Dirección General de Ética e Integridad Gubernamental

Manual de Políticas de Tecnologías de la Información y Comunicación (TIC)

Febrero • 2016

INDICE

INTRODUCCIÓN

I. ASPECTOS GENERALES 1

1.2. Objetivo General 1

1.3. Objetivos Específicos 1

1.4. Alcance 2

1.5. Definiciones 2

1.6. Formatos Requeridos/Referencias 5

1.7. Mecanismos de Control/Responsabilidades 5

1.8. Distribución del Manual 6

1.9. Puesta en Vigencia 6

1.10. Revisiones y Modificaciones 6

1.11. Organigrama Estructural 7

II. POLÍTICAS GENERALES DE TECNOLOGÍA 8

2.1. INFRAESTRUCTURA DE HARDWARE (EQUIPOS, DISPOSITIVOS Y APARATOS) 8

Responsabilidades de TIC: 8

Responsabilidades de los usuarios 10

2.2. INFRAESTRUCTURA DE SOFTWARE (PROGRAMAS DE COMPUTADORA). 11

a) Responsabilidad de TIC 11

Responsabilidades y/o Prohibiciones de los usuarios 12

2.3. SEGURIDAD DEL ÁREA DE INFORMÁTICA 13

2.4. CUSTODIA Y TENENCIA DE ACTIVOS INFORMÁTICOS 14

Responsabilidad de TIC 14

Responsabilidad de los usuarios 14

2.5. TRASLADO DE ACTIVOS INFORMÁTICOS FUERA DE LA DIGEIG. 15

Responsabilidad de TIC 15

Responsabilidad de los usuarios 15

2.6. ROBO O PÉRDIDA DE EQUIPO 16

2.7. SOFTWARE (PROGRAMAS DE COMPUTADORA) 17

Responsabilidad de TIC 17
2.8. MODIFICACIÓN O INSTALACIÓN DE SOFTWARE (PROGRAMAS) 17
Responsabilidad de TIC 17
2.10. SOPORTE TÉCNICO A LOS EQUIPOS ASIGNADOS 18
Responsabilidad de TIC 18
Responsabilidad de los usuarios 19
2.11. PLAN DE CONTINGENCIA 19
Responsabilidad de TIC 19
Responsabilidad de los usuarios 20
2.12. ASIGNACIÓN DE USUARIO 20
Responsabilidad de TIC 20
Responsabilidad de los usuarios 22
2.13. PRIVILEGIOS Y ACCESOS DE LOS SISTEMAS 23
2.14. SEGURIDAD Y RESPALDO DE LAS INFORMACIONES 24
Responsabilidad de TIC 24
Responsabilidad de los usuarios 26
2.16. SEGURIDAD Y ACCESO ÁREA DE EQUIPOS INFORMATICOS 28
2.17. MANEJO DE IMPRESORAS 29
Responsabilidad de TIC 29
Responsabilidad de los usuarios 30
2.18. ACCESO AL INTERNET 31
Responsabilidad de TIC 31
Responsabilidad de los usuarios 32
III. IMPREVISTOS 33
IV. VERSIÓN 33

INTRODUCCIÓN

El Manual de Políticas de Tecnología de la Información Comunicación TIC, de la Dirección General de Ética e Integridad Gubernamental (DIGEIG), servirá para garantizar el buen funcionamiento de los procesos así como para optimizar y garantizar la seguridad de las informaciones y la calidad en el uso de los sistemas internos en cumplimiento de los lineamientos establecidos mediante Normativa general sobre el uso e implementación de las tecnologías de la información y comunicaciones en el Estado Dominicano, dígase NORTIC A1.

Este Manual de Políticas busca brinda apoyo a las DIGEIG en la gestión y mejoramiento de los procesos en donde se involucra a todo los servidores institucionales, así como establecer las políticas de TIC que regirán el uso y mantenimiento de la plataforma de servicios tecnológica de la institución, para asegurar su operatividad, de manera que los responsables del uso de las tecnologías disponibles, aseguren el cumplimiento de las mismas, con miras al desarrollo de un trabajo óptimo y de calidad.

La DIGEIG como institución encargada de promover, fomentar y asesorar a las demás instituciones del Estado Dominicano en materia de la ética y la transparencia, espera que el establecimiento de este manual de políticas pueda transparentar y dar idoneidad a los métodos utilizados para manejar el uso de la tecnología de la información que dispone la institución.

En lo adelante nos referiremos a la **División de Tecnología de la Información y Comunicaciones** con las siglas **TIC**.

I. ASPECTOS GENERALES

1.2. Objetivo General

Establecer las políticas que garanticen el control de los sistemas, plataforma de servicio del acceso y el acceso por parte de los servidores a los sistemas informáticos institucionales y el cumplimiento de las normativas establecidas por los organismos reguladores del Estado Dominicano.

1.3. Objetivos Específicos

Los objetivos del Manual de Políticas de Tecnología de la Información y Comunicaciones de la DIGEIG, son los siguientes:

a) Crear y definirlas políticas generales y específicas que faciliten la ejecución de las actividades de tecnología de la información en las diferentes áreas de la Institución y cumplimiento de la Norma NORTIC A1.

b) Planificar y coordinar todas las actividades de evaluación de procesos.

c) Gestionar mejoras a los procesos de administración sobre servicios de TIC.

d) gestionar todas las actividades relacionadas con el aseguramiento de la calidad de los servicios de TIC

e) Promover el uso adecuado de los recursos humanos, materiales y activos tecnológicos adecuados.

f) Diseñar y desarrollar la implementación y soporte de los programas y sistemas que apoyan los procesos esenciales de la institución.

g) Normar los procesos de información con la finalidad de mejorar el rendimiento de la DIGEIG.

h) Establecer las políticas para resguardo y garantía de acceso apropiado de la información de la DIGEIG.

