

**MUNICIPALIDAD DE SAN JOSE**

**ALCALDÍA MUNICIPAL**

**DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES**



**POLÍTICAS INSTITUCIONALES  
DE SEGURIDAD INFORMÁTICA  
DE LA MUNICIPALIDAD DE SAN JOSÉ**

**MARZO 2011**


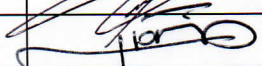


## CONTROL DE DOCUMENTO

### HISTORIAL DE VERSIONES

Versión	Autor	Fecha	Revisión
1.0	Lic. Freddy Sánchez Corrales, D.T.I.	19/01/2011	1
2.0	Lic. Freddy Sánchez Corrales, D.T.I.	16/03/2011	2

### CONTROL DE APROBACIÓN

	Responsable	Firma	Fecha
1	Lic. Carlos Garita Cabezas; Director a.i. TIC		18/03/2011
2	Ing. Johnny Araya Monge; Alcalde Municipal		22/03/2011





## **POLÍTICAS INSTITUCIONALES DE SEGURIDAD INFORMÁTICA**

### **1. INTRODUCCIÓN.**

Las políticas institucionales de seguridad informática de la Municipalidad de San José, surgen como un lineamiento organizacional para normar todas aquellas actividades de la institución en las cuales se requiera el acceso y uso a las tecnologías de información propiedad de la organización.

En especial, persiguen obtener el máximo rendimiento y aprovechamiento de estos recursos por medio del uso razonable y adecuado con base en el criterio que se trata de recursos que la institución pone a disposición de los funcionarios para facilitar y agilizar sus deberes como empleados municipales.

Así, el objetivo es concientizar a cada uno de sus miembros sobre la importancia, criticidad y sensibilidad de la información y de la necesidad de contar con reglas de acatamiento obligatorio para obtener, como se citó anteriormente, el mejor beneficio al contar con equipos que nos permiten hacer nuestro trabajo de mejor y más eficiente manera en pro de una mayor calidad en los productos que damos a la Municipalidad.

Por otro lado, es notoria la relevancia que ha tomado en los últimos tiempos la seguridad informática en las organizaciones, con base en la variabilidad de arquitecturas y plataformas computacionales existentes en la actualidad. Asimismo, la proliferación de posibilidades múltiples de interconexión y acceso a la información ha aumentado la cantidad de riesgos de usos y accesos no autorizados e inadecuados a los sistemas de información y datos propios de las instituciones, lo cual, en el caso particular de la Municipalidad de San José es de vital importancia resguardar con criterios razonables y mantener íntegros y congruentes para poder de esa manera utilizarlos en beneficios tanto de los usuarios internos como externos quienes requieren su uso y consulta constantes.

Así las cosas, la Dirección de Tecnologías de Información se ha dado a la tarea de desarrollar y establecer la presente normativa para orientar a los usuarios en el correcto uso de los recursos informáticos institucionales para obtener los mejores resultados por medio de su uso y así apoyar su gestión.



Asimismo, se pretende contar con una herramienta cuyo contenido contemple buenas prácticas para la gestión de la seguridad de la información en esta Municipalidad, de manera que contenga recomendaciones para la gestión de la seguridad de la información, considerando la Seguridad de la Información como la preservación de la confidencialidad, la integridad, la congruencia y la disponibilidad de la información.

Este documento contiene una serie de políticas que deberán ser acatadas por todos los funcionarios de la Municipalidad de San José quienes sean usuarios de las tecnologías de información de forma obligatoria y sin excepción. Dichas políticas se verán apoyadas en un conjunto de normas que brindan mayor detalle e instrumentalización de la forma de cumplir lo establecido en las políticas. Estas normas serán presentadas en el documento "Normas Generales de Seguridad Informática de la Municipalidad de San José", las cuales, a su vez, brindarán el respaldo correspondiente para la elaboración de procedimientos y manuales para el uso de los recursos y servicios informáticos institucionales y contribuyen con la productividad y eficiencia operativa.

La presente normativa de políticas institucionales de seguridad informática de la Municipalidad de San José toman como referencia lo establecido en:

- Las Normas ISO 27000, relativas a la Seguridad Informática.
- Las Normas Técnicas para la gestión y el control de las tecnologías de información y comunicaciones emitidas por la Contraloría General de la República.
- La Ley de Control Interno.
- La Ley de Administración Pública

De esta manera, consciente de la necesidad de crear normativas para el uso correcto de los sistemas, recursos informáticos y de la información en sí; la Dirección de Tecnologías de Información será la encargada de proponer las políticas y normativa necesarias para regular el uso de las tecnologías de información en la Municipalidad de San José.

En complemento con lo anterior y en procura del cumplimiento de las políticas institucionales de seguridad informática, la Dirección de Tecnologías de Información fungirá como una unidad asesora a la cual se pueden dirigir las consultas y procurará colaborar en la atención de las necesidades de seguridad informática. Asimismo, será la responsable de velar por la correcta aplicación de las políticas, así como la validez y el control de las políticas y normas de seguridad informática.



Finalmente, por su naturaleza y función, la Dirección de Tecnologías de Información es la única unidad institucional competente tanto organizacional como técnicamente que puede establecer lineamientos y normativa relacionada con todos los recursos de tecnologías de información que sean utilizados en la Municipalidad de San José, por lo cual tanto la presentación como la actualización de las políticas institucionales de seguridad informática y demás normas tendientes a la regulación y gestión de estas tecnologías serán hechas única y exclusivamente por esta Dirección, sin que ello implique una imposibilidad de consultar otras unidades o entes para obtener información adicional o asesoría con el fin de afinarlas y mejorarlas, de manera que aquellas se apoyen en las normas y procedimientos relacionados con el tema y que son de acatamiento obligatorio de todos los usuarios de tecnologías de información en la Municipalidad de San José y agentes externos que le brinden servicios y, por lo tanto, se acojan a esta normativa.

