MUNICIPALIDAD DE BAGACES

Unidad de Tecnologías de Información y Comunicaciones(TIC)

Manual Institucional de Políticas de Seguridad en Tecnologías de Información

Autor:	Ing. Roy A. López Salas
Fecha de Creación:	Enero 2010

Contenido

Introducción

Las tecnologías de información constituyen hoy día uno de los cimientos más importantes sobre los cuales se cierne la modernización de una empresa, coadyuvando significativamente a su mejoramiento continuo y su competitividad. Sin embargo, todo proceso tiene un inicio relativamente corto y que pueden identificarse dentro del llamado modelo de madurez de la capacidad o CMM (Capability Maturity Model, por sus siglas en inglés) . Para todo proceso debe existir una normativa que permita su gestión, control y evolución.

Este manual pretende establecer ciertas políticas de seguridad en Tecnologías de Información de la MUNICIPALIDAD DE BAGACES. Estas políticas son de aplicación específica a procesos internos de la Unidad o generales a toda la Institución.

Es importante recalcar que:

- ✧ Circunscribe políticas de seguridad y no la implementación de los procedimientos requeridos para su puesta en marcha.
- ✧ El proceso de readecuación requiere de revisiones periódicas orientadas a un mejoramiento continuo.

Consideraciones generales

A. El objetivo de la seguridad de la información es preservar las características de confiabilidad, integridad, confidencialidad, disponibilidad y cumplimiento de la información que utiliza, con el fin de respaldar sus procesos de misión crítica, como medio para asegurar la continuidad de las operaciones.
B. El personal de la MUNICIPALIDAD DE BAGACES está comprometido con la seguridad de la información que recibe, procesa, genera y almacena en su gestión.
C. Cumplir con las normas de seguridad establecidas es obligatorio para el funcionario público, constituyendo una falta que se puede asociar con eventuales sanciones laborales, las cuales deberán ser normalizadas por las instancias institucionales correspondientes.
D. La Administración General se compromete a apoyar la seguridad de la información, mediante la aprobación, promulgación, mantenimiento y divulgación de los manuales de seguridad que El Departamento de TIC de la MUNICIPALIDAD DE BAGACES desarrolle.

1. Políticas generales para los usuarios

1.1. Todos los usuarios que acceden recursos informáticos de la Red de la MUNICIPALIDAD DE BAGACES, requieren de una intransferible identidad, normalmente compuesta por un nombre de usuario (*username*) y una contraseña secreta (*password*).

1.2. El usuario es el responsable de todas las acciones que se realicen con la identidad asignada.

1.3. El usuario es responsable de cambiar su contraseña, según la periodicidad implementada en los sistemas, considerando no utilizar los ya usados anteriormente y buscando literales de fácil rememoración y difíciles de inferenciar por otros usuarios.

1.4. Será responsabilidad de cada encargado de área, unidad o sección solicitar al departamento de TIC de la MUNICIPALIDAD DE BAGACES, la creación, suspensión y eliminación de los privilegios sobre el uso de las tecnologías de información para los usuarios de su área.

1.5. El usuario es el responsable del uso de los dispositivos de tecnologías de información que le han sido asignados.

1.6. Aquellos equipos o sistemas que representen un riesgo inminente al funcionamiento de las tecnologías de información de la MUNICIPALIDAD DE BAGACES, podrán ser desconectados por el departamento de TIC, sin previa comunicación al usuario. En esto se destacan la desconexión de dispositivos de red, tales como enrutadores o switches, por razones de seguridad y que no medie daño alguno a los datos de sistemas o de usuario.

1.7. El usuario es el responsable del mantenimiento y custodia de la información que mantiene en su estación de trabajo. El Departamento de TIC de la MUNICIPALIDAD

DE BAGACES solo será responsable de los datos que el usuario almacene en la carpeta de red asignada para tales efectos.

1.8. Toda información almacenada localmente en las estaciones de trabajo, debe ser respaldada por los mismos usuarios mediante unidades externas (discos duros externos) o DVD regrabables.

1.9. Toda actividad o servicio que involucre el uso de recursos informáticos, independientemente del origen de estos, deberá ser aprobada por la jefatura de El Departamento de TIC de la MUNICIPALIDAD DE BAGACES.

1.10. En caso de solicitar soporte técnico, el usuario debe completar una formula de solicitud. VER INSTRUCTIVO PARA COMPLETAR SOLICITUD DE SOPORTE TECNICO.