1.4. Alcance

El presente Manual abarca las políticas que serán aplicadas en la Institución, a través de la División de Tecnología de la Información.

1.5. Definiciones

Acceso: grado en que los usuarios, sin importar su capacidad, puedan acceder y manipular un software.

Actualización: se refiere al consolidado de cambios para ser aplicados para corregir errores y agregar funcionalidades.

Amenaza: es un evento que puede provocar un daño o perjuicio al organismo.

Antivirus: es un programa desarrollado con el fin de proteger un computador o servidor contra virus informáticos.

Calidad de servicio: hace referencia al rendimiento de una red telefónica o de computadoras.

Copias de respaldo: son copias de los datos almacenados de un sistema, con el objetivo de tenerlos disponibles en caso de fallas.

Correo electrónico: es un servicio de mensajería en red que permite el intercambio de mensajes, a través de sistemas de comunicación electrónicos.

Datos: hace referencia a un valor íntegro sobre un elemento determinado, el cual por si solo carece de importancia y a través del procesamiento adecuado logra convertirse en información útil.

Formato de Documento Portátil (PDF): es un formato de almacenamiento de datos que funciona y puede ser visualizado independientemente de la plataforma de servicio, siendo así portátil y multiplataforma para su visualización.

Formatos: hace referencia al tipo de codificación de la información en un archivo.
Hardware: se refiere a todas las partes físicas o tangibles de un sistema de información.

Infraestructura de TIC: para fines de esta norma, hace referencia al conjunto de equipos y elementos en lo que se sustenta un sistema de información.

Intranet: es una red interna para compartir de forma segura cualquier información o aplicación y evitar que cualquier usuario de Internet pueda ingresar a la red.

Multimedia: se refiere al conjunto de elementos de audio, video, textos, imágenes o animaciones usados para comunicar una información.

Tecnología de la Información: herramientas y métodos utilizados para recabar, retener, manipular o distribuir información, la cual se encuentra por lo general relacionada con las computadoras y las tecnologías afines aplicadas a la toma de decisiones.

Inventario: es un registro organizado de los activos pertenecientes o bajo la responsabilidad de un organismo determinado.

Permisos de acceso: privilegio que asociado a un usuario le permita acceder, borrar o modificar cualquier recurso informático, o realizar acciones a través de los distintos sistemas tales como enviar un correo, disparar un proceso, modificar un dato, etc.

Plataforma como Servicio: es un servicio de computación en la nube, en el cual el cliente tiene disponible la Información y Comunicación en el Estado Dominicano una plataforma para desarrollar y ejecutar diferentes tipos de software, siempre y cuando estos sean compatibles con dicha plataforma de información.

Red de Área Local (LAN): es una red de datos con un alcance geográficamente limitado. Red de Área Local Inalámbrica (WLAN): es un sistema de comunicación inalámbrico, utilizado como otra opción a las redes locales, usando la tecnología de radiofrecuencia para llevar información de un punto a otro, permitiendo mayor movilidad y disminución en las conexiones cableadas.

Redes sociales: son medios virtuales de comunicación que funcionan como una plataforma para que los usuarios puedan interactuar con otras personas que tienen intereses en común.

Servidores: son equipos informáticos que forman parte de una red de datos y que proveen servicios a otros equipos en dicha red, llamados clientes.

Software: se refiere a todos los componentes lógicos o intangibles de un sistema de información, tales como programas, aplicaciones, sistemas operativos, entre otros.

Sistema de Respuesta de Voz Interactiva (IVR): es un sistema telefónico capaz de recibir una llamada e interactuar con el humano, a través de grabaciones de voz y el reconocimiento de respuestas simples, mediante las teclas del teléfono o el móvil.

Riesgo: es la posibilidad o probabilidad potencial de que un daño o amenaza afecte a un organismo.

Usuario: hace referencia a la persona que consume o manipula un producto, servicio o información.

ZIP: es un formato de compresión de archivos sin pérdida que comprime cada uno de los archivos de forma separada.

Estas definiciones fueron tomadas de la norma NORTIC A1.

1.6. Formatos Requeridos/Referencias

A continuación relación de los documentos jurídicos y administrativos que soportan el Manual:

- **Resolución Interna 01/2014,** de fecha 12 de mayo del año 2014, sobre aprobación Estructura Organizativa de la DIGEIG.
- **Resolución Interna No. RI 002-2014** de fecha 28 de octubre del año 2014, sobre emisión Manual de Organización y Funciones DIGEIG,
- **Comunicación 005612 del Ministerio de Administración Publico, MAP** de fecha 04 de noviembre del año 2014, sobre aprobación Manual de Organización Funciones DIGEIG.
- **Circular No. 09-2014** de fecha 07 de noviembre del año 2014, sobre puesta en circulación Manual De Organización y Funciones a servidores DIGEIG.
- **Resolución Núm. 51-2013** de fecha 03 de diciembre del año 2013, que aprueba los Modelos de Estructura de Organización de las Unidades de Tecnología de Información y Comunicación (TIC).
- **NORTIC A1,** de fecha 15 de mayo del año 2014, sobre la normativa general uso e implementación de las tecnologías de la información y comunicación en el Estado Dominicano

1.7. Mecanismos de Control/Responsabilidades

A continuación las áreas responsables que sirven de mecanismos de control en la ejecución del procedimiento descrito en este Manual, así como los puestos que intervienen, parcial o totalmente en el desarrollo de las actividades:

- **Dirección Ejecutiva:** Director Ejecutivo.