## **2. JUSTIFICACIÓN.**

Los recursos de tecnologías de información son activos de importancia vital en nuestra institución y en los cuales se han invertido considerables sumas de dinero para su obtención o actualización. Además, sin su debida protección y aprovechamiento nos podríamos quedar rápidamente rezagados con respecto a otras instituciones públicas. Por tal razón, la Dirección de Tecnologías de Información de la Municipalidad de San José tiene la obligación de establecer las medidas correspondientes con el fin de que sean utilizados y preservados de forma adecuada y razonable.

Esto implica la necesidad de tomar las acciones apropiadas para asegurar que dichos recursos estén, por un lado, menos expuestos a sus riesgos inherentes, tales como fraude, sabotaje, espionaje, extorsión, violación de la privacidad, intrusos, interrupción de servicio, accidentes, desastres naturales, etc.; y, por otra parte, que sean aprovechados en beneficios de su objetivo de adquisición por medio de buenas prácticas, de manera que se garantice la seguridad, integridad y buen uso de dichos recursos.

## **3. PROPÓSITO.**

El propósito de estas políticas es reducir al mínimo los incidentes negativos que se pudieran presentar en el uso de los recursos de tecnologías de información de la Municipalidad de San José, además de contribuir a elevar los niveles de la confiabilidad, seguridad, disponibilidad e integridad de los mismos.



#### **4. OBJETIVO GENERAL DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA.**

Establecer normativa, por medio de un conjunto de lineamientos, directrices y los instrumentos necesarios; que permita garantizar la seguridad en el ambiente informático, la información y demás recursos tecnológicos y asegurar la correcta utilización y aprovechamiento de los recursos de tecnologías de información de la Municipalidad de San José.

#### **5. OBJETIVOS ESPECÍFICOS DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA.**

- Normar el uso de las tecnologías de información en la Municipalidad de San José.
- Regular el cumplimiento de aspectos legales y técnicos en materia 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 los recursos informáticos 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.
- 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 las diferentes áreas de trabajo, utilización eficiente de los recursos de tecnologías de información.
- Servir de guía para el comportamiento laboral de los funcionarios de la Municipalidad de San José, en procura de minimizar los incidentes de seguridad internos, como hurto de información o vandalismo.

#### **6. ALCANCES.**

La presente normativa y toda aquella que de ésta se derive es de implementación y acatamiento obligatorios y es aplicable a todas las unidades organizacionales y a todos los funcionarios permanentes y temporales de la Municipalidad de San José, visitantes internos o externos, consultores y todas las personas quienes tengan acceso o hagan cualquier tipo de uso de los recursos informáticos de la Municipalidad de San José, por cualquier medio físico o lógico, tanto en el ámbito interno como externo de las instalaciones municipales sin excepción de algún tipo.



Aquellos funcionarios quienes incumplan las políticas de seguridad informática establecidas en este documento y cualquier normativa derivada de éstas, incurrirá en faltas que conllevarán a la institución, según la línea jerárquica correspondiente; a tomar las medidas respectivas por responsabilidad administrativa e incluso civil o penal, de conformidad con el régimen jurídico vigente.

## **7. ACTUALIZACIÓN.**

Por la naturaleza de esta normativa y la que de ella se derive, la Dirección de Tecnologías de Información revisará su contenido con el fin de actualizar y/o agregar las políticas que se utilizan para orientar el uso adecuado de las tecnologías de información en la Municipalidad de San José, según las necesidades y el entorno tecnológico a la institución lo ameriten.

## **8. LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA, COMO BASE DE LA ADMINISTRACIÓN DE LA SEGURIDAD INTEGRAL EN LA MUNICIPALIDAD DE SAN JOSÉ.**

Las políticas de seguridad informática, conforman el conjunto de lineamientos que los funcionarios de la institución deben seguir para poder así, asegurar la confiabilidad de los sistemas y de la información propiedad de la Municipalidad de San José. Las políticas de seguridad informática, son parte del engranaje del sistema de seguridad que la Municipalidad de San José posee para salvaguardar sus activos y su aplicación es obligatoria, en el uso y acceso a los sistemas de información, componentes de hardware, componentes de comunicaciones, equipos especializados que interactúan con componentes y aplicaciones informáticas, así como bases de datos y redes de telefonía y datos.

Las políticas de seguridad informática, constituyen un conjunto de compromisos compartidos, que le permiten a la institución, actuar proactivamente ante situaciones que comprometan la integridad de la información. Por tanto, deben constituir un proceso continuo y retroalimentado que observe la concientización, métodos de acceso a la información, monitoreo de cumplimiento y renovación, aceptación de las directrices y estrategia de implantación, que lleven a una formulación de directrices institucionales que logren aceptación general.

Las políticas por sí solas no constituyen una garantía para la seguridad de la información institucional, ellas deben responder a intereses y necesidades organizacionales, que lleven a un esfuerzo conjunto de sus actores por



administrar sus recursos y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la institución.

Este documento de políticas se verá apoyado por el documento “Normas Generales de Seguridad Informática de la Municipalidad de San José”, el cual contendrá un conjunto de reglas que amplían y dan apoyo al contenido de cada una de las políticas de seguridad y son de carácter más operativo.

## **9. BENEFICIOS DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA.**

Las políticas de seguridad, constituyen la base a partir de la cual la Municipalidad de San José diseña su sistema de seguridad, para garantizar que la inversión que se realice sea la adecuada, que los productos y las soluciones adquiridas cumplan con los objetivos de la institución y que 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.
- Fomento de la cultura organizacional en materia de seguridad informática.
- Minimización de la pérdida de la información y recursos informáticos.
- Proporciona la confianza necesaria a clientes y usuarios, demostrando que la seguridad es un factor que es importante dentro de la Municipalidad de San José y que ésta se aborda correctamente.

## **10. ASPECTOS GENERALES.**

Entre los aspectos a considerar para la implementación de las Políticas y Normas Generales de Seguridad Informática de la Municipalidad de San José tendientes a regular el uso de los recursos informáticos de la institución, se deberán considerar los siguientes aspectos de aplicación general obligatoria y que las fundamentan:

- Realizar actividades de control y seguimiento de la gestión de calidad en las tecnologías de información.
- Potenciar el desarrollo y el uso de las tecnologías de información y la especialización y crecimiento del recurso humano involucrado para su gestión.