2. Políticas sobre el uso de las contraseñas (*Passwords*)

2.1. Los usuarios tienen la responsabilidad de resguardar las contraseñas confidenciales para el acceso a los recursos informáticos de la MUNICIPALIDAD DE BAGACES.

2.2. Estas contraseñas deben construirse de manera que sean difíciles de suponer o adivinar por otros usuarios; deben expirar periódicamente y poseer una longitud mínima. Se sugiere seguir las recomendaciones para el uso de contraseñas que se indican en los anexos 1 y 2, los cuales forman parte integral de este documento.

2.3. El Departamento de TIC deberá eliminar todos los usuarios que vengan instalados inicialmente (*en forma default*) en las aplicaciones computacionales.

2.4. El Departamento de TIC deberá implementar los procedimientos para la asignación, mantenimiento y revocación de estas contraseñas.

2.5. Cuando aplique, El Departamento de TIC asignará un responsable de los archivos de contraseñas existentes bajo su custodia y mantendrá un registro de todos los eventos que los afecten.

2.6. Mediante mecanismos automatizados se exigirá el cambio de la contraseña a nivel de usuario (Ej. correo, Web, Windows), al menos cada tres meses. En los casos cuando ello no sea posible, será responsabilidad del usuario realizar el cambio (Ej. BIOS -Basic Input Output System-, protector de pantalla). En caso de que el usuario desee asignar un password a nivel de BIOS deberá contar con previa autorización de El Departamento de TIC de la MUNICIPALIDAD DE BAGACES, quien procederá conjuntamente a implementar dicha contraseña.

2.7. Las contraseñas de los servidores institucionales serán registrados por el departamento de TIC en sobres identificados y sellados, que se trasladarán a la tesorería del Área Financiera y una copia a la bóveda del Banco de Costa Rica o Banco Nacional, para su custodia. En casos excepcionales y autorizados por el jefe de El Departamento de TIC o por el superior inmediato, se podrá acceder a estas contraseñas, con un procedimiento que deberá quedar documentado.

2.8. Los usuarios que tengan información o aplicaciones locales en el computador asignado y que puedan ser utilizadas por terceras personas, deberán mantener cualquier tipo de contraseña de acceso a estos recursos, en un sobre bajo la custodia del encargado de la unidad. En casos cuando se requiera acceder a la información o sistemas locales de un equipo y no se encuentre el usuario responsable, la jefatura podrá acceder a las contraseñas. El procedimiento deberá quedar documentado.

2.9. Cuando se requiera una palabra clave para acceder un sistema de información y no se encuentre el responsable de la cuenta, El Departamento de TIC podrá asignar una cuenta adicional (palabra clave y contraseña) para uso temporal de alguna persona previamente asignada y autorizada por la jefatura que corresponda. Será responsabilidad de la jefatura notificar el Departamento de TIC de MUNICIPALIDAD DE BAGACES en el momento cuando ya no se requiera más esa cuenta asignada, para que se proceda a removerla de las bases de datos de usuarios.

2.10. El Departamento de TIC realizará procedimientos documentados de "identificación de contraseñas" en forma periódica, que consistirán en tratar, mediante tecnología disponible, de revelar las contraseñas de los usuarios. Si una contraseña es "identificada" durante una de estas revisiones, se le solicitará al usuario que la cambie inmediatamente, siguiendo las recomendaciones planteadas en este documento.

3. Políticas en el uso de Internet

3.1. El derecho de acceso a la red Internet por parte de los usuarios, estará regido por lo dispuesto en la numeral 1.4 anterior.

3.2. Los servicios permitidos de acceso a Internet serán únicamente los que a continuación se detallan:

3.2.1. Acceso a servidores WEB (www.munibagaces.go.cr)

3.2.2. Acceso a servidores WEB (http://www.registronacional.go.cr/)

3.2.3. Acceso a servidores WEB (http://www.cgr.go.cr/)

3.2.4. Acceso a servidores WEB (http://www.datum.net/)

3.2.5. Acceso a Web Mail (www.munibagaces.go.cr/correo)

3.2.6. Acceso a correo electrónico POP3 y SMTP.

3.3. Cualquier acceso adicional a los citados en el punto anterior, deberá solicitarse con la justificación y autorización de la jefatura correspondiente, al departamento de TIC. Será responsabilidad de esta Unidad, el permitir o denegar el acceso a esos servicios.

