

RESOLUCION No. 263
(Octubre 24 de 2014)

“POR LA CUAL SE ADOPA EL MANUAL DE POLITICAS Y ESTANDARES EN
SEGURIDAD INFORMATICA “

LA DIRECTORA GENERAL DEL INSTITUTO DE DESARROLLO MUNICIPAL DE DOSQUEBRADAS, en uso de sus atribuciones legales y especial las conferidas por los artículos 10 del Decreto 275 del 26 de septiembre de 2001, resolución 001 del 03 de enero de 2011 y,

C O N S I D E R A N D O:

1. Que el Instituto de Desarrollo Municipal de Dosquebradas, actualmente se encuentra en la implementación del Sistema de Gestión de Calidad, de acuerdo con los requisitos de la norma NTC-ISO 9001 y la NTC GP 1000, con el fin de lograr la certificación en calidad, para lo cual fue necesario actualizar los procesos y procedimientos de la entidad que determinaron la necesidad de un manual de política y estándares en seguridad informática.
2. Que se hace necesario la implementación de este manual, con el objeto de establecer medidas y patrones técnicos de administración y organización de las Tecnologías de Información y Comunicaciones TIC's, como lo establece la norma NTC- ISO/IEC 27001.
3. Que en virtud a lo anterior,

R E S U E L V E:

ARTICULO PRIMERO: Adoptar el Manual de políticas y estándares en seguridad informática:

1. INFORMACION GENERAL

1.1. Aplicación

Las políticas y estándares de seguridad informática tienen por objeto establecer medidas y patrones técnicos de administración y organización de las Tecnologías de Información y Comunicaciones TIC's de todo el personal comprometido en el uso de los servicios informáticos proporcionados el Instituto de Desarrollo Municipal de Dosquebradas.

También se convierte en una herramienta de difusión sobre las políticas y estándares de seguridad informática a todo el personal del Instituto, facilitando una mayor integridad, confidencialidad y confiabilidad de la información generada por medios tecnológicos, al manejo de los datos, al uso de los bienes informáticos tanto de hardware como de software disponible, minimizando los riesgos en el uso de las tecnologías de información.

1.2. Políticas de Seguridad Informática

SEGURIDAD INSTITUCIONAL - Toda persona que ingresa como usuario nuevo al Instituto de Desarrollo Municipal de Dosquebradas para manejar los equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

SEGURIDAD FISICA Y DEL MEDIO AMBIENTE - Para el acceso a los sitios y áreas restringidas (Rack de Comunicaciones, Servidores, entre otros) se debe notificar a la persona a cargo de Sistemas para la autorización correspondiente, y así proteger la información y los bienes informáticos.

ADMINISTRACION DE OPERACIONES EN LOS CENTROS DE CÓMPUTO - Los usuarios y funcionarios deberán proteger la información utilizada en la infraestructura tecnológica del Instituto de Desarrollo Municipal de Dosquebradas. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna institucional a otras dependencias de sedes alternas o redes externas como internet.

1.3. Evaluación

Las políticas tendrán una revisión periódica se recomienda que sea anual para realizar actualizaciones, modificaciones y ajustes basados en las recomendaciones y sugerencias.

1.4. Beneficios

Las políticas y estándares de seguridad informática establecidas en el presente documento son la base fundamental para la protección de los activos informáticos y de toda la información de las Tecnologías de Información y Comunicaciones (TIC's) en la Institución.

2. SEGURIDAD INSTITUCIONAL

POLITICA - Toda persona que ingresa como usuario nuevo al Instituto de Desarrollo Municipal de Dosquebradas para manejar los equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

2.1. Usuarios Nuevos

Todo el personal nuevo de la Institución, tanto funcionario de planta como contratista, deberá ser notificado a la persona a cargo de TIC, para que le sean creadas sus credenciales de usuario correspondientes acorde a su función (Gesar, Sicru, Reportando, Saga, Correo, Backup, Direccionamiento IP) o en caso de retiro del funcionario, anular y cancelar los derechos otorgados como usuario informático.

2.2. Obligaciones de los Usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente Manual.

2.3. Capacitaciones en Seguridad Informática

Todo servidor, contratista o funcionario nuevo en el Instituto de Desarrollo Municipal de Dosquebradas deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática Manual de Usuarios, donde se den a conocer las obligaciones para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento.