- Incentivar y promover el mejoramiento continuo de las tecnologías de información mediante la investigación de nuevas tecnologías, el desarrollo de mejoras, el desarrollo y la capacitación permanente del recurso humano involucrado en este campo.
- Mejorar los recursos de tecnologías de información según las necesidades y posibilidades de la Municipalidad de San José y los requerimientos puntuales de los usuarios.
- Promover la realización de investigaciones, en el ámbito de las tecnologías de información.
- Realizar y revisar anualmente el Plan de Adquisiciones de Tecnologías de Información con el fin de actualizar oportuna y razonablemente las tecnologías de información de la Municipalidad de San José.
- Definir normas necesarias con la finalidad de fomentar la estandarización en los recursos de tecnologías de información.
- Los recursos de tecnologías de información provistos por la Municipalidad de San José son de su propiedad. Su utilización será dedicada única y exclusivamente para efectos laborales, de capacitación, de investigación, de administración y de atención al cliente.
- El uso de los recursos de tecnologías de información deberá estar acorde con el respeto a las leyes y normas nacionales e internacionales tales como los derechos de propiedad intelectual, la legislación laboral, control interno y el respeto a la dignidad y los derechos humanos.
- Destinar los recursos necesarios para la implementación de estas políticas y para asegurar su cumplimiento, de tal manera que dichas políticas formen parte integral de todas sus funciones y operaciones.
- Asegurar que las responsabilidades asignadas a todo el personal incluyan un control de calidad y una revisión del cumplimiento general de las políticas, estándares, normas y procedimientos establecidos por esta Dirección.

## **11. POLÍTICA DE CONCIENTIZACIÓN EN SEGURIDAD INFORMÁTICA.**

La Dirección de Tecnologías de Información realizará las acciones necesarias tendientes a comunicar y concientizar a todos los funcionarios de la Municipalidad de San José sobre su obligación de conocer y aplicar la normativa en materia de seguridad informática para lograr un cambio favorable en la cultura organizacional.

Todas las unidades organizacionales y los funcionarios de la Municipalidad de San José están en la obligación de atender las normas de cualquier índole que emane la Dirección de Tecnologías de Información relacionadas con el uso y gestión de recursos informáticos.

## **12. POLÍTICA SOBRE EL USO ACEPTABLE DE RECURSOS (UAR).**

La institución concede a los funcionarios diferentes recursos o servicios propiedad de la institución, para facilitarle la realización de las labores, los cuales deben recibir un trato adecuado por parte de los funcionarios, siempre resguardando que no se haga mal uso o abuso de los mismos, razón por la cual las siguientes Políticas se refieren al uso adecuado que deben recibir dichos recursos o servicios que la institución pone a disposición de los funcionarios. Toda área de trabajo y funcionario, deberán velar por el cumplimiento de las siguientes políticas, realizando las coordinaciones respectivas.

### **a. POLÍTICA PARA LA ADMINISTRACIÓN DEL ESPACIO FÍSICO DONDE SE UBIQUEN RECURSOS INFORMÁTICOS.**

Los equipos en los cuales se almacenan y procesan datos críticos que colaboran con el cumplimiento de los servicios informáticos de la institución, deben estar ubicados en un espacio especial que cumpla con condiciones básicas de seguridad para la protección de los datos que contienen y del equipo en sí. Dichas condiciones entre otras son: protección contra humedad y/o polvo, espacio accesible por los funcionarios encargados de los recursos, uso de cables de corriente alterna debidamente aterrizados, uso de aire acondicionado cuando así lo requieran los recursos o, al menos, contar con la ventilación suficiente para el correcto funcionamiento de los recursos asignados y que consista en un sitio en el cual se proteja físicamente el recurso ante la posibilidad de robos o daños físicos a estos recursos.

### **b. POLÍTICA PARA EL USO ADECUADO DE ESTACIONES DE TRABAJO.**

La Municipalidad de San José asigna a los funcionarios, cuando así se requiere, una estación de trabajo en apoyo al cumplimiento de sus labores. Estos equipos son parte del patrimonio institucional y por lo tanto, cada funcionario buscará 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.



**c. POLÍTICA PARA EL USO DE EQUIPOS PORTÁTILES.**

La institución asigna equipos tipo portátil tales como: laptops, tablet 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.

**d. POLÍTICA PARA EL USO DE EQUIPOS ESPECIALIZADOS CON COMPONENTES INFORMÁTICOS.**

La institución debe garantizar para la operación de los servicios, el uso adecuado de los equipos especializados por parte del personal calificado y que la información generada en estos sea administrada solo para efectos de los servicios que presta la institución.

**e. POLÍTICA PARA EL SOFTWARE INSTALADO USADO EN EQUIPOS DE LA MUNICIPALIDAD DE SAN JOSÉ.**

La Municipalidad de San José asigna a los funcionarios, cuando así se requiere, equipos informáticos en apoyo al cumplimiento de sus labores. Estos equipos son parte del patrimonio institucional y por lo tanto, cada funcionario buscará la mejor forma de utilizarlos, considerando solamente el software institucional debidamente licenciado o autorizado y aquellas aplicaciones o sistemas de información institucionales que son necesarios para el cumplimiento de sus labores únicamente.

Ningún equipo informático será configurado de manera distinta para el que fue destinado, salvo que sea requerido y autorizado con base en la Política de Excepciones contenida en este documento.

**f. POLÍTICA DE LA INFORMACIÓN PERMITIDA EN LOS EQUIPOS DE LA MUNICIPALIDAD DE SAN JOSÉ.**

La Municipalidad de San José asigna a los funcionarios, cuando así se requiere, equipos informáticos en apoyo al cumplimiento de sus labores. Estos equipos son parte del patrimonio institucional y por lo tanto, cada funcionario

buscará la mejor forma de utilizarlos, considerando solamente los datos y la información (contenida en directorios y archivos) necesarios para el cumplimiento de sus labores únicamente.

Ningún equipo informático podrá contener directorios, archivos, datos ni información distinta para el que fue destinado, salvo que sea requerido y autorizado con base en la Política de Excepciones contenida en este documento.