3.4. El Departamento de TIC dará seguimiento al empleo que se dé al servicio de Internet por parte de los usuarios, y tendrá la facultad de emitir informes de los sitios visitados por los usuarios o bloquear accesos no permitidos, entendidos como aquellos que no guarden relación con aspectos de trabajo o que pongan en riesgo la seguridad de los recursos informáticos.

4. Políticas de uso del correo electrónico

4.1. El servicio de correo electrónico institucional constituye un medio de comunicación formal, y los usuarios deberán maximizar su aprovechamiento.

4.2. La información contenida en los correos electrónicos es privada y pertenece al usuario titular de la cuenta. Por lo tanto, nadie puede accederla, excepto la Administración, mediante el debido proceso u orden judicial.

4.3. Se prohíbe la utilización del servicio de correo electrónico con fines comerciales, políticos, lucrativos, de entretenimiento, distribución de información no solicitada por el receptor del mensaje, propagación intencional de virus informáticos o cualquier otro que no sea estrictamente de asuntos laborales.

4.4. El usuario deberá velar por el correcto uso del espacio asignado para él en el disco duro, manteniendo almacenados el número mínimo de mensajes posibles, para evitar su saturación. Si la aplicación local lo permite el usuario deberá copiar ("bajar") al equipo personal los mensajes recibidos y borrarlos del servidor principal de correo. La administración de los mensajes ubicados en el computador personal es responsabilidad del usuario.

5. Políticas de seguridad en computadoras estacionarias y móviles

5.1. Solamente en situaciones calificadas y con la autorización y coordinación de El Departamento de TIC se permitirá conectar a la red institucional un equipo que no pertenezca a MUNICIPALIDAD DE BAGACES. Para estos casos El Departamento de TIC debe llevar un registro del equipo y garantizar que cumpla con las políticas de seguridad tecnológica establecidas institucionalmente.

5.2. Al momento de detectarse algún virus, será obligatorio informar de inmediato a la Unidad de Cómputo, para evitar y controlar su posible diseminación. Lo anterior se comunicará mediante llamada telefónica, evitando utilizar el correo interno para notificarlo.

5.3. Los equipos que se encuentren conectados a la red institucional, permanentemente o en forma temporal, deberán contar, además de con el programa antivirus, con un "muro de fuego" o *firewall personal* instalado y configurado por los funcionarios del departamento de TIC. Cualquier anomalía reportada por estos programas deberá notificarse de inmediato a la Unidad de Cómputo, para las acciones correspondientes.

5.4. Todos los programas instalados en las computadoras, deberán haber sido autorizados y registrados previamente por la Unidad de Cómputo, la cual podrá implementar los mecanismos necesarios para manejar inventarios remotos y desinstalar cualquier programa que no esté autorizado. El usuario es el responsable de todos los programas no autorizados que se encuentren en el equipo a su cargo.

5.5. Por ninguna circunstancia un usuario deberá, sin autorización expresa de la Unidad

de TIC, utilizar el equipo a cargo como servidor de servicios adicionales (FTP, Telnet, WWW, o servidor de chat). El Departamento de TIC deberá llevar un registro de los equipos autorizados para ejecutar estos servicios adicionales.

5.6. El Departamento de TIC es responsable de coordinar las labores necesarias para la reparación y ampliación de las computadoras y equipo periférico.

5.7. El usuario a cargo del equipo es el responsable de mantener respaldos adecuados de la información que considere necesaria, según los procedimientos que disponga la Unidad de Cómputo.

6. Políticas de control de virus informáticos

6.1. El Departamento de TIC será la responsable de poner a disposición de los usuarios por los mecanismos más eficientes, las versiones actualizadas del programa de antivirus utilizado institucionalmente.

6.2. Para garantizar un nivel mayor de seguridad en el control de los virus informáticos, El Departamento de TIC deberá contar con dispositivos de validación de contenido, de forma que analicen todo el tráfico de datos proveniente de correos electrónicos que ingresen a MUNICIPALIDAD DE BAGACES. Estos dispositivos deberán tener la posibilidad de actualizar sus archivos de virus en forma automática, y su administración será responsabilidad de la Unidad de Cómputo.

6.3. El Departamento de TIC deberá monitorear permanentemente la existencia –externa e interna- de virus informáticos y proceder a aplicar las medidas preventivas y correctivas para minimizar el riesgo de contagio por parte de los equipos institucionales; para ello contará con la tecnología necesaria.

7. Políticas de seguridad en la administración y control ambiental del centro de cómputo

7.1. El Departamento de TIC será el responsable de definir e implementar los controles relacionados con la administración, las condiciones de ambiente y el acceso físico al centro de cómputo y cuartos de comunicaciones (espacio destinado para ubicar los equipos de comunicaciones de la red institucional).

