

# POLÍTICAS DE TECNOLOGÍA

*Lenín*



PRESIDENCIA DE LA REPÚBLICA  
*POLÍTICAS DE TECNOLOGÍA DE LA PRESIDENCIA*

**ÍNDICE**

|                                                                                          |    |
|------------------------------------------------------------------------------------------|----|
| POLÍTICAS DE TECNOLOGÍA DE LA PRESIDENCIA DE LA REPÚBLICA .....                          | 1  |
| OBJETIVO .....                                                                           | 1  |
| ALCANCE .....                                                                            | 1  |
| JUSTIFICACIÓN .....                                                                      | 1  |
| INCUMPLIMIENTO .....                                                                     | 2  |
| REVISIÓN .....                                                                           | 2  |
| DEFINICIONES .....                                                                       | 3  |
| 1. SEGURIDAD INFORMÁTICA .....                                                           | 5  |
| 1.1 POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DEL PERSONAL .....                               | 5  |
| POLÍTICA .....                                                                           | 5  |
| Obligaciones de los usuarios .....                                                       | 5  |
| Entrenamiento en seguridad informática .....                                             | 5  |
| Medidas disciplinarias .....                                                             | 5  |
| 1.2 POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTE .....                          | 6  |
| POLÍTICA .....                                                                           | 6  |
| Resguardo y protección de la información .....                                           | 6  |
| Controles de acceso físico .....                                                         | 6  |
| Seguridad en áreas de trabajo .....                                                      | 7  |
| Protección y ubicación de los equipos .....                                              | 7  |
| Mantenimiento de equipos .....                                                           | 7  |
| Pérdida de Equipo .....                                                                  | 7  |
| Uso de dispositivos especiales .....                                                     | 8  |
| Daño del equipo .....                                                                    | 8  |
| Protección Física .....                                                                  | 8  |
| 1.3 POLÍTICAS Y ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO ..... | 9  |
| POLÍTICA .....                                                                           | 9  |
| Uso de medios de almacenamiento .....                                                    | 9  |
| Instalación de software .....                                                            | 9  |
| Identificación de incidentes .....                                                       | 10 |
| Administración de la configuración .....                                                 | 10 |
| Seguridad para la red .....                                                              | 10 |
| Uso del Correo electrónico .....                                                         | 10 |
| Controles contra código malicioso .....                                                  | 11 |
| Internet .....                                                                           | 12 |
| 1.4 POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESO Y SEGURIDAD LÓGICA .....               | 12 |
| POLÍTICA .....                                                                           | 12 |
| Controles de acceso lógico .....                                                         | 12 |
| Administración de privilegios .....                                                      | 13 |
| Equipo desatendido .....                                                                 | 13 |
| Administración y uso de Claves .....                                                     | 14 |
| Control de accesos remotos .....                                                         | 14 |
| Desarrollo y adquisición de sistemas .....                                               | 14 |
| 1.5 POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA .....                | 15 |
| POLÍTICA .....                                                                           | 15 |
| Derechos de propiedad intelectual .....                                                  | 15 |
| Revisiones del cumplimiento .....                                                        | 15 |
| Violaciones de seguridad Informática .....                                               | 15 |
| 2. USO DE LOS RECURSOS INFORMÁTICOS .....                                                | 16 |
| 2.1 POLÍTICAS DE ADQUISICIÓN Y USO DE LOS RECURSOS INFORMÁTICOS .....                    | 16 |
| POLÍTICA .....                                                                           | 16 |
| Adquisición de Hardware, Software y Servicios Tecnológicos .....                         | 16 |
| Uso de los Recursos Tecnológicos .....                                                   | 16 |
| Sólo para el área de Tecnología .....                                                    | 17 |
| Gestión de proyectos de tecnología .....                                                 | 18 |
| 3. OBSOLESCENCIA DE EQUIPOS INFORMÁTICOS .....                                           | 18 |
| POLÍTICA .....                                                                           | 18 |

## **POLÍTICAS DE TECNOLOGÍA DE LA PRESIDENCIA DE LA REPÚBLICA**

El presente documento tiene como finalidad definir y poner en conocimiento de todos los usuarios las políticas y estándares por la Secretaría General de la PRESIDENCIA DE LA REPÚBLICA, mismas que deberán ser observadas por los usuarios internos, servidores públicos, usuarios externos y personeros de la Dirección de Tecnología, directos clientes de recursos y servicios de tecnología.

### **OBJETIVO**

Establecer las Políticas de Tecnología que deberán ser aplicadas de forma obligatoria, por todos los servidores públicos de la PRESIDENCIA DE LA REPUBLICA independientemente de la modalidad de contratación que tengan, de manera de precautelar el buen uso de los recursos y servicios informáticos que son provistos para el desempeño de sus funciones y de la información que por ellos se transmite.

### **ALCANCE**

Las políticas deberán ser observadas de manera obligatoria y permanente, por todos los servidores públicos independientemente de la modalidad de contratación, lo que permitirá el buen uso de las herramientas informáticas provistas para su desenvolvimiento y tareas a cumplir; esto contempla el equipo de cómputo, sistemas, aplicaciones y servicios informáticos de la PRESIDENCIA DE LA REPÚBLICA.

### **JUSTIFICACIÓN**

La Dirección de Tecnología, es el ente técnico que asesora, administra, gestiona recursos y provee soluciones en el área tecnológica. Podrá autorizar a otras instancias a ejecutar labores en apego a las normas y políticas establecidas. El objetivo es regular y estandarizar los recursos tecnológicos de tal forma que se minimicen los riesgos de interrupción de servicios.

La Dirección de Tecnología, dentro de sus funciones, está facultada para definir políticas y estándares generales y específicos en materia de su competencia, observando además lo que establecen las Normas de Control Interno de la Contraloría General del Estado (Norma 410-04) para las áreas de Sistemas de Información, mismas que son aprobadas por la Máxima Autoridad de la Institución previa a su puesta en vigencia.

Las políticas de seguridad que se establecen en las áreas de informática tienen como objeto primordial establecer medidas tanto en el aspecto técnico como de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos, sistemas de información, comunicaciones unificadas) y personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de cómputo de la PRESIDENCIA DE LA REPÚBLICA.

Los sistemas de información y comunicación que se diseñen e implanten, deberán concordar con los planes estratégicos y operativos, debiendo ajustarse a sus características y necesidades y al ordenamiento jurídico vigente, según establece las Normas de Control Interno de la Contraloría General del Estado (500 INFORMACIÓN Y COMUNICACIÓN).