#### **g. POLÍTICA PARA EL USO DE DISPOSITIVOS DE ALMACENAMIENTO.**

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 de 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.

#### **h. POLÍTICA REALIZACIÓN DE RESPALDOS.**

La realización periódica de respaldos de la información generada en los sistemas, bases de datos, así como la información residente en los equipos de los funcionarios de la Municipalidad de San José, es de gran importancia para brindar continuidad de los servicios. Por lo tanto todas las unidades de la institución deben elaborar un plan de recuperación y respaldo de información que resida en los equipos (estaciones de trabajo) de los funcionarios de cada unidad y cada funcionario y unidad son responsables de la información almacenada en los equipos asignados a su custodia, de manera que los respaldos deberán realizarse periódicamente conforme las características de los equipos, las aplicaciones y los datos asociados.

El plan de recuperación y respaldo de la información debe contemplar la realización de pruebas continuas para asegurarse que los respaldos estén correctamente ejecutados y deben almacenarse en un lugar seguro y lejano de la fuente de información original.

#### **i. POLÍTICA PARA EL USO DE 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 de las estaciones de trabajo, entre las que podemos mencionar los quemadores de discos compactos y 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 otros equipos) 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.

Adicionalmente deben resguardarse las copias de la información que se reproduce en ellos garantizando que las mismas sean almacenadas de manera segura.

Cuando este tipo de unidades formen parte de un equipo especializado, solo podrán ser utilizadas para los fines propios de operación del equipo.

**j. POLÍTICA PARA EL USO ADECUADO DE LAS UNIDADES DE POTENCIA ININTERRUMPIDA.**

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 éste se corta. 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 y únicamente para los efectos que se han destinado.

**k. POLÍTICA PARA LA ADMINISTRACIÓN Y USO DE REPUESTOS EQUIPO DE CÓMPUTO.**

La sustitución de componentes de equipo de cómputo en las unidades de la Municipalidad de San José que estén dañados, es importante para la continuidad en la prestación oportuna de los servicios, por lo tanto debe contarse con los controles adecuados que permitan tener o adquirir repuestos actualizados y que los mismos estén disponibles cuando se necesiten y que realmente sean utilizados en beneficio de la institución.



Todas las unidades institucionales deberán recurrir y coordinar con el Departamento de Soporte Técnico de la Dirección de Tecnologías de Información para realizar sustituciones o instalaciones de dispositivos a los recursos informáticos institucionales y el coste de los repuestos será cargado al presupuesto de la unidad correspondiente.

De esta manera, solamente la Dirección de Tecnologías de Información está autorizada a hacer modificaciones, ya sean actualizaciones o sustitución de componentes dañados en los equipos institucionales.

Las indicaciones relacionadas con tipo de repuestos y cantidades a adquirir, se detallan en la norma relacionada con esta política.

### **13. POLÍTICA DE CONTROLES DE ACCESO RECURSOS INSTITUCIONALES (CAR).**

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"<sup>1</sup> o funcional, el cual pretende que cada funcionario únicamente tenga acceso a la información y recursos estrictamente necesarios para el desarrollo adecuado de su función.

Así las cosas, se establecen las siguientes Políticas que regulan el acceso a los diferentes recursos institucionales.

#### **a. POLÍTICA PARA EL USO ADECUADO DE LA RED DE DATOS INSTITUCIONAL.**

La Municipalidad de San José 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 funcionario puede acceder 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 ésta, estrictamente en cumplimiento de las labores institucionales, tomando en

---

<sup>1</sup> Principio de seguridad por el que, para que una persona pueda acceder a una determinada información clasificada, es necesario que ésta sea precisa para poder desarrollar su trabajo, no siendo suficiente su puesto o rango, según CNSS Instruction No. 4009. NATIONAL INFORMATION ASSURANCE (IA) GLOSSARY. Committee on National Security Systems. <http://www.cnss.gov/Assets/pdf/cnssi4009.pdf>



consideración la privacidad de otros usuarios y la no saturación de la red por uso indebido del ancho de banda, entre otros argumentos.

**b. POLÍTICA PARA EL CORRECTO USO DE CONTRASEÑAS DE PARTE DE LOS USUARIOS DE RED Y APLICACIONES.**

El uso de contraseñas robustas constituye la primera línea de defensa para el acceso a la información y a los recursos institucionales, razón por la cual el correcto uso de las contraseñas generadas para los usuarios de la red y aplicaciones de la Municipalidad de San José, es de vital importancia en la seguridad de la información institucional, por lo tanto deben cumplirse lineamientos básicos de seguridad que serán de acatamiento obligatorio por parte de todos los usuarios de la red y aplicaciones, dichos aspectos buscan que los usuarios utilicen contraseñas más "robustas" y a la vez más fáciles de recordar.

Es obligación y responsabilidad de cada funcionario conocer y recordar sus contraseñas con el fin de acceder a los recursos institucionales que requiere para la ejecución de sus labores.

**c. POLÍTICA 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 de San José, 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.

**d. POLÍTICA GESTIÓN DE CONTRASEÑAS DE ADMINISTRADOR DE LAS ESTACIONES DE TRABAJO PROPIEDAD DE LA MUNICIPALIDAD DE SAN JOSÉ.**

Con el fin de prevenir el acceso no autorizado a los datos de las estaciones de trabajo propiedad de la Municipalidad de San José, 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 acceder la información almacenada en los mismos.

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.

Ninguna cuenta de usuario institucional será configurada con privilegios de administrador en los sistemas o equipos, salvo que sea requerido y autorizado con base en la Política de Excepciones contenida en este documento.

#### **e. POLÍTICA PARA EL USO DE CORREO ELECTRÓNICO INSTITUCIONAL.**

El correo electrónico se concede a los funcionarios como una herramienta que colabora y apoya en la realización de las tareas y es el único medio electrónico oficial de comunicación institucional. Cada usuario debe darle un uso apropiado a este servicio estrictamente relacionado con las labores que desempeña en la institución, los usos para otros propósitos no son aceptables. El usuario deberá considerar las medidas de racionalidad y seguridad que garanticen que su trabajo se llevará a cabo de una manera eficiente y productiva.

