Manual de Procedimiento y Directriz para uso de internet y correo electrónico de la Municipalidad de Curridabat

MUNICIPALIDAD DE CURRIDABAT

MANUAL DE PROCEDIMIENTOS Y DIRERCTRIZ PARA

USO DE INTERNET Y CORREO ELECTRÓNICO

Por acuerdo N° 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 N° 204-2014, el Concejo de Curridabat, en uso de su potestad normativa dispuso la aprobación del Manual de procedimientos para el marco de seguridad informática MC-SOP-011, versión 1.2 así corno el documento MC-PSIN-0004: Directriz para el uso del servicio de correo electrónico y acceso a Internet. El documento completo se puede ver en la siguiente dirección:

http://www.curridabat.go.cr/reglamentos/MANUAL%20DE%20PROCEDIMIENTOS%20INTER NET.pdf,

http://www.curridabat.go.cr/reglamentos/

El documento se encuentra vigente desde el 27 de marzo de 2014.

(Nota de Sinalevi: La presente norma fue proporcionada por la Municipalidad de Curridabat y se transcribe a continuación:)

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 2º, capítulo 6º, 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

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

Ficha articulo

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.

Ficha articulo

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.

Ficha articulo

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 %,&,@,[],%

Curridabat, 23 abril de 2014.

Ficha articulo

Fecha de generación: 20/08/2020 11:26:56 a.m.

Ir al principio del documento