7.2. Se deberán implementar las recomendaciones que resulten procedentes, según las prioridades y disponibilidad presupuestaria, relacionadas con el control ambiental del centro de cómputo (indicadas en el anexo 3 de este documento).

ANEXO 1: DIRECTRICES DE USO Y CREACIÓN DE CONTRASEÑAS (*PASSWORDS*)

Los passwords o contraseñas secretas son utilizados para varios propósitos en los sistemas informáticos de la MUNICIPALIDAD DE BAGACES. Algunos de los usos más comunes incluyen: cuentas al nivel de usuario, cuentas web, cuentas de correo, protectores de pantallas y para acceder a enrutadores locales.

Todos los usuarios deben conocer cómo elegir contraseñas robustas.

Las contraseñas robustas tienen las siguientes características:

- ✧ Contienen letras en mayúscula y en minúscula (Ej.: a-z, A-Z)
- ✧ Tienen dígitos y caracteres de puntuación, así como letras, por ejemplo, 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./) Son de por lo menos ocho caracteres alfanuméricos.
- ✧ No son una palabra en ningún lenguaje, dialecto, muletilla o jerga cotidiana. No están basados en información personal, o nombres de familiares.

Las contraseñas débiles tienen las siguientes características:

- ✧ Menos de ocho caracteres.
- ✧ Palabra encontrada en un diccionario.
- ✧ Palabra de uso común: nombres de familia, mascotas, amigos, compañeros, o fábulas. Términos y nombres de computadoras, comandos, sitios, compañías, *hardware*, *software*.
- ✧ Fechas de cumpleaños y otra información personal como direcciones y números de teléfono. Patrones de números y letras como aaabbb, qwerty, zyxwvuts, y 123321.
- ✧ Cualquiera de las de arriba deletreadas, al revés.
- ✧ Cualquiera de las de arriba señaladas, precedidas o seguidas por un dígito (Ej.: secreto1, 1secreto)

ANEXO 2: DIRECTRICES PARA PROTECCIÓN DE CONTRASEÑAS (*PASSWORDS*)

- ✧ No utilice la misma contraseña que utiliza en los sistemas de MUNICIPALIDAD DE BAGACES en otras cuyo acceso no pertenece a la Institución, por ejemplo cuentas bancarias, correos externos diferentes al Institucional, etc.

- ✧ No lo escriba en papel ni lo almacene en su oficina

- ✧ No almacene esta contraseñas en NINGUNA computadora de la oficina.

- ✧ No se permite compartir las contraseñas de la Institución con nadie. Todas las contraseñas deben ser tratadas como sensitivas y de información confidencial de la Institución.

- ✧ No se permite utilizar las funciones de "recordar *password*" ("Remember Password") de aplicaciones que permitan esta facilidad (Ej. Eudora, Outlook, Mozilla, Netscape Messenger, entre otros)

- ✧ No se permite realizar ninguna de las condiciones descritas abajo, las cuales atentan contra la confidencialidad de las contraseñas:

    - Revelar una contraseña en una conversación telefónica.
    - Revelar una contraseña en un mensaje de correo.
    - Revelar una contraseña a terceras personas.
    - Hablar de una contraseña en frente de otros.
    - Dar pistas sobre el formato de una contraseña (Ej.: "Mi apellido paterno").
    - Revelar una contraseña en un cuestionario o formularios de seguridad.
    - Compartir las contraseñas con miembros de la familia.
    - Revelar una contraseña a un compañero de trabajo mientras está de vacaciones.

ANEXO 3: DIRECTRICES DE CONTROL AMBIENTAL DEL CENTRO DE CÓMPUTO

Lineamientos de Acceso Físico.

- ✧ El Departamento de TIC de MUNICIPALIDAD DE BAGACES designará una persona que se encargará de administrar el acceso físico al centro de cómputo, la cual deberá llevar los mecanismos de control necesarios que garanticen los esquemas de seguridad de los equipos ubicados en esta área. En este centro no pueden estar transitando personas, para desplazarse a otras oficinas. Es exclusivo del Departamento de TIC.

- ✧ El control de acceso al centro de cómputo debe tener no sólo la capacidad de identificación, sino también asociarla a la apertura o cierre de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector, horarios semanales y días feriados.

- ✧ El sistema de control de acceso debe contar con capacidad para llevar el control de ingreso de usuarios a las áreas asignadas y poder exportar el archivo a otros formatos que puedan ser leídos fácilmente por otros programas.

