para detectar fallas en la realización de los respaldos.

- Una vez al mes, el departamento de informática debe realizar pruebas de recuperación de información para garantizar que la información respaldada puede ser recuperada.

- La información respaldada es completamente confidencial. El departamento de informática deberá garantizar que únicamente los dueños de la información respaldada puedan tener acceso a ella.

- En caso de procesos e investigaciones judiciales, únicamente los funcionarios judiciales a cargo del proceso podrán tener acceso a la información.

- Los medios para almacenaje de información deberán garantizar al menos dos niveles de redundancia.

- La información respaldada no deberá ser tratada como información para consultas. Su uso está limitado a la recuperación ante fallas y errores (sin importar si son debidos a fallas humanas o tecnológicas). Por esta razón, los funcionarios deberán almacenar información histórica que consideren importantes para sus funciones.

- Los respaldos de información nunca deberán ser realizados en el mismo equipo en donde se encuentra la información original.

MC-PSIN-0004: Directriz para el Uso del Servicio de Correo electrónico y Acceso a Internet

Introducción

Objetivo

Regular el uso de los servicios de correo y el acceso a Internet, para lo cual emite los siguientes lineamientos de cumplimiento obligatorio para todo el personal (Interno, Comisiones, u otros organos instalados en la institución) que utilicen los recursos de la red.

Alcance

La Alcaldía y el Departamento de Informática considera indispensable regular el uso de los servicios de correo y el acceso a Internet, para lo cual emite los siguientes lineamientos, que son de cumplimiento obligatorio para todo el personal que utilice los recursos de la red.

Los usuarios deben estar enterados y asumir los compromisos, normas y reglamentos que han adquirido para el uso del correo y el acceso a Internet, tomando todas las medidas que correspondan para que estas normas se respeten y se cumplan.

El uso de la red y recursos de información, están disponibles para fortalecer el flujo de información interna, la investigación en materia tributaria, administrativa y apoyar a las diferentes tareas encomendadas para mejoramiento de nuestras labores. Todos los usuarios de la red están sujetos a esta política y a los términos de este Reglamento, y a una actuación con altos principios morales y éticos al utilizar los recursos de la Municipalidad, el uso inapropiado de la red será sancionado con la eliminación del acceso a estos recursos y puede conllevar a la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables.

El uso de los recursos deberá tomar en cuenta las medidas de seguridad que garanticen la integridad de los sistemas información, ya instalados y su accesibilidad por otros, para hacer el trabajo eficiente y productivo.

Los Directores y Jefes de cada área tienen la potestad de dar seguimiento al empleo que se dé al servicio de Internet por sus subalternos. Solicitando informes cuando los requieran de los sitios visitados al departamento de informático y procederá a valorar el correcto uso del servicio y de tomar las acciones estipuladas en reglamento Disciplinario, para tales fines.

Definiciones, Acrónimos, y Abreviaciones

- **Internet:** Conjunto de redes, redes de ordenadores y equipos físicamente unidos mediante cables que conectan puntos de todo el mundo. Estos cables se presentan en muchas formas: desde cables de red local (varias máquinas conectadas en una oficina o campus) a cables telefónicos convencionales, digitales y canales de fibra óptica.

- **Correo electrónico:** En inglés e-mail (electrónico mail), es un servicio de red que permite a los usuarios enviar y recibir mensajes rápidamente (también denominados mensajes electrónicos o cartas electrónicas) mediante sistemas de comunicación electrónicos. Por medio de mensajes de correo electrónico se puede enviar, no solamente texto, sino todo tipo de documentos digitales.

- **Intranet:** Describe la implantación de las tecnologías de Internet dentro de una organización, más para su utilización interna

- **Mensajería Instantánea:** La mensajería instantánea (conocida también en inglés como IM) es una forma de comunicación en tiempo real entre dos o más personas basada en texto. El texto es enviado a través de dispositivos conectados a una red como Internet.