2.4. Sanciones

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de este Instituto, o de que se le declare culpable de un delito informático.

3. SEGURIDAD FISICA Y DEL MEDIO AMBIENTE

POLITICA - Para el acceso a los sitios y áreas restringidas (Rack de

NOMBRE DEL DOCUMENTO: ACTOS ADITIVOS RESOLUCIONES
COD: DG-100.12 VERSION: 3 FECHA: 2-08-13

Comunicaciones, Servidores, entre otros) se debe notificar a la persona a cargo de Sistemas para la autorización correspondiente, y así proteger la información y los bienes informáticos.

3.1. Protección de la Información y de los Bienes Informáticos

- 3.1.1. El usuario o funcionario deberá reportar de forma inmediata al personal a cargo de las TIC cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.
- 3.1.2 El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.
- 3.1.3 Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

3.2. Controles de Acceso Físico

- 3.2.1. Las computadoras, portátiles, y cualquier activo de tecnología de información, podrá ser retirados de las instalaciones del Instituto de Desarrollo Municipal de Dosquebradas únicamente con la autorización de salida del Subdirector Administrativo y Financiero, anexando la descripción técnica del equipo, tiempo, objeto o labor, solicitud debidamente firmado por el Jefe Inmediato del área que requiere el retiro.

3.3. Seguridad en Áreas de Trabajo

El Rack de comunicaciones del Instituto de Desarrollo Municipal es un área restringida, por lo que solo el personal autorizado puede acceder a él.

3.4. Protección y Ubicación de los Equipos

- 3.4.1. Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la persona a cargo de las TIC, en caso de requerir servicio deberá solicitarlo.

- 3.4.2. El Área de Inventarios de activos será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación previamente designada.
- 3.4.3. El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de los funcionarios o servidores del Instituto de Desarrollo Municipal de Dosquebradas.
- 3.4.4. Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
- 3.4.5. Es responsabilidad de los usuarios mantener la información respaldada en el servidor para backups designado para tal fin.
- 3.4.6. Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.
- 3.4.7. Se debe evitar colocar objetos encima del equipo cómputo o tapar las salidas de ventilación del monitor o de la CPU.
- 3.4.8. Se debe mantener el equipo informático en un lugar limpio y sin humedad.
- 3.4.9. Cuando se requiera realizar cambios múltiples de los equipo de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, éstos deberán ser notificados con 2 días de anticipación al personal a cargo de las TIC a través de un plan detallado.
- 3.4.10. Queda terminantemente prohibido que el usuario o funcionario distinto al personal a cargo de las TIC abra o destape los equipos de cómputo.

3.5. Mantenimiento de Equipos

- 3.5.1. Únicamente el personal a cargo de las TIC podrá llevar a cabo los servicios y reparaciones al equipo informático.

- 3.5.2. Los usuarios deberán asegurarse de respaldar en copias de respaldo o backups la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

3.6. Perdida de Equipo

- 3.6.1. El servidor o funcionario que tengan bajo su responsabilidad o asignados algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.
- 3.6.2. El préstamo de laptops o portátiles tendrá que solicitarse a la Subdirección Administrativa y Financiera, mediante documento escrito que describa entre otros las características técnicas del equipo y accesorios con los que se solicita, duración del préstamo, objeto o labor a realizar.
- 3.6.3. El servidor o funcionario deberán dar aviso inmediato a la Subdirección Administrativa y Financiera y a la Administración de Inventarios de Activos de la desaparición, robo o extravío de equipos de cómputo, periféricos o accesorios bajo su responsabilidad, también se deberá dar aviso al personal a cargo de las TIC para proceder a bloquear cualquier clave de usuario que pueda comprometer la seguridad de los diferentes aplicativos informáticos de la Institución.

3.7. Uso de Dispositivos Extraíbles (USB – DVD RW – HD)

- 3.7.1. El uso de los quemadores externos o grabadores de disco compacto es exclusivo para Backups o copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.
- 3.7.2. El servidor o funcionario usuario que tengan asignados estos tipos de dispositivos serán responsable del buen uso de ellos.

3.7.3. Si algún área o dependencia por requerimientos muy específicos del tipo de aplicación o servicios de información tengan la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por el personal a cargo de las TIC con el respectivo visto bueno de la Subdirección Administrativa y Financiera o en su defecto de su Jefe inmediato o un superior de la Alta Dirección.