- ✧ El sistema de control de acceso deberá proveer un mecanismo que permita ante emergencias naturales o por eventos imprevistos que pongan en peligro la integridad física de las personas en las áreas restringidas, poder desactivar los mecanismos de apertura de puertas para la inmediata evacuación del sitio.

- ✧ Todos los funcionarios con acceso al centro de cómputo son responsables de aplicar adecuadamente los procedimientos de seguridad de acceso físico y de informar cualquier sospecha de violación de las medidas a su jefe inmediato.

Lineamientos de Control Ambiental.

- ✧ Los materiales de construcción del Centro de Cómputo no deberán ser inflamables, igualmente no se deberán almacenar en este lugar materiales inflamables.

- ✧ El local del centro de cómputo no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.

- ✧ El piso y el techo en el recinto de ubicación de la computadora y de almacenamiento de los medios magnéticos deben ser impermeables.

- ✧ El Centro de Cómputo debe contar con mecanismos de ventilación y detección de incendios adecuados.

- ✧ El centro de cómputo debe tener instalados suficientes extintores portátiles de dióxido de

carbono y del tipo llamados rociadores en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.

- ✧ El centro de cómputo debe tener un sistema de ventilación y aire acondicionado dedicado al cuarto de computadoras y equipos de proceso de datos en forma exclusiva. Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de incendios e inundaciones (provocados por fugas a través de los ductos) es recomendable instalar redes de protección en todo el sistema de cañería al interior y al exterior, detectores y extintores de incendio, monitores y alarmas de sonido efectivas.

- ✧ El centro de cómputo debe contar con sistemas UPS (no-break o fuente de energía ininterrumpible) contra fallas de energía que garanticen la correcta operación de los sistemas de cómputo. Será preferible que el sistema de UPS sea independiente para el centro de cómputo y no sea compartido con el resto de la Institución.

- ✧ Se debe asegurar que el sistema de UPS esté ventilado apropiadamente, sin materiales u objetos que lo obstruyan.

- ✧ El centro de cómputo debe tener detectores de humo, agua, humedad y temperatura y se les deberá dar un mantenimiento preventivo y correctivo.

- ✧ Las superficies destinadas al tránsito de funcionarios dentro del centro de cómputo deben estar libres de obstáculos para poder circular con seguridad.

- ✧ En los pisos de las áreas de trabajo del centro de cómputo debe evitarse el almacenamiento de líquidos, para evitar derrames.

- ✧ Se debe asegurar que los cables eléctricos y las cajas de empalme estén separadas del piso y que los cables eléctricos, cajas de empalme, switches, toma de energía eléctrica y paneles estén localizados fuera del alcance de derrames potenciales de líquidos.

- ✧ Se prohíbe el uso de cables eléctricos sueltos en áreas de tráfico de funcionarios y se debe asegurar que todos los circuitos estén conectados a una tierra común; y de que haya suficientes circuitos y que estén instalados distribuidamente para que ninguno se sobrecargue.

- ✧ Los controles eléctricos serán guardados en paneles debidamente controlados. Se deberá procurar que las cajas de interruptores de energía eléctrica estén accesibles fácilmente e instalados cerca de la entrada al centro de computo.

- ✧ Se debe proveer la iluminación adecuada para prevenir esfuerzo innecesario de la vista de los funcionarios, que haya iluminación exterior adecuada para prevenir cualquier situación imprevista y que exista iluminación de emergencia en el centro de cómputo. Este equipo se debe chequear periódicamente.

- ✧ Se deben de adherir etiquetas identificadoras a los cables eléctricos, cajas de empalme, paneles y equipo eléctrico.

- ✧ Los racks de piso del cableado estructurado y equipos de red de piso, deberán estar colocados en gabinetes con llave y apropiados para tal efecto (o en su defecto en

recintos con puertas aseguradas) y de fácil acceso por parte de los funcionarios de El Departamento de TIC de MUNICIPALIDAD DE BAGACES.

- ✧ Las llaves utilizadas en los gabinetes de piso (o recintos) estarán bajo el control de El Departamento de TIC de MUNICIPALIDAD DE BAGACES y será la jefatura la encargada de establecer a los responsables de administrarlas.

- ✧ El encargado Unidad de Cómputo de MUNICIPALIDAD DE BAGACES deberá velar por que se cumplan y acaten las políticas de control de acceso y seguridad física anteriormente descritas.