- **División de Tecnología de la Información y comunicación**, ***TIC****: Soporte Técnico, Soporte a Usuario y Programadores,*

1.8. Distribución del Manual

Una copia completa de este manual en físico será entregada al encargado División de TIC, el cual contendrá una comunicación interna del Director Ejecutivo de la DIGEIG instruyendo su validación y puesta en ejecución.

Será puesto al conocimiento de todos los demás encargados de áreas vía correo electrónico con el Manual de Política anexo en formato de Documento Portátil (PDF) indicando la ruta en el Público. Cada encargado de área será responsable de compartir este documento con los servidores que se encuentren bajo su dependencia.

1.9. Puesta en Vigencia

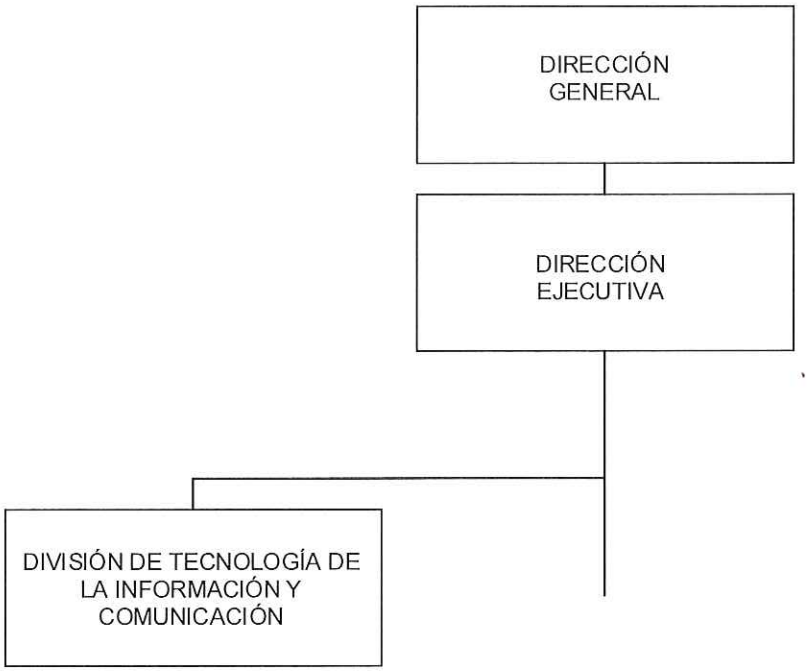
Este manual será puesto en vigencia tan pronto el mismo sea aprobado por el Director Ejecutivo de la Institución, permanecerá por tiempo indefinido introduciéndosele las revisiones y las mejoras que amerite el mismo.

1.10. Revisiones y Modificaciones

Cualquier cambio, corrección o recomendación se comunicará al Departamento de Planificación y Desarrollo, responsable de llevar a cabo revisiones periódicas al documento.

1.11. Organigrama Estructural

División de Tecnología de la Información y Comunicación, TIC.



II. POLÍTICAS GENERALES DE TECNOLOGÍA

La División de Tecnología de la Información y Comunicación (TIC), como área de servicio interno, se encarga de resguardar, velar por el uso y funcionamiento de la plataforma de servicio tecnológica de la institución y asegurar permanente asistencia a los usuarios de la Institución, constituyéndose además en:

a) El reformador y operador de la Infraestructura Informática de la DIGEIG y sus funciones deberán unificarse sin importar la localidad **donde se encuentren las demás instalaciones de la institución**, a partir de la fecha de aprobación de este Manual de Políticas.

b) A su vez está autorizado, para delimitar o definir los equipos y programas existentes y a ser adquiridos, para la ejecución de los procesos.

2.1. INFRAESTRUCTURA DE HARDWARE (EQUIPOS, DISPOSITIVOS Y APARATOS)

Responsabilidades de TIC:

La responsabilidad de **TI** ante la adquisición, instalación, mantenimiento y buen funcionamiento de los equipos, dispositivos de la Institución son las siguientes:

1. Deberá vigilar y llevar un inventario detallado de la infraestructura de Hardware de la Institución, acorde con las necesidades existentes de la misma.

2. Será la única responsable de hacer requerimientos de los activos informáticos que hayan sido proyectados, según las necesidades que se presenten en cada área de trabajo.

3. Deberá determinar la vida útil de los equipos de informática, con la finalidad de optimizar su uso.

4. Deberá participar en los contratos de adquisición de bienes y/o servicios, donde se incluyan equipos informáticos como parte integrante o complementaria de otros.

5. Deberá confirmar que los equipos de informática cumplan con las especificaciones indicadas en las solicitudes de compra, de no ser así se encargará de la devolución de los mismos.

6. Deberá realizar el mantenimiento técnico preventivo de todos los equipos informáticos de la Institución.

7. Será responsable de instalar los equipos y programas informáticos utilizados en la Institución.

8. Será responsable de evaluar el área física donde se instalara un nuevo equipo informático, confirmando que el área este óptima para la instalación de los mismos.

9. Verificará que los equipos tecnológicos tengan: disponibilidad de energía eléctrica, cableado estructurado y mantengan las condiciones físicas aceptables y adecuadas de temperatura, entre otros.