La PRESIDENCIA DE LA REPÚBLICA, a través de la Dirección de Talento Humano, en coordinación con la Dirección de Tecnología, es quien dará a conocer estas políticas de seguridad internamente.

La Dirección de Tecnología puede modificar, agregar guías particulares complementarias de acuerdo a su naturaleza y funciones. Además será el responsable de cumplir y de hacer cumplir estas políticas.

## **INCUMPLIMIENTO**

En el caso de darse cualquier tipo de incumplimiento a las políticas, dependiendo de su naturaleza y gravedad, será objeto de la sanción pertinente que será aplicada por el área competente, conforme lo que establezca la normativa vigente y el reglamento interno emitido por la Dirección de Talento Humano de la PRESIDENCIA DE LA REPÚBLICA.

## **REVISIÓN**

Frecuencia de revisión de las políticas:

La Secretaría General revisará las políticas del presente documento, con una frecuencia anual y para ello determinará un plan.

Las políticas serán revisadas por la Dirección de Tecnología con una frecuencia semestral y para ello, especificará su alcance y organización.

El seguimiento al cumplimiento de las políticas será permanente y para ello, cada Jefatura de la Dirección de Tecnología será responsable de emitir los informes mensuales.

## DEFINICIONES

|                               |                                                                                                                                                                                                                      |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Almacén:</b>               | Lugar donde se guarda y administra todos los bienes de la Institución.                                                                                                                                               |
| <b>Autenticación:</b>         | O autenticación es el acto de establecimiento o confirmación de alguien como auténtico. La autenticación de una persona a menudo consiste en verificar su identidad.                                                 |
| <b>BCP:</b>                   | Plan de Continuidad del Negocio ( <b><i>Bussines Continuity Plan</i></b> ).                                                                                                                                          |
| <b>Caracteres Especiales:</b> | Aquellos que no son ni números ni letras. Ejemplo: ¿, %, \$, ?, *, >, <, etc.,.                                                                                                                                      |
| <b>Caballo de Troya:</b>      | Software malicioso que al ejecutarlo ocasiona daños, permitiendo la administración remota a un usuario no autorizado                                                                                                 |
| <b>Centro de Datos:</b>       | Cualquier oficina que cuente con equipamiento de cómputo.                                                                                                                                                            |
| <b>Clave de Acceso:</b>       | Conjunto de caracteres que permite el acceso de un usuario a un recurso informático ( <b><i>password</i></b> /contraseña).                                                                                           |
| <b>CPU:</b>                   | Unidad Central de Procesamiento (Central Processing Unit), microprocesador electrónico, componente principal del computador; por extensión, se le conoce también como CPU al equipo que contiene al microprocesador. |
| <b>DRP:</b>                   | Plan de Recuperación de Desastres ( <b><i>Disaster recovery plan</i></b> ).                                                                                                                                          |
| <b>DT:</b>                    | Dirección de Tecnología                                                                                                                                                                                              |
| <b>Dueño del Proceso:</b>     | Persona responsable de definir accesos dentro de las actividades de cada usuario.                                                                                                                                    |
| <b>Encriptado:</b>            | Información que está codificada.                                                                                                                                                                                     |
| <b>Equipo Desatendido:</b>    | Computador que se encuentra fuera de línea, no conectado a ninguna red.                                                                                                                                              |
| <b>FTP:</b>                   | Protocolo para transferencia de archivos ( <b><i>File Transfer Protocol</i></b> ).                                                                                                                                   |
| <b>ID Usuario:</b>            | Identificador de Usuario para accesos a los recursos informáticos.                                                                                                                                                   |
| <b>Gusano:</b>                | Software malicioso que tiene la propiedad de duplicarse a sí mismo, utilizando partes automáticas de un sistema operativo.                                                                                           |
| <b>Política:</b>              | Documento con las directrices y recomendaciones que orientan en el uso adecuado de los recursos informáticos y las nuevas tecnologías, para obtener el mayor provecho y evitar el uso indebido de las mismas.        |

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Privilegios:</b>         | Derechos de acceso que se otorga a un usuario para acceder a los recursos informáticos.                                                                                                                                                                                                                                                                                                                                     |
| <b>Recurso informático:</b> | Cualquier componente físico o lógico de un sistema de información.                                                                                                                                                                                                                                                                                                                                                          |
| <b>Release:</b>             | Liberación de mejoras o actualizaciones de un sistema.                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Resetear Clave:</b>      | Volver a otorgar y habilitar una clave de acceso.                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Screensaver:</b>         | Protector de pantalla o salvapantallas, programa informático diseñado para activarse después de un tiempo que la computadora no se está usando, mostrando una imagen preestablecida. Cuando se configura con clave, se utiliza para seguridad de la información.                                                                                                                                                            |
| <b>SQL Injection:</b>       | Es un método de infiltración de código intruso, para realizar consultas a una base de datos.                                                                                                                                                                                                                                                                                                                                |
| <b>TIC:</b>                 | Tecnologías de Información y Comunicaciones, conjunto de teorías y de técnicas que permiten el aprovechamiento práctico de la Información.                                                                                                                                                                                                                                                                                  |
| <b>Upgrade:</b>             | Mejora o ampliación de las características de un recurso informático.                                                                                                                                                                                                                                                                                                                                                       |
| <b>Usuario:</b>             | Cualquier persona (servidor público o no) que haga uso de la infraestructura y servicios de las tecnologías de información proporcionadas por la DT, tales como equipos de cómputo, sistemas de información, redes de telemática, dispositivos.                                                                                                                                                                             |
| <b>Versionamiento:</b>      | Código secuencial que permite mantener un control de las actualizaciones o cambios en las versiones de los programas informáticos.                                                                                                                                                                                                                                                                                          |
| <b>Virus informático:</b>   | Programa ejecutable o pieza de código con habilidad de ejecutarse y reproducirse, regularmente escondido en documentos electrónicos, que causan problemas como: ocupar espacio de almacenamiento, destrucción de datos y reducción del desempeño de un equipo de cómputo. <b>software</b> malicioso, que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. |

## 1. SEGURIDAD INFORMÁTICA

Este capítulo contiene cinco políticas generales de seguridad para usuarios de informática, con sus respectivos estándares que consideran los siguientes puntos:

- Seguridad de Personal.
- Seguridad Física y Ambiental.
- Administración de Operaciones de Cómputo.
- Controles de Acceso Lógico.
- Cumplimiento.