- **IRC:** IRC (Internet Relay Chat) es un protocolo de comunicación en tiempo real basado en texto, que permite debates entre dos o más personas. Se diferencia de la mensajería instantánea en que los usuarios no deben acceder a establecer la comunicación de antemano, de tal forma que todos los usuarios que se encuentran en un canal pueden comunicarse entre sí, aunque no hayan tenido ningún contacto anterior

- ICQ: ("I seek you", en castellano te busco) es un cliente de mensajería instantánea y el primero de su tipo en ser ampliamente utilizado en Internet, mediante el cual es posible chatear y enviar mensajes

instantáneos a otros usuarios conectados a la red de ICQ. También permite el envío de archivos, videoconferencias y charlas de voz.

- Messenger: Cliente de Mensajería de Microsoft.

Referencias

- *Normas y Políticas en el uso de Servicios de Correo y Acceso a Internet*. Ministerio de Hacienda.
-
- *Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE), emitidas por la Contraloría General de la República.*

Responsabilidades

Es responsabilidad de todo funcionario de la Municipalidad de Curridabat, cumplir con las normas y procedimientos establecidos en este documento para el uso de los servicios de correo e Internet.

Lineamientos Establecidos

Usos Aceptables

a. Comunicación e intercambio con la comunidad académica, universitaria u otras instituciones con el fin de tener acceso a los últimos avances relacionados con la especialidad o tareas desempeñadas
b. No utilizar para publicidad de tipo comercial o personal alguno.
c. Comunicación entre instituciones o empresas privadas siempre y cuanto estén vinculadas con las tareas encomendadas.
d. Actividades de capacitación por medio virtuales o en línea.

Usos Inaceptables

a. Cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular.

b. Acceso a lugares obscenos, que distribuyan libremente material pornográfico, o bien materiales ofensivos en perjuicio de terceros.

c. Queda prohibido el acceso a sitios de descarga de programas gratuitos de música, salas de charla de cualquier tipo, toda clase de mensajería instantánea, IRC, ICQ, así como servicios de correo gratuito de cualquier índole para enviar información laboral.

d. El único correo electrónico autorizado para uso de los Funcionarios Municipales, para realizar labores institucionales dentro de la RED es el Correo Municipal.

e. El Messenger será el único canal de comunicación extra a utilizar por los funcionarios, quedando supeditado al uso correcto del mismo para fines laborales y en beneficio de la institución.

Administración de la Red

a. La administración de la red, del Departamento de Informática, se reserva el derecho de ejercer control sobre el contenido de la información que pase por la red, o de quien la utilice, quedando bajo la responsabilidad del funcionario que la accede o la utilice. Expuesto lo anterior, la administración tiene en funcionamiento herramientas de control (Firewalls a nivel de Software e implementando actualmente a nivel de hardware) que posibilitan analizar y detectar usos indebidos, por lo anterior se advierte que el contenido de la información consultada en Internet y el contenido de los correos electrónicos es monitoreada y sujeta a controles y reportes sobre su uso.

b. Corre por cuenta o riesgo del usuario cualquier información obtenida por medio del servicio de Internet.

c. Los mensajes que se envíen vía Internet, serán de completa responsabilidad del usuario emisor y en todo caso deberán basarse en la racionalidad y la responsabilidad individual. Se asume que en ningún momento dichos mensajes podrán emplearse en contra de los intereses de personas individuales, así como de ninguna otra institución o compañía.

d. El Departamento de Informática, tiene la autoridad para controlar y negar el acceso a cualquier funcionario que viole las políticas o interfiera con los derechos de otros usuarios. También tiene la responsabilidad de notificar a aquellas personas que se vean afectadas por las decisiones tomadas así como a las jefaturas inmediatas.

e. El Departamento de Informática, utiliza herramientas de monitoreo del uso de los recursos, por lo cual podrá establecer controles de acceso a sitio y de envío de información masivamente por la red.

f. El Departamento de Informática enviará reporte del uso del servicio de correo o Internet a las Jefaturas respectivas con copia al departamento de recursos humanos, para que tomen medidas tendientes a mejorar su utilización.

g. La demanda de servicios puede ocasionalmente exceder la disponibilidad de recursos de la institución, por lo que serán establecidas prioridades, dando la más alta prioridad a las actividades consideradas más esenciales para el buen funcionamiento de las gestiones y servicios de la Municipalidad.

h. El administrador de la red monitorea en forma automática los sitios visitados por los funcionarios, por lo cual se advierte que se aplicaran las sanciones establecidas por el acceso indebido.