10. Deberá solicitar al Departamento Administrativo y Financiero la sinfraestructuras o servicios de disponibilidades eléctricas, previamente a la instalación de los equipos informáticos requeridos.

11. Velará por el adecuado uso de las instalaciones eléctricas requerida para el funcionamiento de los equipos tecnológicos.

12. Verificará el inventario de los equipos y programas informáticos que sean instalados, con la finalidad de llevar un control de los mismos.

13. Instalará todas las aplicaciones de los equipos y programas informáticos utilizados por la Institución.

14. Instruirá al Usuario sobre el uso y manejo adecuado de los equipos y programas informáticos instalados.

15. Verificará que los suplidores de programas de computadoras suministren los manuales correspondientes al funcionamiento de los equipos o programas especializados.

Responsabilidades de los usuarios

Los recursos informáticos asignados a los usuarios, deben usarse adecuadamente, con responsabilidad acorde a los siguientes lineamientos:

1. Solo podrán utilizar los equipos asignados para ejecutar las actividades o tareas Institucionales.

2. No podrán usar equipos tecnológicos personales como: laptops, dispositivo informático, etc., en el área de trabajo.

3. No podrá traer ni efectuar solicitudes a **TIC**, de reparación de equipos tecnológicos personales.

4. Solicitará a TIC un levantamiento de los equipos informáticos necesarios que requiera el área.

2.2. INFRAESTRUCTURA DE SOFTWARE (PROGRAMAS DE COMPUTADORA)

TIC, es responsable ante la institución de la instalación, actualización y modificación de los programas de computadoras utilizados por la misma.

a) Responsabilidad de TIC

1. Llevará inventario del software (programas) instalados en la Institución.

2. Velará porque todo el software instalado en la DIGEIG, este legalmente licenciado.

3. Tendrá la custodia y almacenamiento de todos los programas informáticos de la Institución.

4. Definirá los discos de Red de todas las áreas, para poder fragmentar el acceso a la información y una mejor organización.

5. Establecerá configuraciones automatizadas para que los usuarios guarden toda su información en los discos de red y se puedan facilitar los backups o copias de respaldo para seguridad.

6. Restringirá el acceso a los equipos tecnológicos fuera de horario de trabajo, a aquellos usuarios que no cuenten con una autorización previa de su superior inmediato para laborar fuera de horario.

Responsabilidades y/o Prohibiciones de los usuarios

El software existente en los equipos asignados a los usuarios estará regido por los siguientes lineamientos:

1. Está prohibido instalar y/o descargar juegos, videos, música ni aplicaciones de ningún tipo de las páginas del Internet, que no guarden relación con la DIGEIG.

2. Está prohibido tener en los discos de Red archivos que no tengan o guarden relación con la DIGEIG. Tales como:

   - MP3 (u otro formato de música)
   - EXE (archivos ejecutables)
   - MSI (archivos de instalación)
   - JPG; JPEG, GIF, BMP, PNG, ETC (imágenes)
   - INI (Archivos de configuración de instalación)
   - INF (Archivos de configuración de instalación)
   - DLL (librerías de archivos)
   - ZIP (archivos comprimidos, por lo regular son archivos personales y aplicaciones)
   - RAR (archivos comprimidos, por lo regular son archivos personales y aplicaciones)
   - ACE (Archivos comprimidos, por lo regular son aplicaciones alteradas (hacks) o descargas ilegales)
   - Entre otros

c) Está prohibido desinstalar o desactivar el Antivirus de su equipo, ya es de alto riesgo para la seguridad ante el peligro de los virus.

d) Deberá informar a TI, en caso de presentarse cualquier problema de virus en su equipo informático.

7. Los encargados deberán informar a TI cuales empleados de su área están autorizados para laborar fuera de horario de trabajo.

2.3. SEGURIDAD DEL ÁREA DE INFORMÁTICA

Todos los sistemas de informática deberán estar resguardados dentro del área asignada a TIC.

1. Los Usuarios o visitantes externos no podrán acceder al área destinada a TIC, sin la previa autorización del Encargado o acompañados de un empleado de la misma.

2. Solo podrán acceder al área de infraestructura informática los empleados de TIC.

2.4. CUSTODIA Y TENENCIA DE ACTIVOS INFORMÁTICOS

Responsabilidad de TIC

El uso indebido de los recursos informáticos puede afectar negativamente el funcionamiento de los equipos de oficina (PC), la red, los servidores por tanto TIC:

1. Custodiará todos los activos informáticos de la DIGEIG.

2. Asignará los equipos informáticos a todos los usuarios, de acuerdo con los requerimientos de las áreas.

3. Verificará que no le sea asignado un mismo activo informático a más de un Usuario.

4. Verificará que los Usuarios sean empleados regulares de la DIGEIG, así como contratistas externos, consultores, etc.

5. Llevará el control de los equipos informáticos portátiles (Laptop) asignados al personal gerencial que realice trabajos fuera de la Institución.

Responsabilidad de los usuarios

Al ser asignado un activo a un usuario todo lo concerniente al mismo será de su responsabilidad por lo cual:

1. Será responsable de la custodia de los equipos informáticos asignados (PC´s, monitores, teclados, impresoras, USB, etc.)

2. Notificará, vía electrónica o cualquier otra vía los inconvenientes o anomalías presentada con los equipos, accesorios, impresoras, sistemas, entre otros.