La Dirección de Tecnología será quien suministre las medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas, así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad de la infraestructura y sistemas de la PRESIDENCIA DE LA REPÚBLICA. Sin embargo, debido a la amplitud y constante innovación de los mecanismos de ataque, se buscará siempre llegar al más alto porcentaje de eficiencia y efectividad de manera de garantizar la seguridad, cuidando siempre mantener altos niveles de calidad en el servicio.

### 1.1 POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DEL PERSONAL

#### POLÍTICA

***Todo usuario interno de bienes y servicios informáticos, debe firmar un convenio en el que acepte las condiciones de confidencialidad, para el uso adecuado de los recursos informáticos y de información de la PRESIDENCIA DE LA REPÚBLICA, con estricto apego en el cumplimiento de lo establecido en el Manual de Políticas del Área de Tecnología para su caso.***

#### Obligaciones de los usuarios

- Es responsabilidad de los usuarios internos de recursos y servicios informáticos, el dar cumplimiento a las Políticas, bajo el compromiso de aceptación como servidores públicos de la PRESIDENCIA DE LA REPÚBLICA.

#### Entrenamiento en seguridad informática

- Todo servidor público que ingrese a la PRESIDENCIA DE LA REPÚBLICA, deberá contar con la inducción sobre las Políticas del Área de Tecnología para usuarios, a través de la Dirección de Talento Humano, donde se darán a conocer las obligaciones para los usuarios, así como las sanciones a las que estarán expuestos en caso de cualquier tipo de incumplimiento, conforme la normativa vigente.

#### Medidas disciplinarias

- El momento en que la Dirección de Tecnología evidencie el incumplimiento de las políticas, remitirá el reporte correspondiente a la Secretaría General para que proceda conforme su competencia y atribuciones.
- Se consideran violaciones graves el daño, robo, seccionamiento, duplicación, divulgación de información confidencial de la PRESIDENCIA DE LA REPÚBLICA, o que se haya encontrado responsabilidad en el cometimiento de un delito informático, ya sea de manera directa o como cómplice o encubridor de alguna persona.

## 1.2 POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTE

### POLÍTICA

***Dentro del control del acceso físico, tanto para el personal como de terceros, se permitirá el ingreso a las instalaciones, áreas restringidas de la PRESIDENCIA DE LA REPÚBLICA y al Centro de Datos, exclusivamente a personas autorizadas, con el fin de salvaguardar las instalaciones en general y la información de la PRESIDENCIA DE LA REPÚBLICA.***

### Resguardo y protección de la información

- Todo usuario deberá reportar de forma inmediata a la Dirección de Tecnología, cuando detecte que existan riesgos reales o potenciales para equipos de cómputo que tengan asignados; dentro de ellos podemos mencionar fugas de agua, cortocircuitos, derrame de líquidos, conatos de incendio, readecuaciones físicas, entre otros.
- Todo usuario tiene la obligación de proteger los discos, memorias y en general dispositivos externos de almacenamiento de información y equipos de comunicación, que se encuentren bajo su responsabilidad y contengan información, especialmente la confidencial, evitando sean mal utilizados.
- Es responsabilidad, principalmente del usuario, evitar en todo momento la fuga de información de la PRESIDENCIA DE LA REPÚBLICA, bajo cualquier modalidad y que se encuentre almacenada en los equipos de cómputo que tengan asignados.

### Controles de acceso físico

- Cualquier persona que tenga acceso a las instalaciones de la PRESIDENCIA DE LA REPÚBLICA, deberá registrar y/o autorizar al momento de su entrada, el equipo de cómputo, equipo de conectividad, medios de almacenamiento y herramientas que no sean propiedad de la Institución, los cuales quedarán reportadas en una bitácora que será responsabilidad de la recepción/seguridad. En caso contrario, antes de abandonar las instalaciones de la PRESIDENCIA DE LA REPÚBLICA, deberá tramitar la autorización de salida correspondiente, con el responsable del área visitada.
- El ingreso de terceras personas estará plenamente identificado, controlado y vigilado durante el acceso, mediante la entrega de una credencial que les será asignada por el personal de seguridad de acceso al edificio.
- Las computadoras personales, las computadoras portátiles y cualquier activo de tecnología de información, podrá salir de las instalaciones de la PRESIDENCIA DE LA REPÚBLICA para fines de trabajo o mantenimiento, únicamente con la autorización del Jefe Inmediato.
- Para el caso de equipos portátiles cuya salida sea frecuente por razones propias de las funciones del servidor público a quien está asignado, se generará un documento único donde constará: el nombre del servidor público, la justificación de la necesidad de sacar el equipo, las características del mismo, tales como tipo de equipo, marca, modelo, número de serie. Este documento deberá ser requerido por la recepción/seguridad del edificio, quienes tienen la responsabilidad de verificar que se trate del mismo equipo autorizado a salir.
- En lo referente a los sistemas fijos de comunicaciones, estarán protegidos con la infraestructura adecuada de manera que el usuario no tenga acceso físico directo. Esto incluye el equipo activo y los medios de comunicación.



### **Seguridad en áreas de trabajo**

- El Centro de Datos de la PRESIDENCIA DE LA REPÚBLICA es área restringida, por lo que sólo el personal autorizado por la Dirección de Tecnología puede acceder a él.

### **Protección y ubicación de los equipos**

- Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Dirección de Tecnología. En caso de requerir algún servicio, deberá solicitarlo al área de Soporte Técnico.
- El Almacén será el encargado de recabar la firma de actas del usuario informático como responsable de los activos informáticos que se le asignen y de verificar que se encuentren en la ubicación autorizada por la Dirección de Tecnología.
- Cuando se requiera realizar cambios múltiples del equipo de cómputo, derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con la anticipación suficiente a la Dirección de Tecnología.
- Para aquellos servidores públicos que posean laptops, los equipos no deberán quedar en el escritorio y deberán guardarse con la seguridad respectiva al momento de retirarse de su puesto de trabajo.
- Queda prohibido que el usuario abra o desarme los equipos de cómputo directamente o con la intervención de terceros.
- Los equipos asignados a los usuarios no deben permanecer físicamente en un lugar distinto al dispuesto dentro de las áreas de la PRESIDENCIA DE LA REPÚBLICA, menos aún si contienen información relevante o confidencial, para ellos mismos o para la Institución, salvo los casos autorizados.