Derivado del mal uso o abuso del correo electrónico, se podrá proceder a la suspensión o eliminación del servicio, dado que la Municipalidad de San José como proveedora del servicio tiene la autoridad para controlar y negar el acceso a cualquiera persona que no cumpla con las políticas.

La Municipalidad de San José, cuenta con herramientas automatizadas para monitorear y filtrar las actividades que al respecto del uso del correo electrónico realicen los usuarios, por ejemplo envío de archivos adjuntos potencialmente inseguros, o material de contenido obsceno.

En las revisiones del correo electrónico no se da intervención manual, por lo que se asegura a los usuarios que no hay ningún funcionario administrador de la Municipalidad de San José, leyendo o analizando el contenido de los correos para eliminarlos, dicho proceso se hace de manera completamente automática, mediante la configuración de reglas de filtrado en los sistemas de protección para el correo electrónico institucional.





**f. POLÍTICA PARA LA NAVEGACIÓN EN INTERNET, MEDIANTE EL SERVICIO BRINDADO POR LA MUNICIPALIDAD DE SAN JOSÉ.**

El uso de Internet se concede a los funcionarios como una herramienta que colabora y apoya en la realización de las tareas, por lo tanto cada usuario debe darle un uso apropiado a este servicio estrictamente relacionado con las labores que desempeña en la institución, cualquier uso para otros propósitos no es aceptable. El usuario deberá considerar las medidas de racionalidad y seguridad que garanticen que su trabajo se llevará a cabo de una manera eficiente y productiva.

La Municipalidad de San José, dependiendo del mal uso o abuso que le dé el usuario al servicio otorgado para la navegación en Internet, suspenderá o eliminará el servicio, en caso de comprobarse mal uso o abuso del mismo, según se define en la norma asociada con esta política.

La Municipalidad de San José, cuenta con herramientas automatizadas para monitorear y filtrar todas las actividades que respecto al uso de Internet realicen los usuarios y los informes y reportes que se generan con dichas herramientas podrán ser utilizadas como evidencia del mal uso o abuso del servicio<sup>2</sup> de navegación, según se define en la norma asociada con esta política.

**14. POLÍTICA DESARROLLO, MANTENIMIENTO Y ACTUALIZACIÓN DE APLICACIONES.**

El desarrollo de aplicaciones y la gestión de proyectos informáticos, sean estos internos o externos, deberán basarse en los lineamientos institucionales para el desarrollo y mantenimiento de sistemas de información, según lo defina la Dirección de Tecnologías de Información, con el propósito de gestionar de forma óptima y homogénea las actividades que conlleva este proceso; ello de forma tal que fomente un clima de estímulo al desarrollo de iniciativas surgidas en una unidad o en grupos de unidades de la institución que sean de interés local o con mayor razón cuando se trata de un sólido interés institucional y que además, la más consolidada experiencia desde los usuarios internos, también contribuya a generar lineamientos institucionales.

La implementación de políticas y estándares para el desarrollo y mantenimiento de sistemas, además de homologar la forma de trabajo, fomentará el avance y sobre todo la innovación tecnológica, aprovechando al máximo los recursos

---

<sup>2</sup> Abuso del servicio. Ver definición en el glosario.



actuales y futuros, procurando además la integración de las tecnologías y evitando su obsolescencia prematura; lo anterior siempre con base en una fluida, cooperativa y constructiva retroalimentación de las diferentes unidades.

El desarrollo o adquisición de sistemas, equipos o cualquier recurso de tecnologías de información es de la competencia única y exclusiva de la Dirección de Tecnologías de Información, por lo cual toda necesidad deberá ser coordinada con ésta con el fin de mantener los estándares y normativa institucional atinente.

Para el caso de aplicaciones o sistemas operativos locales, la unidad correspondiente deberá solicitar la asesoría de la Dirección de Tecnologías de Información con el fin de alinear en la medida de lo posible las necesidades con el portafolio de aplicaciones y de sistemas institucionales.

**a. POLÍTICA UTILIZACIÓN DE MÓDULOS INTEGRADOS DE SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN DE LA MUNICIPALIDAD DE SAN JOSÉ.**

Un Módulo Integrado de Seguridad, es un sistema que brinda servicios de seguridad a las aplicaciones desarrolladas, el mismo administra lo relacionado con cuentas de usuarios, perfiles, permisos en los diferentes módulos y componentes de aplicaciones, de modo que los nuevos desarrollos realizados en la institución o contratados, no tendrán que desarrollar individualmente un módulo de seguridad, sino que podrán utilizar los servicios del módulo, lo que si deben considerar los nuevos desarrollos de aplicaciones es la conectividad con el Módulo Integrado de Seguridad.

La utilización generalizada del Módulo Integrado de Seguridad, en las aplicaciones desarrolladas en la Municipalidad de San José, así como las contratadas externamente, es de suma importancia para salvaguardar la información, la continuidad del negocio y la no generación de problemas por pérdida de imagen. Por lo tanto el Módulo Integrado de Seguridad, deberá ser utilizado de manera obligatoria en todos los desarrollos realizados en la institución así como los contratados, considerando que el mismo se instala y funciona en forma independiente de la aplicación de usuario, manteniendo una estrecha relación con la aplicación de usuario final, al compartir las bases de datos que administran la seguridad.



## **b. POLÍTICA PARA LA CONFIDENCIALIDAD DE LA INFORMACIÓN INSTITUCIONAL Y TRATO CON TERCEROS.**

Cada funcionario contratado por la institución, permanente o temporal, tiene acceso a información institucional en diferentes formatos (escrita, digital o verbal) para cumplir con las tareas propias de su cargo. Ejemplos de este tipo de información son las notas, circulares, minutas, acuerdos, bases de datos, reportes, consultas a los sistemas de información, equipos que interactúan con componentes y aplicaciones informáticas, entre otros.

Toda la información confidencial<sup>3</sup> 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.