2.5. TRASLADO DE ACTIVOS INFORMÁTICOS FUERA DE LA DIGEIG.

Responsabilidad de TIC

Al momento de recibir una solicitud de las áreas, para el traslado de un equipo informático fuera de la institución, el compromiso de **TIC**, es el siguiente:

1. Verificará el estado de los equipos tecnológicos a ser entregados a las áreas, a través del ***Formulario Movimientos de Activos (Equipos)***, aprobado por el Departamento Administrativo y Financiero, para comprobar su salida y recepción en buen estado.

2. Verificará con el Departamento Administrativo y Financiero que el plazo otorgado a los equipos tecnológicos que serán utilizados fuera de la Institución no sea mayor de cinco (5) días.

Responsabilidad de los usuarios

El compromiso de los usuarios al momento de solicitar el traslado de un equipo informático fuera de la institución son los siguientes:

1. Deberá llenar completamente hasta la casilla "*Descripción del Equipo*" en el ***Form. DIGEIG/DAF-FMA "****Movimientos de Activos (Equipos)"* el cual debe ser aprobado por el Departamento Administrativo y Financiero.

2. Si el equipo tecnológico facilitado llegara a cumplir el plazo solicitado mediante el ***Form. DIGEIG/DAF-FMA*** deberá de efectuar otra solicitud la cual será evaluada por TIC, y el Departamento Administrativo y Financiero.

3. Deberá reportar cualquier daño o/y deterioro de los equipos informáticos facilitados.

2.6. ROBO O PÉRDIDA DE EQUIPO

1. A partir de las políticas definidas, el Departamento Administrativo y Financiero, determinara los pasos a seguir para el inventario de los equipos que se reporten como sustraídos.

2. El usuario de un equipo asignado deberá reportar dentro de veinticuatro (24) horas cualquier pérdida o sustracción del mismo, tanto al área Administrativa y Financiera como a la División de TIC, y estos a la Dirección Ejecutiva.

3. El Departamento Administrativo y Financiero se encargará de realizar los procesos pertinentes para que se establezca responsabilidad ante dicha pérdida.

4. Ante el caso de que se determine responsabilidad por parte del usuario de dicha perdida, se empoderara a la Dirección Ejecutiva como a la Departamento de Recursos Humanos de la institución para que se proceda con la aplicación de las medidas que se consideren correspondientes.

2.7. SOFTWARE (PROGRAMAS DE COMPUTADORA)

La procedencia del software utilizado y adquirido por la Institución, deberá estar acorde a las especificaciones técnicas que requiera la disponibilidad de la tecnología que disponga la institución.

Responsabilidad de TIC

1. Velará que el software incluya información de instalación y mantenimiento, para facilitar la labor del personal de soporte técnico.

2. Deberá requerirle a los proveedores, el entrenamiento en el uso de los software especializados.

2.8. MODIFICACIÓN O INSTALACIÓN DE SOFTWARE (PROGRAMAS)

Para satisfacer las necesidades de la Institución en cuanto a las modificaciones o Instalaciones de Software, que cumplan con los atributos de calidad adecuados, se definen las siguientes responsabilidades.

Responsabilidad de TIC

1. Evaluará todas las modificaciones propuestas al software (programas) actuales, tomando en cuenta el buen funcionamiento y costo en beneficio de la Institución.

2. Modificará o Instalará los sistemas de Información acorde a las necesidades de los usuarios, que busquen mejorar los procesos automatizados de la DIGEIG.

2.10. SOPORTE TÉCNICO A LOS EQUIPOS ASIGNADOS

Las responsabilidades descritas constituyen la normativa ante las solicitudes recibidas para la asistencia de soporte técnico a los equipos asignados a los usuarios.

Responsabilidad de TIC

1. Todas las solicitudes de Soporte Técnico, deberán ser remitidas, vía correo electrónico al ***Encargado de Informática***, quien le dará las instrucciones necesarias al personal técnico bajo su cargo.

2. Deberá dar un tiempo de respuesta a cada una de las solicitudes que hayan sido notificadas por los usuarios en un plazo no mayor de un (1) día laborable.

3. Cuando TI considere que el reporte de avería es mínimo, se podrá proceder con la reparación de inmediato.

4. Deberá de asegurar que el usuario este satisfecho con el servicio prestado.

5. Deberá recibir e instalar los equipos tecnológicos solicitados por las diferentes áreas de la Institución.

6. Se encargará de revisar todos los equipos, accesorios, programas, entre otros.

7. Dará soporte técnico solamente a los equipos informáticos de la DIGEIG.

Responsabilidad de los usuarios

La responsabilidad de los usuarios ante la solicitud de asistencia del área de informática es la siguiente:

a) Solicitará, vía correo electrónico a **TI**, las solicitudes de modificaciones o servicio técnico, así como cualquier anormalidad en su equipo, con copia a su superior inmediato.

b) Solicitará todos los servicios de soporte tecnológicos, a través de correo electrónico con copia a su superior inmediato. En caso que el equipo no responda, será efectuada, vía telefónica.

2.11. PLAN DE CONTINGENCIA

El propósito de un Plan de Contingencia en la informática, busca reanudar las actividades ante un desastre a fin de que la institución pueda mitigar los efectos del mismo, para lo cual **TIC**:

Responsabilidad de TIC

1. Deberá tener siempre en caso de fallas un Plan de Contingencia que permita recuperar en corto tiempo todas las informaciones contenidas en la Red.

2. Deberá programar una vez al año un simulacro, con la finalidad de examinar la efectividad del Plan de Contingencia establecido.