### **Mantenimiento de equipos**

- Únicamente el personal perteneciente o autorizado por la Dirección de Tecnología, podrá llevar a cabo el mantenimiento y/o reparaciones a equipos informáticos, por lo que los usuarios deberán, ante cualquiera de estos casos, solicitar identificación del personal autorizado antes de permitir el acceso a sus equipos.
- Los usuarios deberán asegurarse de respaldar de manera frecuente la información que consideren relevante, sobre todo cuando el equipo sea enviado a mantenimiento y/o reparación, así como de borrar aquella información sensible que se encuentre en el equipo, previniendo así la pérdida o fuga involuntaria de información, derivada de este proceso.
- Para el caso en que el equipo informático no permita realizar el respaldo indicado por los medios regulares, el personal perteneciente o autorizado por la Dirección de Tecnología, utilizará las herramientas tecnológicas que permitan realizar este trabajo, siempre y cuando técnicamente sea posible.
- Los servidores públicos de la PRESIDENCIA DE LA REPÚBLICA, no podrán solicitar que se realice ningún tipo de instalación de software, mantenimiento o reparación a equipos personales o que no sean parte del parque informático que mantiene la Institución.

### **Pérdida de Equipo**

- El usuario que tenga bajo su cargo algún equipo de cómputo, comunicación o accesorios, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de hurto, robo, extravío o pérdida del mismo.
- El usuario deberá dar aviso inmediato a la Máxima Autoridad, Dirección de Tecnología de la desaparición, hurto, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

- Para el manejo del inventario físico, firmas de responsabilidad para préstamos y usos específicos de equipos de tecnología de información, se observarán las políticas aprobadas en lo que fuere pertinente.
- El Centro de Datos, como también las áreas que cuenten con equipos de misión crítica deberán contar con las seguridades necesarias o algún tipo de sistema que recabe información de accesos físicos a las instalaciones.

#### **Uso de dispositivos especiales**

- Los dispositivos tecnológicos especiales asignados a los usuarios son de uso exclusivo para el cumplimiento del trabajo.
- El uso de los grabadores de discos (CD o DVD) y discos externos, es exclusivo para copias de seguridad de software en la PRESIDENCIA DE LA REPÚBLICA y para respaldo de información que por su volumen así lo justifique.
- Queda prohibido el uso de módems externos en las computadoras de escritorio, excepción hecha en requerimientos muy específicos en que, por el tipo de aplicación o servicio de información, exista la necesidad de contar con uno de ellos, bajo autorización de la Dirección de Tecnología.
- Los dispositivos móviles de internet de banda ancha asignados a los usuarios, deberán ser utilizados exclusivamente cuando no se pueda conectar a la red de la PRESIDENCIA DE LA REPÚBLICA.

#### **Daño del equipo**

- Para el caso en que el equipo de cómputo o cualquier recurso tecnológico sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario, el área de Soporte Técnico presentará un informe donde se determine la causa de dicha descompostura. Este informe será entregado a la Máxima Autoridad para que se aplique el procedimiento establecido para estos casos.

#### **Protección Física**

- El Centro de Datos deberá regirse por estándares vigentes para una protección adecuada de los equipos servidores, redes y telecomunicaciones.
- Los sistemas de tierra física, de protección e instalaciones eléctricas del Centro de Datos, deberán contar con un contrato de mantenimiento por lo menos anual, con el fin de garantizar la efectividad del sistema.
- Contar con esquemas de contingencia y continuidad, los cuales incluyen los procedimientos para activar y desactivar la contingencia, de manera de asegurar la continuidad del servicio; estos son: Plan de Recuperación de Desastres (DRP) y Plan de Continuidad de Operaciones (BCP).

La infraestructura tecnológica que se adquiera, deberá contemplar todas las normas establecidas para la fabricación de equipos, referentes al cuidado del medio ambiente, seguridad y del consumo de energía.

### 1.3 POLÍTICAS Y ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

#### POLÍTICA

***Los usuarios utilizarán los mecanismos institucionales para la protección de la información que reside en y utiliza la infraestructura tecnológica de la PRESIDENCIA DE LA REPÚBLICA. Esto incluye la información confidencial que por necesidades institucionales deba ser almacenada o transmitida, tanto en la red interna de la PRESIDENCIA DE LA REPÚBLICA como hacia redes externas utilizando Internet u otros medios.***

#### Uso de medios de almacenamiento

- Los usuarios deberán respaldar periódicamente la información que se encuentre en sus computadoras personales, estaciones de trabajo, laptops o tabletas, especialmente la que sea sensible y crítica.
- En caso de que, por el volumen de información se requiera algún respaldo en CD o DVD, disco externo, servidores de respaldo, unidades de almacenamiento, este servicio deberá solicitarse a Soporte Técnico con conocimiento del Jefe inmediato del área correspondiente, cuando no se cuente con el dispositivo necesario para hacer la grabación.
- Los usuarios de la PRESIDENCIA DE LA REPÚBLICA deben conservar los registros o información que se encuentra activa y aquella que ha sido clasificada como confidencial, de conformidad con lo establecido por la Institución.
- Las actividades que realicen los usuarios en la infraestructura Tecnológica de la PRESIDENCIA DE LA REPÚBLICA son registradas y susceptibles de auditoría.
- Las Bases de Datos y la información en general de la PRESIDENCIA DE LA REPÚBLICA, serán respaldadas periódicamente en forma automática y/o manual, debiendo ser almacenados en un lugar apropiado, seguro, y para ello se elaborarán los procedimientos necesarios.

#### Instalación de software.

- Los usuarios que requieran la instalación de software que no sea propiedad de la PRESIDENCIA DE LA REPÚBLICA, deberán justificar su uso y solicitar la autorización a la Dirección de Tecnología, a través de un oficio firmado por el Jefe del área respectiva, indicando la razón de la solicitud, el equipo de cómputo donde se instalará el software y el período de tiempo que permanecerá dicha instalación. En el caso de que el software solicitado requiera de una licencia, este valor deberá estar presupuestado por el área requirente.
- Se considera una falta grave el que los usuarios hayan instalado o instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, tabletas, servidores o cualquier equipo conectado a la red de la PRESIDENCIA DE LA REPÚBLICA, que no este autorizado por la Secretaría General/Dirección de Tecnología.
- La Dirección de Tecnología y el área de Soporte Técnico, son los únicos autorizados para instalar, actualizar y desinstalar software o programas en los equipos de la PRESIDENCIA DE LA REPÚBLICA, aplicando para ello las mejores prácticas y la normativa internacional de seguridad informática. El objetivo es proteger la integridad del software, la información y la plataforma tecnológica de ataques, software malicioso y programas no autorizados.