Prohibiciones

a. La transmisión de materiales en violación de cualquier regulación, queda prohibida. Esto incluye, pero no se limita, a materiales con derechos de propiedad intelectual, materiales que legalmente se consideren amenazantes u obscenos. Lo anterior en cumplimiento con el

Decreto N° 29915-MP Prohibiciones Material Pornográfico-Equipo Electrónico-Reglamento Autónomo de Servicio-Dirección General de Servicio Civil.

b. Debido al alto nivel de seguridad con el que se debe de contar en la Municipalidad, las claves de acceso a la red, sistemas y correo electrónico deberán de ser estrictamente confidenciales y personales.

c. Utilizar los servicios de comunicación, incluyendo el correo electrónico o cualquier otro recurso, para intimidar, insultar o acosar a otras personas, interferir con el trabajo de los demás provocando un ambiente de trabajo no deseable dentro del contexto de las políticas de la Municipalidad.

d. Utilizar los recursos de la Municipalidad para ganar acceso no autorizado a redes y sistemas remotos.

e. Provocar deliberadamente el mal funcionamiento de computadoras, estaciones o terminales periféricos de redes y sistemas.

f. Poner información en la red que infrinja los derechos de los demás.

g. Utilizar los servicios de red para juegos a través del servicio de Internet o Intranet.
h. Utilizar los servicios de red para enviar archivos que sean confidenciales.

i. La exhibición de material pornográfico en cualquier lugar de la institución utilizando el equipo de cómputo y/o los servicios de comunicación de la Institución, así mismo el uso de equipo electrónico para observar o reproducir pornografía. El incurrir en el incumplimiento de esta normativa. Acarrea una falta grave que será sancionada según las regulaciones vigentes.

Uso del Correo electrónico

a. PRIVACIDAD DE CORREO: Todos los usuarios tienen derecho a la privacidad del correo electrónico, cuando éste es usado para fines de trabajo, teniendo en mente que el uso del correo es para efectuar labores, en la especialidad que tenga dicha persona. La administración de la red monitorea de manera automática el contenido del correo electrónico a fin de garantizar que el uso del mismo es el antes expuesto.

b. LIBERTAD DE EXPRESIÓN: La red está abierta a la expresión libre de ideas y puntos de vista, que tengan relación con las actividades de cada individuo en la Municipalidad; no obstante lo anterior, queda prohibido el envío de correos masivos y discusiones por este medio.

c. Lectura de Correo (para efecto laboral)

- Se debe leer el correo frecuentemente, al menos una vez al día.

- Si por una situación especial no se puede dar respuesta a un mensaje recibido, se debe enviar un breve mensaje de forma tal, que la persona que lo envió sepa que fue recibido.

- Se deben eliminar aquellos correos que ya no se requiera o no sean documentos de trabajo.

d. Envío de Correo

- Los correos deben ser enviados siguiendo un formato pre-establecido, ya que puede ocasionar que personas que reciben gran cantidad de correos puedan no leer el mensaje por su pobre estructura.

- Se deben utilizar tabuladores en los correos enviados.
- Se debe recordar que los lectores del mensaje no pueden ver su cara o escuchar su voz, todas las expresiones deben ser palabras o signos de puntuación. Se debe evitar ser sarcástico.

- Claridad en el mensaje escrito, haciendo uso adecuado de signos de puntuación.

- Se deben utilizar correos con fondos prediseñados o imágenes innecesarias que incrementan el tamaño del menaje innecesariamente y confunden los equipos encargados del trasiego del correo.

- Se deben enviar mensajes a todo el personal de la Municipalidad o dependencia, a menos que sea un asunto oficial que involucre a toda la institución.

- Antes de enviar el mensaje debe revisar el texto que lo compone y los destinatarios. Esto con el fin de corregir errores de ortografía, forma o fondo.