3.7.4. Todo funcionario o servidor del Instituto de Desarrollo Municipal de Dosquebradas deberá reportar al personal a cargo de las TIC el uso de las memorias USB asignados para su trabajo y de carácter personal y responsabilizarse por el buen uso de ellas.

3.8. Daño del Equipo

3.8.1. El equipo de cómputo, periférico o accesorio de tecnología de información que sufra algún desperfecto, daño por maltrato, descuido o negligencia por parte del usuario responsable, se le levantara un reporte de incumplimiento de políticas de seguridad.

4. ADMINISTRACION DE OPERACIONES EN LOS CENTROS DE COMPUTO

POLITICA - Los usuarios y funcionarios deberán proteger la información utilizada en la infraestructura tecnológica del Instituto de Desarrollo Municipal de Dosquebradas. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna institucional a otras dependencias de sedes alternas o redes externas como internet.

4.1. Seguridad y Protección

4.1.1. Los usuarios y funcionarios del Instituto de Desarrollo Municipal de Dosquebradas que hagan uso de equipos de cómputos, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red.

4.1.2. Cuando un funcionario no autorizado o un visitante requieran la necesidad

de ingresar al área donde se encuentre el rack de comunicaciones y servidores, debe solicitar mediante comunicado interno debidamente firmada y autorizado por el Jefe inmediato de su sección o dependencia y para un visitante se debe solicitar la visita con anticipación la cual debe traer el visto bueno de la Dirección, y donde se especifique tipo de actividad a realizar, y siempre contar con la presencia de un funcionario de la oficina TIC.

- 4.1.3. Cuando se vaya a realizar un mantenimiento en algunos de los equipos del Rack de Comunicaciones o Servidores, se debe dar aviso con anticipación a los usuarios para evitar traumatismos.
- 4.1.4. La Dirección del Instituto de Desarrollo Municipal de Dosquebradas debe dotar la zona donde estén los servidores y rack de comunicaciones con los equipos de protección contra incendios, inundaciones, sistema eléctrico de respaldo, UPS.

4.2. Uso de los medios de almacenamiento

- 4.2.1. Los usuarios y servidores del Instituto de Desarrollo Municipal de Dosquebradas deben conservar los registros o la información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial.
- 4.2.2. Las actividades que realicen los usuarios y funcionarios en la infraestructura Tecnología de Información y Comunicaciones (TIC's) del Instituto de Desarrollo Municipal de Dosquebradas serán registradas y podrán ser objeto de auditoria.

4.3. Adquisición y Licenciamiento de Software

- 4.3.1. Los usuarios y funcionarios que requieran la instalación de software que sea propiedad del Instituto de Desarrollo Municipal de Dosquebradas, deberán justificar su uso y solicitar su autorización por la Oficina Nuevas Tecnologías con el visto bueno de su Jefe inmediato, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que será usado.

- 4.3.2. Se considera una falta grave el que los usuarios o funcionarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red del Instituto de Desarrollo Municipal de Dosquebradas que no esté autorizado por la Oficina Nuevas Tecnologías y que no cuenten con la debida licencia de uso.
- 4.3.3. La Oficina Nuevas Tecnologías, tiene a su cargo la tarea de informar periódicamente a los funcionarios y contratistas del Instituto de Desarrollo Municipal de Dosquebradas su política institucional contra la piratería de software, utilizando todos los medios de comunicación disponibles: Página WEB, Emails, Carteleros y Boletines. Debemos considerar también la publicación de las posibles sanciones o multas en los que se puede incurrir.
- 4.3.4. Las licencias y el inventario de los Medios, paquete de CD's serán almacenados en la oficina de Dirección .
- 4.3.5. El Grupo de Apoyo (Técnicos) de la Oficina Nuevas Tecnologías tiene la responsabilidad de velar por el buen uso de los equipos de cómputo y del cumplimiento de las políticas de seguridad. A su vez deberán ofrecer mantenimiento preventivo a las computadoras del Instituto.
- 4.3.6. En el proceso de reinstalar un programa el técnico debe borrar completamente la versión instalada para luego proceder a instalar la nueva versión que desea, esto siempre y cuando no sea una actualización del mismo.
- 4.3.7. Se debe mantener un inventario de equipos físicos y de los programas instalados y solo se pueden borrar o instalar programas o software autorizados y legalmente licenciados.
- 4.3.8. Se debe brindar semestralmente capacitación al personal para estimular en gran medida la utilización de los programas adquiridos legalmente, evitando la práctica indebida de utilizar y la proliferación software no autorizado (pirata).