### **Identificación de incidentes**

- El usuario que tenga conocimiento de la ocurrencia de un incidente de seguridad informática, deberá reportarlo al área de Soporte Técnico de la manera más urgente, indicando claramente los datos bajo los cuales considera que se trata de un incidente de seguridad informática.
- Cuando exista la sospecha o el conocimiento de que información confidencial ha sido revelada, modificada, alterada o borrada sin la autorización del servidor o de la unidad administrativa competente, el usuario informático deberá notificar a Soporte Técnico quien se encargará de revisar el incidente y tomar las acciones pertinentes.
- Cualquier incidente generado durante la utilización u operación de los activos tecnológicos de la PRESIDENCIA DE LA REPÚBLICA debe ser reportado al área de Soporte Técnico.

### **Administración de la configuración**

- Los usuarios de las áreas de la PRESIDENCIA DE LA REPÚBLICA están prohibidos de establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando protocolos de transferencia de archivos como FTP u otros, empleando la infraestructura de red de la PRESIDENCIA DE LA REPÚBLICA, sin la autorización de la Secretaría General/Dirección de Tecnología.

### **Seguridad para la red**

- Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por la Dirección de Tecnología, en la cual los usuarios realicen la exploración de los recursos informáticos en la red de la PRESIDENCIA DE LA REPÚBLICA, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

### **Uso del Correo electrónico**

- Los usuarios utilizarán la herramienta de colaboración que la PRESIDENCIA DE LA REPÚBLICA establezca como estándar y no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros o de tipo personal, salvo que estén autorizadas y haya sido puesto en conocimiento de la Dirección de Tecnología.
- Si fuera necesario leer información de algún usuario (mientras esta persona no se encuentre en su puesto de trabajo o de vacaciones) el usuario ausente podrá redirigir el correo a otra cuenta de correo interno (Jefe Inmediato, encargado del área), quedando prohibido hacerlo a una cuenta de correo electrónico externa a la PRESIDENCIA DE LA REPÚBLICA.
- Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de la PRESIDENCIA DE LA REPÚBLICA. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.
- Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico encriptado y destinado exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.
- La PRESIDENCIA DE LA REPÚBLICA se reserva el derecho de acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal que ha comprometido la seguridad, violado políticas de Seguridad Informática o realizado acciones no autorizadas, siempre y cuando exista de por medio una petición formal de la Máxima Autoridad.
- El usuario debe utilizar el correo electrónico de la PRESIDENCIA DE LA REPÚBLICA única y exclusivamente en los equipos que tenga asignados y en concordancia con las

facultades que les hayan sido atribuidas para el desempeño de su trabajo, cargo o comisión, quedando prohibido cualquier otro uso.

- Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.
- Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.
- El usuario deberá cuidar, en todo momento, la utilización de un lenguaje apropiado, evitando palabras ofensivas o altisonantes.
- Queda prohibido enviar o reenviar correos masivos o cadenas, publicidad y propaganda comercial, política o social, etcétera, salvo en casos que sean afines a sus funciones y responsabilidades.
- El responsable de Administrar el Correo electrónico no podrá revisar ni redirigir correos de ningún usuario, salvo por pedido expreso de la Máxima Autoridad o del Director de Tecnología. De evidenciarse esta situación, se procederá a reportar al área de Talento Humano para que aplique la sanción que corresponda de acuerdo al Reglamento Interno.
- Todo usuario debe respetar la intimidad, confidencialidad y derechos individuales de los demás usuarios.
- Los usuarios deberán solicitar apoyo a Soporte Técnico ante cualquier duda en el manejo del correo institucional.

#### Controles contra código malicioso

- Para prevenir infecciones por virus informático, los usuarios de la PRESIDENCIA DE LA REPÚBLICA deben evitar el uso de cualquier clase de software que no haya sido proporcionado, autorizado o validado por la Dirección de Tecnología.
- Los usuarios de la PRESIDENCIA DE LA REPÚBLICA deben verificar que la información y los medios de almacenamiento externos, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software instalado y autorizado por la Dirección de Tecnología.
- Todos los archivos de computadora que sean proporcionados por personal externo o interno, como programas de software, bases de datos, documentos, hojas de cálculo, presentaciones, etc. que tengan que ser descomprimidos, para este efecto el usuario debe verificar que estén libres de virus, utilizando el software instalado y autorizado por la Dirección de Tecnología, antes de ejecutarse.
- Se prohíbe a todo servidor de la PRESIDENCIA DE LA REPÚBLICA intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o introducir código de computadora diseñado para auto replicarse, redirigir, dañar, o impedir el normal funcionamiento de cualquier componente de computadora, memoria, archivos de sistema, discos o software. Mucho menos probarlos en cualquiera de los ambientes o plataformas de la PRESIDENCIA DE LA REPÚBLICA.
- Ningún usuario, servidor público o personal externo, podrá bajar o descargar software de sistemas, paginas WEB, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la Secretaría General/Dirección de Tecnología.
- Cualquier usuario que sospeche de alguna infección por virus, deberá dejar de usar inmediatamente el equipo y llamar a Soporte Técnico para la detección y erradicación del virus.
- Periódicamente, las actualizaciones del software antivirus se ejecutarán de manera automática en el computador o laptop que se encuentre conectado a la Red de la PRESIDENCIA DE LA REPÚBLICA; en caso de que se detecte que este software no está actualizado, se deberá reportar al área de Soporte Técnico.
- Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean instaladas por la PRESIDENCIA DE LA REPÚBLICA para: Antivirus, Correo Electrónico, Herramientas de Oficina, Navegadores u otros programas.

- Debido a que algunos virus son extremadamente complejos, ningún usuario de la PRESIDENCIA DE LA REPÚBLICA debe intentar erradicarlos de las computadoras por su propia cuenta, deberá llamar a Soporte Técnico.