Responsabilidad de los usuarios

1. Deberán respetar los lineamientos establecidos en el Plan de Contingencia y abocarse a colaborar con el mismo.

2. Ante la advertencia de un desastre deberá apoyar a TI en la protección de los equipos.

2.12. ASIGNACIÓN DE USUARIO

El objetivo de la asignación de usuarios corresponde a establecer el acceso a los equipos informáticos de la institución, a aquellas personas que forman parte de la misma, otorgándole el derecho y el privilegio de inicio de sesión en la red de la institución.

Responsabilidad de TIC

1. Recibirá las informaciones requeridas para evaluar las solicitudes de creación o modificación de usuarios en los sistemas de información por parte de la Departamento de Recursos Humanos.

2. Deberá crear el usuario de los nuevos empleados, con la finalidad de otorgarle el acceso al dominio de la red de la Institución y que permita asociarlo con las acciones realizadas en el sistema.

3. Designar a los nuevos usuarios inicialmente, una contraseña temporal para el ingreso al sistema de la DIGEIG.

4. Las contraseñas temporales deben ser únicas para cada usuario.

5. Las contraseñas temporales serán entregadas de manera personal a los nuevos usuarios por el personal asignado del área de TIC, evitando el uso de correo electrónico.

6. Para el cambio de contraseña se debe solicitar a la persona una identificación que permita verificar la identidad de la misma.

7. Deberá informar al Departamento de Recursos Humanos la creación de nuevos usuarios en el dominio de la red.

8. Velará por que los datos de los usuarios en el dominio de la data serán los siguientes: el primer nombre seguido del signo de punto y luego el primer apellido del empleado. *Ejemplo: Ignacio.Torres.*

9. Programará el sistema para que le notifique cada Ciento veinte (120) días a los usuarios el registro de cambio de contraseña.

10. TIC deberá asignar una cuenta temporal a los servidores que ingresen a la DIGEIG de manera temporal (consultores, asesores, auditores, entre otros), luego de haber recibido previamente notificación escrita por parte del Departamento de Recursos Humanos, indicando el tiempo de duración de los mismos.

11. Deberá en función de las licencias disponibles y de la información suministrada por Recursos Humanos, evaluar la posibilidad de aprobar las solicitudes de creación o modificación de usuarios en los sistemas de informática.

12. Deberá monitorear toda anomalía detectada en la aprobación de creación o modificación de usuarios en el sistema de información.

13. Los servidores institucionales mantendrán activa la data informática de sus equipos tecnológicos durante los períodos de disfrute de vacaciones o licencias médicas.

14. Se deshabilitará los usuarios de los empleados que hayan finalizado su contrato de trabajo, según información remitida, vía correo electrónico por parte de Recursos Humanos.
15. El Departamento de Recursos Humanos deberá notificar al Encargado de TIC, la desvinculación de un servidor, tres (3) días antes de darlo a conocer de manera oficial.

16. Suspenderá el permiso a la red a todo empleado que se encuentre bajo investigación interna por haber cometido alguna infracción en el uso de la tecnología e informara al superior inmediato de dicha suspensión.

Responsabilidad de los usuarios

1. Ningún usuario podrá solicitar directamente a TI, la creación de acceso a la red de la institución.
2. Deberá asegurarse del cierre de manera correcta de la sesión de usuario al momento de finalizar sus labores.

3. No permitirá a persona ajena a la institución el acceso a su Equipo informático asignado.

4. Deberá cambiar la contraseña provisional tan pronto tenga acceso al sistema tecnológico de la DIGEIG.

2.13. PRIVILEGIOS Y ACCESOS DE LOS SISTEMAS

El área de TIC deberá asegurar y tener control al acceso autorizado otorgado a los usuarios, para prevenir el acceso no autorizado a los sistemas de informática de la DIGEIG, a los fines deberá:

1. Realizar un levantamiento trimestral sobre las asignaciones de privilegio otorgado a los usuarios, para el acceso a: Carpetas compartidas, páginas de internet, programas e instalación de programas, entre otros.
2. Controlar el uso y asignación de privilegios otorgados a los usuarios.
3. Los Encargados de áreas deberán remitir vía correo electrónico, al Delegado de TIC, los accesos que desean retirar u otorgar a los servidores bajo sus respectivas dependencias, según lo indicado en la estructura organizacional de la DIGEIG.
4. Monitorear y reportar el uso inapropiado de los privilegios y recursos tecnológicos provistos.
5. Otorgar los privilegios acorde a las tareas propias de los usuarios y aprobación escrita, del superior inmediato, vía correo electrónico.
6. Implementar mecanismos que eviten el acceso no autorizado a otros recursos manejados por los usuarios de otras áreas.
7. Desactivar las cuentas de red de los usuarios que no fueron accedidas durante un período mínimo de tres (3) meses.
8. Eliminar las cuentas de correo electrónico de los usuarios inmediatamente sean desvinculados de la institución, previo respaldo de las informaciones remitidas por el área de Recursos Humanos de la DIGEIG.

9. Modificar o revocar los permisos de acceso de los usuarios por motivo de: promoción, desvinculación o cambios de actividades propias del cargo y notificadas por la vía escrita correspondiente, por el Departamento de Recursos Humanos.

10. Los permisos de acceso deben ser revisados y reasignados cuando se modifica la condición laboral del usuario, por motivo a una promoción, degradación o terminación de empleo.

2.14. SEGURIDAD Y RESPALDO DE LAS INFORMACIONES

TIC ha previsto las siguientes medidas de seguridad y respaldo de las informaciones institucional con el propósito de proteger y normar los niveles de acceso y confidencialidad, a ser observadas y cumplidas por los servidores, así como el personal en servicio temporal, con la finalidad de normal en el uso y manejo de los activos de informáticas de la organización.