4.4. Identificación de un incidente

- 4.4.1. El usuario o funcionario que detecte o tenga conocimiento de la posible ocurrencia de un incidente de seguridad informática deberá reportarlo al Área de la Oficina Nuevas Tecnologías lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.
- 4.4.2. Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las Directivas Administrativas competentes, el usuario o funcionario informático deberá notificar a la Oficina Nuevas Tecnologías.
- 4.4.3. Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información del Instituto de Desarrollo Municipal de Dosquebradas debe ser reportado a la Oficina Nuevas Tecnologías.

4.5. Administración de la red

- 4.5.1. Los usuarios de las instalaciones del Instituto de Desarrollo Municipal de Dosquebradas no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la entidad, sin la autorización de la Oficina Nuevas Tecnologías.

4.6. Seguridad para la red

- 4.6.1. Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por la Oficina Nuevas Tecnologías, en la cual los usuarios o funcionarios realicen la exploración de los recursos informáticos en la red del Instituto de Desarrollo

Municipal de Dosquebradas, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

4.7. Uso del correo electrónico

- 4.7.1. Los usuarios y funcionarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe re direccionar el correo a otra cuenta de correo del Instituto.
- 4.7.2. Los usuarios y funcionarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad del Instituto de Desarrollo Municipal de Dosquebradas. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.
- 4.7.3. Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera encriptado y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y responsabilidades.
- 4.7.4. Queda prohibido falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.
- 4.7.5. Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

4.8. Controles contra virus o software malicioso

- 4.8.1. Para prevenir infecciones por virus informático, los usuarios no deben hacer uso de software que no haya sido proporcionado y validado por la Oficina Nuevas Tecnologías.
- 4.8.2. Los usuarios deben verificar que la información y los medios de

Almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por la Oficina Nuevas Tecnologías.

- 4.8.3. Todos los archivos de computadoras que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.
- 4.8.4. Ningún usuario, funcionario, empleado o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la Oficina Nuevas Tecnologías.
- 4.8.5. Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y notificar a la Oficina Nuevas Tecnologías para la revisión y erradicación del virus.
- 4.8.6. Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por la Oficina Nuevas Tecnologías en: Antivirus, Outlook, office, Navegadores u otros programas.
- 4.8.7. Debido a que algunos virus son extremadamente complejos, ningún usuario o funcionario, distinto al personal de la Oficina Nuevas Tecnologías deberá intentar erradicarlos de las computadoras.

4.9. Controles para las copias de respaldo (Backup)

- 4.9.1. Establecer como medida de seguridad informática la necesidad de realizar copias de respaldo o backups periódicamente en los equipos de cómputo administrativos y servidores.
- 4.9.2. Cada funcionario es responsable directo de la generación de los backups o
- 4.9.3.

copias de respaldo, asegurándose de validar la copia. También puede solicitar asistencia técnica para la restauración de un backups.

- 4.9.4. El Usuario debe conocer y manejar el software utilizado para la generación y/o restauración de copias de respaldo, registrando el contenido y su prioridad. Rotación de las copias de respaldo, debidamente marcadas.
- 4.9.5. Las copias de seguridad o Back ups se deben realizar al menos una vez a la semana y el último día hábil del mes y son responsabilidad de cada Usuario o Funcionario realizarlas oportunamente, al igual que la información en ella contenida.

ARTICULO SEGUNDO: La presente Resolución rige a partir de la fecha de su expedición.

COMINIQUESE Y CÚMPLASE

Dada en Dosquebradas, Rda, a los veinticuatro (24) días del mes de octubre del año dos mil catorce (2014).

PAULA ANDREA VIDAL POLANIA
Directora Encargada IDM

DUPARFAY BUITRAGO TORRES
Vo. Bo. Asesor Jurídico Externo

PROYECTO | HUGO ANDRES OROZCO RIOS | REVISÓ | DUPARFAY BUITRAGO TORRES | APROBO | PAULA ANDREA VIDAL POLANIA