#### Internet

- El acceso a Internet provisto a los usuarios de la PRESIDENCIA DE LA REPÚBLICA es exclusivamente para las actividades relacionadas con las necesidades del cargo y función que desempeña.
- La asignación del servicio de Internet, deberá solicitarse por escrito a la Secretaría General/Dirección de Tecnología, señalando los motivos por los que se requiere el mismo. Esta solicitud deberá contar con el visto bueno del Jefe Inmediato.
- Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por la PRESIDENCIA DE LA REPÚBLICA. La única forma de acceder al servicio de Internet es a través de la red de la Institución.
- Los usuarios de Internet de la PRESIDENCIA DE LA REPÚBLICA tienen que reportar todos los incidentes de seguridad informática a la Dirección de Tecnología a través del Soporte Técnico.
- Los usuarios de la PRESIDENCIA DE LA REPÚBLICA que poseen dispositivos móviles institucionales tales como: tabletas, teléfonos celulares u otros similares, deberán solicitar acceso a la Dirección de Tecnología con la debida autorización del Jefe Inmediato, siempre y cuando justifique su uso.
- Los usuarios de Internet que tienen asignados dispositivos móviles de banda ancha no podrán utilizar estos, si se encuentran conectados a la red de la PRESIDENCIA DE LA REPÚBLICA.
- Los usuarios que naveguen en Internet, al utilizar el servicio, están aceptando que:
  1. Están sujetos de auditoría de las actividades que realiza en Internet.
  2. Existe expresa prohibición al acceso de páginas no autorizadas.
  3. Existe la prohibición de transmisión de archivos confidenciales no autorizados.
  4. Existe la prohibición de descarga de software sin la autorización de la Dirección de Tecnología.
  5. La utilización de Internet es para el desempeño de sus actividades y puesto en la PRESIDENCIA DE LA REPÚBLICA y no para propósitos personales.

## 1.4 POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESO Y SEGURIDAD LÓGICA

### POLÍTICA

***Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario (ID Usuario) y clave de acceso (password) necesarios para acceder a la infraestructura tecnológica y la información de la PRESIDENCIA DE LA REPÚBLICA, por lo cual deberá mantenerlo de forma confidencial, siendo responsable de su buen uso.***

El permiso de acceso a los sistemas de información que se encuentra en la infraestructura tecnológica de la PRESIDENCIA DE LA REPÚBLICA, debe ser proporcionado por el titular de los permisos (dueño del proceso), con base en el principio de la “necesidad de saber” el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

### Controles de acceso lógico

- La Dirección de Tecnología debe mantener un control total y sistematizado de los recursos de cómputo tanto de hardware como de software.



- Está prohibido que los usuarios utilicen la infraestructura tecnológica de la PRESIDENCIA DE LA REPÚBLICA para obtener acceso no autorizado a la información u otros sistemas de información.
- Cada usuario de servicios de información es responsable por el código de usuario y clave que recibe para el uso y acceso de los recursos.
- Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por la Dirección de Tecnología, antes de poder usar la infraestructura tecnológica de la PRESIDENCIA DE LA REPÚBLICA.
- Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de la PRESIDENCIA DE LA REPÚBLICA.
- Cada usuario que acceda a la infraestructura tecnológica de la PRESIDENCIA DE LA REPÚBLICA debe contar con un identificador de usuario (ID Usuario), único y personalizado.
- La obtención de la cuenta de usuario y claves de acceso a los servicios tecnológicos debe hacerse de forma segura, para ello la Dirección de Talento Humano remitirá el formulario respectivo de ingreso de personal a la Dirección de Tecnología, a fin de que proceda conforme a lo dispuesto, quedando de tal manera el usuario habilitado para acceder como servidor público de la PRESIDENCIA DE LA REPÚBLICA a la infraestructura tecnológica y servicios.
- Los usuarios son responsables de todas las actividades realizadas con su identificador de usuario (ID Usuario). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario.
- La Dirección de tecnología no es responsable por el contenido de datos ni por el tráfico que circule por la red; la responsabilidad recae directamente sobre el usuario que los genere o solicite.
- El uso de analizadores de red es permitido única y exclusivamente por el personal de la Dirección de Tecnología y/o personal autorizado para tal efecto, con el fin de monitorear la funcionalidad y operatividad de la Red de la PRESIDENCIA DE LA REPÚBLICA, todo enmarcado dentro de las políticas y normativas de seguridad establecidas.
- En el caso de detectarse un uso no aceptable, se inhabilitará temporalmente la cuenta del usuario o red involucrada. La reconexión se hará en cuanto se haya establecido con el Jefe Inmediato si es susceptible de habilitación.
- La Dirección de Talento Humano, a través de su Director, deberá reportar inmediatamente al Director de Tecnología, cuando un servidor público / usuario deje de laborar o de tener una relación con la Institución.

#### **Administración de privilegios**

- Cualquier cambio en los roles y responsabilidades de los usuarios que deba modificar sus privilegios de acceso a la información en la infraestructura tecnológica de la PRESIDENCIA DE LA REPÚBLICA, deberá ser solicitados a la Dirección de Tecnología, previa autorización del Jefe Inmediato.

#### **Equipo desatendido**

- Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como claves y protectores de pantalla (screensaver) previamente instalados y autorizados por la Dirección de Tecnología, cuando no se encuentren en su lugar de trabajo, con un tiempo de espera máximo de 10 minutos.
- El usuario deberá obligatoriamente bloquear el computador, cuando tenga que ausentarse temporalmente.

### **Administración y uso de Claves**

- La asignación de las claves debe ser realizada de forma individual, por lo que su uso compartido está prohibido.
- Todas las cuentas de acceso a los sistemas, infraestructura y recursos de TI, son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.
- Cuando un usuario olvide, bloquee o extravíe su clave, deberá contactarse con Soporte Técnico quienes se encargarán de resetear la clave en caso de bloqueo o proporcionarle una nueva clave, de ser necesario, pero forzará el cambio para que una vez que acceda el usuario le obligue a cambiarlo, garantizando así que se mantenga la confidencialidad y seguridad en el momento en que acceda nuevamente a la información en la infraestructura tecnológica de la PRESIDENCIA DE LA REPÚBLICA.
- Está prohibido que las claves se encuentren de forma legible en cualquier medio ya sea manuscrito o impreso y dejarlos en lugares visibles, donde personas no autorizadas puedan descubrirlos.
- Bajo ninguna circunstancia, las claves deben ser compartidas o reveladas. Caso contrario, el usuario será responsable de todas las acciones que se realicen con su cuenta. Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus claves:
  1. Deben estar compuestos de al menos ocho (8) caracteres y máximo diez (10), en los que se incluirán números, letras y caracteres especiales permitidos.
  2. Deben ser de difícil deducción, esto implica que las claves, preferentemente, no deben relacionarse con el trabajo o la vida personal del usuario, y no deben contener caracteres que expresen listas secuenciales y caracteres de control.
  3. No deben ser idénticos o similares a claves que hayan usado previamente.
- Las claves tendrán una vigencia máxima de 90 días; finalizado este periodo, el usuario deberá realizar el cambio de contraseña, para lo cual existirán las alertas suficientes.
- Todo usuario que tenga la sospecha de que su clave es conocida por otra persona, deberá cambiarla inmediatamente.
- Los usuarios no deben escribir ni almacenar sus claves en ningún programa o sistema que proporcione esta facilidad.
- Los usuarios tendrán tres (3) oportunidades para ingresar su clave; de no conseguirlo, su cuenta se bloqueará automáticamente.