Responsabilidad de TIC

1. Deberá establecer un plan de análisis de riesgo institucional.

2. Velará para que los equipos estén libres de vulnerabilidades a fin de reducir los riesgos a que puedan someterse.

3. Conformara un equipo de seguridad de la información con un miembro de cada departamento que pueda velar por la aplicación de las medidas de seguridad.

4. Velará por la seguridad de la información que se genere día a día.

5. Deberá almacenar en la bóveda o archivo fuerte ubicado en la oficina del director ejecutivo todos los backups o copia de respaldo para seguridad.

6. Deberá realizar semanalmente el Backups o copia de respaldo para seguridad de las informaciones contenidas en los sistemas informáticos de la DIGEIG.

7. El Encargado de TIC deberá asignar de manera fija a uno de los servidores bajo su responsabilidad la ejecución del Backups o copia de respaldo para seguridad de las informaciones contenidas en los sistemas informáticos de la DIGEIG.

8. Deberá realizar un Backups a los equipos informáticos de los usuarios desvinculados de la DIGEIG, previa notificación oficial del Departamento de Recursos Humanos.

9. Se encargará de monitorear el uso indebido de las informaciones contenidas y manejadas por los usuarios en todos los equipos tecnológicos de la institución.

10. Velará por la instalación de programas que garanticen la seguridad de la información en los archivos compartidos.

11. Asegurará que los encargados de áreas que manejan plataformas de servicios de datos electrónicos, se rijan por las políticas establecidas en este Manual de Políticas.

12. Realizará auditorías continuas a las carpetas compartidas en el disco público, para determinar responsabilidad en el manejo de las informaciones como borradas.

13. Se encargará de la destrucción Discos Duros al momento de que se vallan a descargar un equipo en caso de que este dañado, si funciona puede reutilizarse.

Responsabilidad de los usuarios

1. Solo utilizará el correo electrónico Institucional para recibir y/o enviar correspondencia relacionadas con su trabajo.

2. Los usuarios deberán revisar y responder día a día todos los correos electrónicos internos como externos relacionados con las actividades de la Institución.

3. Deberá manejar todas las informaciones institucionales exclusivamente a través de los correos internos que dispone la organización.

4. Se asegurará de salvar y proteger la información que maneja.

5. No podrá transferir a terceros informaciones consideradas como confidenciales sin autorización previa.

6. Guardará la información de trabajo en los discos de red asignados por usuario, garantizando así la integridad de la información.

7. Deberá crear una contraseña privada, con la finalidad de acceder a los datos, servicios y programas de su equipo, asegurándose que tenga las siguientes características:
    - Ocho (8) o más caracteres
    - Combinar letras mayúsculas, minúsculas y números
    - Fácil de recordar y difícil de adivinar

8. No deberá compartir la contraseña creada para acceder al Equipo Informático asignado
9. No hará uso indebido de la información institucional que maneja.
10. Deberá guardar los datos importantes en la carpeta de "My Documents o Escritorio" para realización de copia de seguridad.
11. Guardará únicamente el contenido multimedia en la carpeta compartida llamada "MEDIA".
12. Deberán asegurarse al finalizar la jornada laboral:

    - Cerrar las aplicaciones una vez terminado el trabajo en ellas
    - Desconectarse de las aplicaciones o servidores una vez finalizado el trabajo.

13. Deberán proteger sus equipos informáticos de trabajo que gestionan información sensible con salva pantalla controlado por contraseña.
14. Los usuarios que tengan asignados y/o utilicen equipos móviles tecnológicos (laptop, mini-laptop, tabla) propiedad de la DIGEIG, deberán:

    - Desactivar los mismos al momento de encontrarse en lugares públicos, realizando actividades desvinculadas a la institución.
    - Prescindir de conectarse a redes inalámbricas no confiables o desconocidas para transmitir información sensible.
    - Solo utilizar los equipos en tareas propias del cargo.
    - Para transmitir informaciones consideradas como relevantes.

2.16. SEGURIDAD Y ACCESO ÁREA DE EQUIPOS INFORMATICOS

1. Los equipos informáticos con equipamiento de hardware, software y otros servicios de cómputos, estarán ubicados en el área asignada para Tecnología de la Información y Comunicaciones, TIC, quien se encarga del resguardo de los mismos.

2. El área de TIC destinadas para equipos contendrá las siguientes herramientas tecnológicas:

    - Servicios con los sistemas de información
    - Servidores que manejan los Sistemas de Respuesta de Voz interactiva (SVR) o comunicación de voz
    - Servidores para correo electrónico, archivo, dominio de usuarios, control de internet, entre otros.
    - Cableado de red LAN y WLAN
    - Equipos de Comunicaciones (switches, routers, firewall, para las redes LAN y WLAN)
    - Dispositivos para controlar la seguridad de la red hacia el acceso externo.

3. Solo estará permitida la entrada al personal autorizado mediante sistema de huella digital, quienes protegerán los equipos informáticos.

4. El sistema de información instalado para inspeccionar el acceso del personal autorizado estará en la entrada del área de TIC y registrará automáticamente, fecha, hora de entrada y salida de los mismos.
5. Los servidores o personal ajeno al área autorizados para realizar algún trabajo en el área de TIC, deberán estar acompañadas en todo momento de un servidor autorizado.

6. El Encargado de TIC, será responsable de autorizar el acceso al área.

7. El área donde se encuentren los equipos informáticos deberá estar provista de herramientas para minimizar los riesgos de daños contra los equipos: extintores, deshumidificador, alarmas, sistemas automático contra incendio, UPS, aire acondicionado, sensores contra humedad relativa del aire, líquido y temperatura, entre otros.