## **15. POLÍTICA DESECHO DE EQUIPO DE CÓMPUTO.**

Todas las unidades de la Municipalidad de San José deben velar porque el desecho del equipo de cómputo y componentes se realice periódicamente y con base en la normativa vigente, lo anterior con el fin de mantener los espacios físicos despejados.

Para lo anterior, deberán coordinar con el Departamento de Soporte Técnico de la Dirección de Tecnologías de Información con el fin de mantener actualizado el registro correspondiente de recursos informáticos de la institución.

---

<sup>3</sup> Información confidencial. Ver definición en el glosario.



## **16. POLÍTICA PARA LA ELABORACIÓN DE PLANES DE CONTINUIDAD DE LA GESTIÓN.**

Todas las unidades de la institución que utilizan servicios informáticos, deberán elaborar sus respectivos Planes de Continuidad de la Gestión y de procesos alternos a las tecnologías de información. Para ello todas las unidades deberán coordinar con la Dirección de Tecnologías de Información, la cual brindará la asesoría y guía respectiva.

Los Planes de Continuidad de la Gestión, deben mantenerse en vigencia y transformarse en una parte integral del resto de los procesos de administración y gestión.

La administración de la continuidad de la gestión debe incluir controles, procedimientos, asignación de responsable, pruebas, destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables. Adicionalmente como los planes de continuidad de la gestión pueden fallar debido a suposiciones incorrectas, negligencias o cambios en el equipamiento o el personal, debe considerarse dentro de su administración la realización de pruebas periódicas para garantizar que los mismos estén actualizados y son eficaces. Las pruebas también deben garantizar que todos los miembros del equipo de recuperación y demás personal relevante estén al corriente de los planes.

## **17. POLÍTICA DE EXCEPCIONES.**

Existirán casos aislados para los cuales no aplica una política específica, debido a que estas no pueden ser creadas e impuestas en un 100% para todas las actividades de la institución. En aquellas circunstancias en que las necesidades institucionales justifiquen la ejecución de acciones, que se encuentren en conflicto con las políticas y estándares de la institución, se provee el siguiente mecanismo de excepción.

Cualquier funcionario que debido a las necesidades institucionales detecte que debe aplicarse una excepción a una determinada política, deberá informarla por escrito a la Alcaldía Municipal y a la Dirección de Tecnologías de Información, las cuales analizarán el caso y determinarán en conjunto la validez o no de la excepción, basándose en un análisis de riesgos. Si la excepción es válida, se comunicará por escrito indicando el período válido de la excepción acorde con el riesgo asociado. Una vez pasado el período de excepción la Dirección de Tecnologías de Información valorará si continúa siendo una excepción, caso en el cual deberá ser aprobada y evaluada nuevamente.

## 18. GLOSARIO.

- **Abuso del servicio.** La institución brinda diferentes servicios a los usuarios de las tecnologías de información, como uso de Internet, red, correo electrónico, el abuso de estos servicios depende de la naturaleza de cada cual, sin embargo pueden ser abusos los siguientes: Invertir mucho tiempo laboral navegando en páginas que no tienen que ver con trabajo (entretenimiento, ocio u otro), lo que incide directamente en el rendimiento del funcionario, acceso a páginas prohibidas, envío de cadenas de correo electrónico, envío de correos obscenos, el uso del correo para fines lucrativos personales, entre otros. Los usos prohibidos o permitidos están descritos en las Normas Institucionales de seguridad Informática.
- **Acceso.** Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.
- **Activo tangible.** Se consideran activos tangibles todos los bienes de naturaleza material susceptibles de ser percibidos por los sentidos, tales como: materias primas y stocks, el mobiliario, las maquinarias, los terrenos, el dinero.
- **Activo intangible.** Se consideran activos intangibles aquellos bienes de naturaleza no material tales como: el conocimiento del saber hacer, nuestras relaciones con los clientes, nuestros procesos operativos, el software, las bases de datos, las capacidades, habilidades y motivaciones de los empleados.
- **Administrador del equipo.** Usuario que administra un equipo. El administrador del equipo puede realizar cambios en todo el sistema, lo que incluye instalar programas y tener acceso a todos los archivos del equipo, y puede crear, cambiar y eliminar las cuentas de los demás usuarios. Persona responsable de configurar y administrar controladores de dominio o equipos locales, y sus cuentas de usuario y de grupo correspondientes, asignar contraseñas y permisos, y ayudar a los usuarios a solucionar problemas de red.
- **Administrador de Bases de Datos (DBA).** El administrador de base de datos (DBA) es la persona responsable de los aspectos ambientales de una base de datos. En general esto incluye: Recuperabilidad - Crear y probar respaldos, Integridad - Verificar ó ayudar a la verificación en la integridad de datos, Seguridad - Definir y/o implementar controles de acceso a los datos, Disponibilidad - Asegurarse del mayor tiempo de encendido, Desempeño Asegurarse del máximo desempeño incluso con las limitaciones, Desarrollo y soporte a pruebas - Ayudar a los programadores e ingenieros a utilizar eficientemente la base de datos.
- **Amenaza.** Riesgo no materializado que pueda interferir con el funcionamiento adecuado de un recurso informático o causar la difusión no autorizada de información. Ejemplo: fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