### **Control de accesos remotos**

- Esta prohibido el acceso a redes externas vía cualquier dispositivo de conexión; cualquier excepción deberá ser documentada y contar con el registro de la Dirección de Tecnología.
- La administración remota de equipos conectados a Internet no esta permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por el dueño del proceso y de la Dirección de Tecnología.

### **Desarrollo y adquisición de sistemas**

- La Dirección de Tecnología es el responsable de definir y establecer los estándares y procedimientos para el desarrollo, mantenimiento y adquisición de sistemas de información, incluyendo la custodia del código fuente, ambientes de prueba, planes piloto, pruebas de concepto y toda la infraestructura tecnológica relacionada, de conformidad con las mejoras prácticas del mercado y reglas internacionales de seguridad informática. El objetivo es minimizar los riesgos de falla en los sistemas y aplicativos, velar por la utilización adecuada de los recursos y garantizar que estos contribuyan con el cumplimiento de los objetivos institucionales.



## 1.5 POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

### POLÍTICA

***La Dirección de Tecnología tiene como una de sus funciones y atribuciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para salvaguardar equipos, información e instalaciones de cómputo, así como de bancos de datos de información automatizada en general de la PRESIDENCIA DE LA REPUBLICA.***

#### Derechos de propiedad intelectual

- Está prohibido por las leyes de derechos de autor y por la PRESIDENCIA DE LA REPÚBLICA, realizar copias no autorizadas de software, ya sea adquirido o desarrollado por la Institución.
- Los sistemas y aplicativos desarrollados por personal interno o externo son propiedad intelectual de la PRESIDENCIA DE LA REPÚBLICA.

#### Revisiones del cumplimiento

- La Dirección de Tecnología realizará acciones de verificación del cumplimiento de estas Políticas, de acuerdo a lo establecido en su programa anual de trabajo.
- La Dirección de Tecnología podrá implementar mecanismos de control que permitan identificar tendencias y comportamientos en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecutan los usuarios.
- Los dueños de los procesos establecidos en la PRESIDENCIA DE LA REPÚBLICA deben apoyar las revisiones de los sistemas para el cumplimiento de las políticas y estándares de seguridad informática establecidos.

#### Violaciones de seguridad Informática

- Está prohibido el uso de herramientas de hardware o software que pretendan vulnerar los controles de seguridad informática, a menos que se autorice por la Dirección de Tecnología conforme un análisis previo.
- Está prohibido realizar pruebas a los controles de los diferentes elementos de Tecnología de Información. Ninguna persona puede probar o intentar comprometer los controles internos a menos que cuente con la autorización de la Dirección de Tecnología.
- Ningún usuario de la PRESIDENCIA DE LA REPÚBLICA debe probar o intentar probar fallas de la Seguridad Informática identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas por la Dirección de Tecnología.
- Está prohibido realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios tecnológicos.
- No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa, sentencia), virus, gusanos ó caballos de Troya, SQL injection, diseñados para auto replicarse, alterar el normal funcionamiento de un programa, sistema, aplicativo, dañar o afectar el desempeño o acceso a las computadoras, redes o información de la PRESIDENCIA DE LA REPÚBLICA.

## 2. USO DE LOS RECURSOS INFORMÁTICOS

### 2.1 POLÍTICAS DE ADQUISICIÓN Y USO DE LOS RECURSOS INFORMÁTICOS

#### POLÍTICA

***Se entenderá como Recursos Informáticos a todas las herramientas informáticas que la PRESIDENCIA DE LA REPÚBLICA pone a disposición del conjunto de sus usuarios. Establecer los lineamientos principales para asegurar el uso eficiente, eficaz y económico de los recursos y servicios informáticos, los mismos que serán utilizados exclusivamente en las actividades propias de la institución.***

#### Adquisición de Hardware, Software y Servicios Tecnológicos

- La Secretaría General / Dirección de Tecnología es responsable de definir, consolidar, estandarizar, recomendar, asesorar y avalar lo relativo a la adquisición y distribución de software, equipos de computación, redes, seguridad, comunicaciones y otros dispositivos y accesorios que compongan la plataforma tecnológica. Así mismo de definir, gerenciar y ejecutar los proyectos tecnológicos de la PRESIDENCIA DE LA REPUBLICA.

#### Uso de los Recursos Tecnológicos

- Todos los recursos informáticos deberán ser utilizados para trabajos que contribuyan al cumplimiento de los objetivos de la PRESIDENCIA DE LA REPÚBLICA.
- El equipo de cómputo asignado, dispositivos especiales, dispositivos de almacenamiento externo, dispositivos de comunicación, software y en general recursos informáticos deberán ser para uso exclusivo de las funciones y responsabilidades asignadas a los servidores públicos de la PRESIDENCIA DE LA REPÚBLICA.
- El usuario es responsable del buen uso que se dé a todos los recursos tecnológicos que estén bajo su resguardo o a los que tenga acceso para el cumplimiento de su trabajo.
- El usuario deberá reportar cualquier riesgo potencial del que tenga conocimiento y que pueda afectar a los recursos informáticos.
- Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.
- Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del CPU y se debe mantener el equipo informático en un entorno limpio y sin humedad.
- El resguardo para las laptops, tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.
- Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas especializadas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
- El software que se encuentre instalado en los equipos propiedad de la PRESIDENCIA DE LA REPÚBLICA deberá, de ser el caso, contar con licencias vigentes en cumplimiento con las disposiciones aplicables.
- Mediante estas políticas, se habilita a todo el personal de la PRESIDENCIA DE LA REPÚBLICA, contratado bajo las diferentes modalidades, a tener acceso a los recursos informáticos con el fin de que puedan desempeñar sus funciones.
- Los niveles de acceso de los servidores públicos a los recursos tecnológicos serán en función de sus necesidades de trabajo, dentro de los objetivos de la Institución observando el esquema tanto de seguridades, seguimiento y controles.