8. Está prohibido comer, beber o fumar en el área destinada para los equipos tecnológicos.

9. Está prohibido tener materiales o líquidos inflamables en el área destinada

10. El área de TIC. Dispondrá de un plan de mantenimiento de los equipos a llevarse a cabo de manera trimestral.

2.17. MANEJO DE IMPRESORAS

Buscando regular la impresión de documentos innecesarios por parte de los usuarios de las impresoras asignadas y establecer un control interno, se han establecido los siguientes lineamientos:

Responsabilidad de TIC

1. Se encargará de monitorear el uso de las impresoras de red.

2. Coordinara con los encargados de área, el personal que puede tener acceso a las impresoras de red como a las impresoras disponibles en los departamentos.

3. Las impresoras a color solo serán utilizadas para imprimir documentos que exclusivamente requieran ser impresos a color, no para hacer pruebas ni borradores.

4. Coordinara con los encargados de las áreas la concientización del personal para su área sobre el uso indebido de las impresoras.

5. No se imprimirán trabajos que no tengan relación con la institución

6. Cada área solicitara el papel de impresión a utilizar y será responsable del uso del mismo.

7. Solo se utilizaran para impresiones, tóneres y tintas originales.

8. Solo tendrán acceso al uso de impresoras en red fuera de horario de trabajo, los encargados de áreas y el personal autorizado por ellos.

9. Reportara bajo informes el uso indebido de las impresoras.

10. Se limitara el horario de uso de equipos en red, para asegurar que el mismo se utilice exclusivamente para asuntos de trabajo.

Responsabilidad de los usuarios

1. No podrán imprimir documentos personales, ni a terceras personas en los equipos de la institución.

2. Deberá contar con la previa autorización de su superior inmediato vía correo electrónico, para utilizar impresoras fuera de horario de trabajo.

3. Deberá triturar los borradores impresos de trabajos considerados como confidenciales.

4. Los "borradores" de trabajos serán impresos bajo el mandato de economía de tinta.

5. Podrá utilizar para borradores de trabajo, hojas recicladas que no contengan información considera como confidencial

6. Hará buen uso del material de trabajo disponible en el área para sus impresiones.

2.18. ACCESO AL INTERNET

El Internet es un medio importante y eficiente de comunicación, por lo cual es importante lograr un uso equitativo y eficiente del mismo, por tanto TI velará porque se cumplan los siguientes lineamientos:

Responsabilidad de TIC

1. Se asegurará de coordinar con los encargados de áreas, las páginas de Internet a las que puede tener acceso el personal bajo su cargo, bloqueando aquellas páginas que no sean relevantes para el desempeño de las funciones.

2. Deberá monitorear el acceso de las páginas de internet por parte del personal e informar cualquier violación de acceso, vía correo electrónico a los encargados de las áreas.

3. Deberá informar vía correo electrónico al encargado de área, los casos continuos de violación de acceso a internet a páginas no relacionadas con el trabajo institucional como por ejemplo: de juegos, de música, descargas, videos, entre otras; con la finalidad de que se tomen las medidas de lugar.

4. Dará seguimiento a la plataforma de servicios de internet, notificando a las áreas los inconvenientes presentados en la misma.

Responsabilidad de los usuarios

1. Está prohibido la transmisión y/o, descarga de material obsceno o pornográfico, que contenga amenazas o cualquier tipo de información que atente contra la moral o buenas costumbres.

2. Durante la jornada laboral podrá acceder a las páginas de internet o redes sociales propias de la DIGEIG

3. Deberá abstenerse de usar las redes sociales y demás medios Web durante la jornada laboral establecida en la DIGEIG, para propósitos personales. Entre estas páginas las siguientes:

    - YouTube
    - Facebook
    - Twitter
    - De descarga de torrents o de compartir archivos.
    - Redes sociales
    - Otras de igual finalidad

4. Solo tendrá acceso a páginas de internet: bancarias, educativas, periodísticas e institucionales.

III. IMPREVISTOS

Los casos que se presenten y que estén vinculados al trabajo y no estén contemplados en este Manual de Políticas, serán atendidos o resueltos por la Dirección Ejecutiva de la Institución.

IV. VERSIÓN

Esta es la tercera (3ra.) actualización aplicada a este Manual de Políticas de TIC, siendo la segunda (2da.) en el mes de octubre del año 2012, donde solo se modificó el nombre de la institución, el logo institucional y la fecha de revisión en la portada.

Esta tercera modificación contiene algunas de las directrices normadas en la NORTIC A1, y otros lineamientos internos establecidos en la Estructura Organizativa de la DIGEIG, aprobada por el Ministerio de Administración Publica, MAP.

Este Manual deberá estar firmado por los Encargados de las áreas responsables y la Dirección Ejecutiva de la DIGEIG, así como estar todas sus páginas selladas con el sello oficial de la institución como medida de control interna.

DIRECCIÓN GENERAL DE ÉTICA E INTEGRIDAD GUBERNAMENTAL

Elaboración : **Dpto. Planificación y Desarrollo**

Ing. Joel Leonardo Peña

Lic. Karen Machuca

Revisión : **División de Tecnología de la Información y Comunicación, TIC**

Ing. Dahiri Espinosa

Aprobación : **Dirección Ejecutiva**

Lic. George Koury

Dirección General de Ética e Integridad Gubernamental Presidencia de la República DIGEIG RNC 430032069 Sto. Dgo., R.D.