- Cada buzón de correo tiene un máximo aproximado de **7000 MB** de espacio disponible, tomando en cuenta los mensajes ubicados en las diferentes carpetas de la casilla de correo (bandeja de entrada, elementos enviados, elementos eliminados y cualquier otra carpeta creada en su buzón), una vez que este espacio es consumido, no será posible enviar ni recibir mensajes hasta que libere el espacio del buzón

e. Reenvío de Mensajes

- Cuando se reenvía un mensaje, se debe incluir el mensaje original, para que la o las personas, hacia las que va el mensaje, conozcan de que se está hablando en un momento dado.

- Si se utiliza un mensaje para entremezclar una respuesta, eliminando las partes que son irrelevantes. Es altamente recomendable incluir el mensaje original, tal y como fue recibido.

f. Listas de Correos

- No haga que un tema de discusión se convierta en otro tópico. Si así lo desea comience con otro mensaje.

- No se debe utilizar la cuenta de correo municipal para suscripciones a listas de amigos por Internet o de otras índoles, y en general grupos de distribución de correo, ya que provoca que gran cantidad de mensajes lleguen al correo, provocando saturación.

g. Virus

- La administración de la RED automáticamente revisa todos los correos entrantes y salientes para verificar que no tengan virus.

- Cualquier mensaje que contenga virus será inmediatamente revisado o borrado del servidor.

Sanciones aplicables

1. El Departamento de Recursos Humanos, de oficio o a solicitud de las Jefaturas respectivas recomendará al Alcalde la sanción aplicable, entre las cuales están las siguientes: amonestación verbal, en una primera falta detectada, escrita, en caso de reiterarse la misma, y el Procedimiento Administrativo Disciplinario de acuerdo al Libro Segundo de la Ley General de Administración Pública y el artículo 81 inciso H e I del Código de Trabajo de darse una tercera falta.

2. Podrá recomendar también, que la Alcaldía ordene la suspensión del servicio de Internet, en la computadora de uso del presunto responsable de la falta correspondiente, como medida cautelar mientras se determina su responsabilidad o no en ella, dejándole habilitado, en este último caso, el correo out look para que pueda seguir enviando correos electrónicos de trabajo.

3. Asimismo se establece que la acción de suspensión no impide que se establezcan procedimientos administrativos, para aplicar sanciones disciplinarias por el uso indebido del equipo electrónico y las telecomunicaciones en la institución.

A manera de ejemplo se incluyen algunas normas que regulan el uso adecuado de los servicios tecnológicos que dispone la institución:

a) Capítulo IX de Prohibiciones, Artículo 23 del Reglamento Autónomo de Servicio y Organización de la Dirección General de Servicio Civil, Decreto N° 25813-MP, publicado en La Gaceta N° 36 del jueves 20 de febrero de 1997,

"...inciso s) La exhibición de material pornográfico en cualquier lugar de la institución utilizando el equipo de cómputo y/o los servicios de comunicación de la institución, asimismo el uso de equipo electrónico del Estado para observar o reproducir pornografía. El incurrir en el incumplimiento de esta normativa. Acarrea una falta grave que será sancionada según las regulaciones vigentes....."

b) Ley 8131 de Administración Financiera de la República Presupuestos Públicos:

Artículo 111 Delito Informático. " Cometerán delito informático, sancionando con prisión de 1 a 3 años, los funcionarios públicos o particulares que realicen, contra los sistemas informáticos de la Administración Financiera y de Proveeduría, alguna de las siguientes acciones:

-Apoderarse, copiar, destruir, alterar, transferir o mantener en su poder, sin el debido permiso de la autoridad competente, información, programas o bases de datos de uso restringido

-Causar daño, dolosamente, a los componentes lógicos o físicos de los aparatos, las máquinas o los accesorios que apoyan el funcionamiento de los sistemas informáticos.

-Facilitar a terceras personas el uso del código personal y la clave de acceso asignados para acceder a los sistemas.

-Utilizar las facilidades del sistema para beneficio propio o de terceros..."

c) Artículo 72, inciso d) del Código de Trabajo:

"Queda absolutamente prohibido a los trabajadores:

d) Usar los útiles y herramientas suministrados por el patrono, para objeto distinto de aquel a que están normalmente destinados.

Rige a partir del 27 de marzo de 2014. Curridabat 23 de abril de 2014. Allan Sevilla Mora, Secretario.