- Se otorgarán los recursos informáticos y los accesos necesarios, siempre que exista la debida autorización.
- La atención, soporte y entrenamiento de usuarios cuando se requiera, será responsabilidad de la Dirección de Tecnología, en lo que está relacionado con su competencia.
- Toda actividad actual o futura, que involucre el uso de recursos informáticos, deberá informarse y coordinarse con la Dirección de Tecnología.
- Todas las modificaciones y actualizaciones de los recursos informáticos de la PRESIDENCIA DE LA REPUBLICA deben ser realizados bajo la asesoría, supervisión y autorización de la Dirección de Tecnología.
- La Dirección de Tecnología elaborará las especificaciones técnicas para la adquisición de hardware, software y servicios tecnológicos; así como, para su mantenimiento, actualización o remplazo.
- Los mensajes que se envíen vía Internet, serán de completa responsabilidad del usuario emisor y en todo caso deberán basarse en la racionalidad y la responsabilidad individual.
- Cuando el usuario de un equipo portátil (laptop), tableta, dispositivo de banda ancha u otro dispositivo o accesorio del cual sea custodio, cumpla una Comisión de Servicios, el Jefe Inmediato deberá respaldar la información existente, de ser el caso, o solicitar a Soporte Técnico que se formatee la máquina, para que pueda ser entregada al Guarda Almacén.
- La Dirección de Tecnología es la responsable de generar políticas, procedimientos y en general normativas que permita normar el buen uso de los recursos informáticos, así como de modificarlas o mejorarlas, una vez realizado este trabajo deberá ser enviado para aprobación de la Máxima Autoridad, quien dispondrá su publicación y cumplimiento obligatorio.

#### **Sólo para el área de Tecnología**

- Todos los servicios, sistemas, soluciones, herramientas de tecnología que requiera o utilice la PRESIDENCIA DE LA REPÚBLICA serán suministrados, manejados, distribuidos y operados exclusivamente por la Dirección de Tecnología utilizando para ello la infraestructura de su Centro de Datos.
- La Dirección de Tecnología llevará a cabo los proyectos de la PRESIDENCIA DE LA REPUBLICA siempre buscando optimizar los recursos existentes, adquiriendo y aplicando la mejor tecnología disponible en el mercado, con la mejor calidad de servicio y cubriendo las necesidades de las unidades de la PRESIDENCIA DE LA REPÚBLICA y sus objetivos.
- El control, administración y operación de todos los recursos y servicios informáticos de la PRESIDENCIA DE LA REPÚBLICA son responsabilidad de la Dirección de Tecnología.
- La Dirección de Tecnología será responsable de desarrollar estrategias, planes y acciones para mantener los recursos informáticos de la PRESIDENCIA DE LA REPÚBLICA siempre operativos y con calidad de servicio, por lo que los usuarios deberán acatar las recomendaciones que emita.
- La red de la PRESIDENCIA DE LA REPÚBLICA solamente puede utilizarse para propósitos en apego a la misión Institucional. Al utilizar la red, el usuario deberá comprometerse a dar un uso adecuado, por lo tanto la Dirección de Tecnología es responsable de procedimientos e instructivos consistentes y divulgarlos entre sus usuarios.
- La Dirección de Tecnología a través de los administradores de las redes, base de datos, soporte y sistemas, tienen la facultad de tomar las acciones necesarias para preservar la disponibilidad y la integridad de los sistemas, restaurar los sistemas en caso de fallas, abusos, virus, y otras situaciones similares, con la finalidad de garantizar la integridad de la información y la continuidad de las operaciones de la PRESIDENCIA DE LA REPÚBLICA.

#### Gestión de proyectos de tecnología

- La Dirección de Tecnología en el ámbito de sus competencia, y en conjunto con las diferentes áreas funcionales de la PRESIDENCIA DE LA REPÚBLICA serán los responsables de diseñar, documentar, liderar, administrar y gestionar los proyectos de tecnología, utilizando herramientas, metodologías y procedimientos de conformidad con las mejoras prácticas del sector y reglas internacionales, garantizando la consecución de los objetivos de la Institución.

### 3. OBSOLESCENCIA DE EQUIPOS INFORMÁTICOS

#### POLÍTICA

***Se entenderá por obsolescencia, el desuso de máquinas, equipos, componentes y tecnologías, originadas no por un mal funcionamiento del mismo, sino por un insuficiente desempeño de sus funciones en comparación con las nuevas máquinas, equipos y tecnologías introducidos en el mercado. Definir aspectos generales para garantizar la efectividad y el aprovechamiento del rendimiento del equipamiento informático como soporte para el desarrollo de los servicios de la institución.***

- Para garantizar un eficaz servicio, se define que el período de obsolescencia de los equipos informáticos: PC's, LapTops, Servidores, Switches, Routers y demás equipos tecnológicos y audiovisuales es de máximo 2 años y de conformidad con las necesidades institucionales. Dentro de este plazo, se procederá automáticamente a reemplazar o repotenciar el equipo. Para lo cual será necesario realizar un análisis técnico producto de la evaluación efectuada a los equipos y a la carga de trabajo.
- El software desarrollado deberá ser actualizado (nuevos **release**, versiones o **upgrades**), o si amerita reemplazarlo según sea el caso, luego de un análisis de requerimientos, funcionalidades y nuevas tecnologías. Para ello se deberá utilizar una herramienta de **versionamiento** y paso a producción.

Estas políticas serán observadas y aplicadas por todos los servidores públicos, usuarios de la PRESIDENCIA DE LA REPUBLICA.

***Elaborado por:***

***Revisado por:***

***Aprobado Por:***

**NOTAS:**

[illegible]

**NOTAS:**

[illegible]

[www.presidencia.gob.ec](http://www.presidencia.gob.ec)  
<http://intranet.presidencia.gob.ec/>





**RAZÓN:** Quito, quince de enero de dos mil veintiuno. La presente es materialización del documento denominado "POLÍTICAS DE TECNOLOGÍA DE LA PRESIDENCIA DE LA REPÚBLICA", expedido en enero de 2013 por la Dirección de Tecnologías de la Información y Comunicación. El mencionado documento está compuesto por (23) veintitrés hojas, el mismo que consta en la página de Intranet de la Presidencia de la República: [https://intranet.presidencia.gob.ec/wp-content/uploads/2020/01/POLITICAS-TEC\\_01.pdf](https://intranet.presidencia.gob.ec/wp-content/uploads/2020/01/POLITICAS-TEC_01.pdf).

Liliana del Rosario Ortiz Lemos  
**DIRECTORA DE GESTIÓN DOCUMENTAL Y ARCHIVO**