- **Ancho de banda.** Para señales analógicas, el ancho de banda es la anchura, medida en hercios, del rango de frecuencias en el que se concentra la mayor parte de la potencia de la señal. Puede ser calculado a partir de una señal temporal mediante el análisis de Fourier. También son llamadas frecuencias efectivas las pertenecientes a este rango. Ancho de banda digital a la cantidad de datos que se pueden transmitir en una unidad de tiempo. En comunicaciones analógicas, la diferencia entre la frecuencia más alta y la más baja en un intervalo determinado. Por ejemplo, una línea telefónica analógica admite un ancho de banda de 3.000 hercios (Hz), que es la diferencia entre la menor frecuencia (300 Hz) y la mayor frecuencia (3.300 Hz) que puede transportar. En comunicaciones digitales, el ancho de banda se expresa en bits por segundo (bps).
- **Antivirus.** Programas especializados en la detección y, si es posible, en la destrucción de virus informáticos. Dada la velocidad con que aparecen nuevos y más sofisticados de estos programas, el mayor problema es la actualización continua, teniendo en cuenta los rendimientos conseguidos en cuanto a la detección de virus desconocidos.
- **Aplicación.** En informática, las aplicaciones son los programas con los cuales el usuario final interactúa a través de una interfaz y que realizan tareas útiles para éste. Conjunto completo y auto contenido de instrucciones que se utilizan para realizar una determinada tarea, como procesamiento de texto, contabilidad o administración de datos.
- **Ataque.** Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.
- **Base de Datos.** Conjunto de ficheros dedicados a guardar información relacionada entre sí, con referencias entre ellos de manera que se complementen con el principio de no duplicidad de datos y que, además, están almacenados con criterios independientes de los programas que los utilizan.
- **CD o disco compacto.** Dispositivo óptico para el almacenamiento de datos, voz o vídeo. Pueden ser de lectura y escritura o únicamente de lectura.
- **Cinta magnética.** Dispositivo magnético secuencial para el almacenamiento masivo de información. Solo permite el almacenamiento de datos.
- **Centro de cómputo.** Salas de cómputo y/o salas de procesamiento de información que cuenten con equipamiento de cómputo.
- **Confidencialidad.** Característica de la información y los datos, que garantiza que los mismos solo podrán ser acesados por personal autorizado para su lectura y/o modificación. Ver definición de información confidencial.



- **Contraseña.** Palabra de paso compuesta por la combinación de caracteres alfabéticos, numéricos y especiales; la cuál es requerida para tener acceso a los sistemas de información, componentes de hardware, bases de datos y otros componentes electrónicos.
- **Contraseñas robustas.** Palabras de paso confeccionadas tomando en cuenta reglas de seguridad que impiden que la composición de las mismas, sea fácil de deducir por medios manuales o automatizados. Las contraseñas robustas no se corresponden con palabras o frases de uso común en los idiomas conocidos.
- **Correo electrónico.** Herramienta informática que permite el trasiego de mensajes entre usuarios de computadoras. Permite además la incorporación de archivos de documentos, imágenes y voz.
- **Datos.** Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), video (secuencia de tramas), etc.
- **DBA.** Administrador de las bases de datos de los Sistema de Información municipales.
- **Dependencia.** Corresponde a toda unidad funcionar organizativa de la Municipalidad de San José, por ejemplo: Gerencias, Direcciones, Departamentos, Secciones y Unidades.
- **Delito.** Conducta que se realiza por una persona contraria al ordenamiento jurídico y que merece la imposición de una pena. En términos generales, se trata de un comportamiento desviado que se considera grave dentro de un sistema social y que es calificado como tal por órganos legislativos con competencia para ello.
- **Directorio Activo.** El Directorio Activo es un servicio de red utilizado por Microsoft Windows que almacena información acerca de los recursos existentes en la red y controla el acceso de los usuarios y las aplicaciones a dichos recursos. De esta forma, se convierte en un medio de organizar, administrar y controlar centralizada mente el acceso a los recursos de la red.
- **Disponibilidad.** La disponibilidad se refiere a un nivel de servicio proporcionado por aplicaciones, servicios o sistemas. Los sistemas de alta disponibilidad tienen un tiempo de inactividad mínimo, ya sea previsto o imprevisto. La disponibilidad se suele expresar como el porcentaje del tiempo que un servicio o un sistema está disponible; por ejemplo, el 99,9 por ciento para un servicio que no está disponible durante 8,76 horas al año (un año consta de 8.760).
- **Discos.** Es un dispositivo de almacenamiento primario para computadoras al que se accede directamente para guardar o recuperar documentos. Pueden ser magnéticos (discos rígidos, flexibles) u ópticos (CD-ROM).
- **Disco Duro.** Dispositivo encargado de almacenar información de forma permanente en una computadora. Disco de metal cubierto con una superficie de grabación magnética. Haciendo una analogía con los discos

musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y regrabados como una cinta de audio.

- **DVD.** Unidad de almacenamiento de datos. De aspecto similar a un CD-ROM, su capacidad es varias veces superior a éste (4,7 GB). Para leerlos, es necesario contar con una lectora de DVD. Pueden utilizarse como medio para almacenar y ver películas o guardar en ellos gran cantidad de información para ser leída en una PC.
- **Equipos especializados.** Equipos dedicados a actividades especiales o cuya función es limitada a una actividad en particular y pueden establecer comunicación o conectividad con sistemas de información para la recolección y almacenamiento de datos para procesos específicos.
- **Estación de trabajo.** PC por sus siglas en inglés Personal Computer, una estación de trabajo (en inglés Workstation) es un ordenador que facilita a los usuarios el acceso a los servidores y periféricos de la red. A diferencia de un ordenador aislado, tiene una tarjeta de red y está físicamente conectada por medio de cables u otros medios no guiados con los servidores.
- **Hacker.** Persona que esta totalmente enfrascada en la tecnología informática o en la programación de equipos informáticos o a quien le gusta examinar el código de los sistemas operativos y de otros programas para ver cómo funcionan. Una persona, más comúnmente considerada un cracker, que utiliza su experiencia informática con fines ilícitos, como, por ejemplo, obteniendo acceso a sistemas informáticos sin permiso y alterando los programas y los datos.
- **Hardware.** Son todos los componentes y dispositivos físicos y tangibles que forman una computadora como la CPU o la placa base.
- **Internet.** Conjunto de redes de ordenadores creada a partir de redes de menos tamaño, cuyo origen reside en la cooperación de dos universidades estadounidenses. Es la red global compuesta de redes de área local (LAN) y de redes de área extensa (WAN) que utiliza TCP/IP para proporcionar comunicaciones de ámbito mundial a hogares, negocios, escuelas y gobiernos.
- **Integridad.** Se refiere a las medidas de salvaguarda que se incluyen en un sistema de información para evitar la pérdida accidental de los datos.
- **Incidente.** Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido.
- **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 y pacientes, tecnología, diseño y técnicas o cualquier información relacionada con la prestación de servicios. La información confidencial, cuenta con las siguientes excepciones:

- Sea de dominio público por publicación u otros medios, excepto por omisión o acto no autorizado por parte de la Municipalidad de San José.
- Sea obtenida legalmente por la Municipalidad de San José de un tercero independiente de la entidad, quien en el conocimiento de la Municipalidad de San José, no tiene ninguna restricción u obligación de confidencialidad con la entidad.
- Sea ordenada y requerida por autoridades judiciales, gubernamentales o regulatorias.
- **Integridad.** Se refiere a la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.
- **Llave maya, pendrive o memoria USB (de Universal Serial Bus, en inglés pendrive o USB flash drive).** Dispositivo de almacenamiento masivo que facilita la copia y el traslado de datos (data traveler). Se conecta al puerto USB de la computadora y tiene la característica de ser plug and play (conecte y use), por lo tanto no requiere de software adicional para su configuración ya que son reconocidas por el sistema operativo, a excepción del sistema operativo Windows 98/SE. Estas memorias son resistentes a los rasguños y al polvo que han afectado a las formas previas de almacenamiento portátil, como los CD y los disquetes, las hay de diferentes capacidades de almacenamiento y su uso se ha vuelto muy popular.
- **Metodologías de programación.** Distintos sistemas de desarrollos de programas de manera que estudie optimizar al máximo la forma de escribir y de interpretar el ordenador los mismos. Son clásicos Bernier o Jackson con metodologías modulares y/o estructuradas, completamente vigentes y base de la mas extendida en estos momentos que es la Programación Orientada a Objetos.
- **Planes de Continuidad de la Gestión.** Se elaboran con el fin de reducir la discontinuidad de los servicios que pueda ser ocasionada por debilidades o fallas de seguridad que pueden materializarse luego de desastres naturales, accidentes, fallas en los equipos y acciones deliberadas como vandalismo. La elaboración de los planes busca principalmente que la prestación de los servicios o procesos sean reestablecidos dentro de los plazos requeridos.
- **Periférico.** Cualquier componente físico externo al ordenador, o a la CPU, (dependiendo a que se refiera el concepto) ya sea pantallas, impresoras, teclados o cualquier otro. Con carácter general suelen diferenciarse en periféricos o dispositivos de entrada, es decir, los que envían datos al ordenador, bien a través de la acción del usuario, como puede ser el teclado, o bien de forma automática, dentro de sistemas de robótica, por ejemplo; en periféricos o dispositivos de salida, que es cuando el ordenador proporciona el resultado de sus operaciones,



como en el caso de las impresoras; o periféricos de entrada-salida, que pueden cumplir ambas funciones, como una pantalla táctil, un modem, etc.

- **Privacidad.** Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidas o transmitidas a otros.
- **Recurso informático.** Cualquier componente físico o lógico de un sistema de información.
- **Recursos de Tecnología de Información.** Todos aquellos recursos informáticos disponibles al Usuario que son propiedad de la Municipalidad de San José o que están licenciados a su nombre. Entre ellos se encuentran las licencias de uso de software, los sistemas automatizados, las computadoras, los servidores, las redes de transmisión de datos y sus medios de acceso, etc.
- **Red.** Equipos de cómputo, sistemas de información y otros recursos interconectados de manera que pueden comunicarse entre sí.
- **Respaldos.** Hacer una copia de seguridad, copia de respaldo o simplemente respaldo, consiste en guardar en un medio extraíble (para poder guardarlo en lugar seguro) la información sensible referida a un sistema. Esta se puede realizar tanto en ordenadores personales como en servidores. Este medio puede ser un disco duro externo, un CO-ROM grabable, cintas de datos (OAT), dispositivos USB u otros.
- **Responsabilidad.** Cargo u obligación moral de responder por un posible error en una cosa o asunto determinado.
- **Riesgo.** Es una pérdida o daño futuro potencial que puede seguir por alguna acción presente, como por ejemplo: 1) Acceso y uso no autorizado 2) Daño o pérdida de los recursos, por algún desastre natural, error humano, fallo en los sistemas, o acción maliciosa y etc. Combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC Guía 73:2002)
- **Seguridad.** Medidas tomadas para reducir al máximo cualquier tipo de riesgo.
- **Seguridad informática.** Consiste en asegurar que los recursos informáticos (software y hardware) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización. Es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios. Técnicamente es imposible lograr un sistema informático ciento por ciento seguro, pero buenas medidas de seguridad evitan daños y problemas que pueden ocasionar intrusos. Existen dos tipos de seguridad con respecto a la naturaleza de la amenaza:
  - **Seguridad lógica:** aplicaciones para seguridad, técnicas, etc.
  - **Seguridad física:** mantenimiento eléctrico, antiincendio, humedad, etc.



- **Sistema de información.** Conjunto de procedimientos manuales y/o automatizados que están orientados a proporcionar información para la toma de decisiones.
- **Software.** Es el equipamiento lógico e intangible como los programas y datos que almacena la computadora.
- **Stock.** es una voz inglesa que se usa en español con el sentido general de reserva de alguna cosa disponible para un uso futuro. Stock de mercancías: Existencias, reservas.
- **USB.** Siglas en inglés de Universal Serial Bus (bus serial universal). Corresponde a conectores físicos de los computadores y otros dispositivos informáticos en los cuales se persigue la facilidad de conexión y uso inmediato de los dispositivos que se conectan por medio de este conector al equipo. De igual manera se considera la facilidad que los periféricos pueden conectarse y desconectarse con el equipo en funcionamiento, configurándose de forma automática.
- **Usuario:** se refiere a cualquier persona física contratada por la Municipalidad de San José, que haya sido autorizada para hacer uso de los recursos tecnológicos de información institucionales.
- **Virus.** Un virus es un programa informático que se ejecuta en el ordenador sin previo aviso y que puede corromper el resto de los programas, archivos, el sistema operativo e inclusive el hardware del ordenador. Los virus se transmiten, normalmente, a través de medios de almacenamiento extraíbles o de los archivos enviados a través de Internet, especialmente durante el intercambio de documentos entre usuarios.
- **Vulnerabilidad.** En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.