PARTIDO DE LA UNIÓN POR LA GENTE - PARTIDO DE LA U

# SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Políticas y manual de Seguridad Informática

# Contenido

# VERSIONES

| VERSION | FECHA | CAMBIOS INTRODUCIDOS | RESPONSIBLE |
|---|---|---|---|
| 01/06/2020 | | Versión Inicial | Leonor García Tamayo- Ing. de Sistemas |
| | | | |
| | | | |
| | | | |

## DERECHOS DE AUTOR

Todas las referencias a los documentos del modelo de seguridad y privacidad de la Información son derechos reservados por parte del Partido de La Unión por la Gente - Partido de la U.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27001:2013, así como a los anexos son derechos reservados por parte de ISO/ICONTEC.

## AUDIENCIA

Este documento está elaborado para militantes, funcionarios, contratistas, proveedores de servicios y terceros que utilicen o accedan a la información y/o infraestructura tecnológica del Partido de La Unión por la Gente - Partido de la U.

# I. INTRODUCCIÓN

Los requerimientos de seguridad que involucran las tecnologías de la información, en pocos años han cobrado un gran auge y más aún con las de carácter globalizador como lo son la de internet y en particular, la relacionada con la Web, situación que ha llevado a la aparición de nuevas amenazas a los sistemas computarizados.

Teniendo en cuenta la importancia que tiene que el partido defina las necesidades de sus grupos de interés, y la valoración de los controles precisos para mantener la seguridad de la información, se definirán políticas que tengan en cuenta el marco general del funcionamiento del mismo, sus objetivos institucionales, sus procesos misionales, que se adaptarán a las condiciones específicas y particulares de cada una de las necesidades según corresponda, y que serán de estricto cumplimiento y aplicación para cada uno de los usuarios internos y externos que apoyen el desarrollo y cumplimiento de los objetivos del Partido.

Por lo anterior, El Partido de la Unión por la Gente – Partido de la U, en adelante "El Partido", identificó la necesidad de normar el uso adecuado de estas destrezas tecnológicas para aprovechar estas ventajas, y así evitar el uso indebido y problemas en los bienes y servicios que presta el mismo.

De esta manera, estos lineamientos de seguridad para los equipos y programas de informática, emergen como el instrumento de apoyo a los funcionarios y/o usuarios del Partido, acerca de la importancia y sensibilidad de la información y servicios críticos y de la superación de las posibles fallas.

Los presentes lineamientos deberán seguir un proceso de actualización cuando sea necesario, están sujetos a los cambios organizacionales relevantes: crecimiento de la planta personal, cambio en la infraestructura informática, desarrollo de nuevos servicios, entre otros.

## II. OBJETIVOS

### GENERAL

Establecer lineamientos de trabajo para el área de Tecnología Informática (TI) con el fin seguir los procedimientos adecuados para proporcionar seguridad en el manejo y resguardo de información e infraestructura tecnológica.

### ESPECIFICOS

Dar a conocer a cada funcionario y/ usuario sobre los procedimientos y normativas a seguir en cuanto a la seguridad informática y socializar con todas las áreas los lineamientos que se pueden y deben seguir para el manejo adecuado de software y hardware.

## III. ALCANCE

Esta política aplica a todo El Partido, sus militantes, funcionarios, contratistas, terceros, e involucrados en el uso tanto de software como hardware y aplica para todas las áreas y para el manejo de la información crítica de El Partido, desde los accesos a datos hasta la eliminación de los mismos, instalaciones de equipos, servicios, y mantenimientos.

## IV. GLOSARIO

- **Política:** Declaración de alto nivel que describe la posición del Partido sobre un tema específico.
- **Estándar:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel del Partido antes de crear nuevas políticas.
- **Mejor Práctica:** Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.
- **Guía:** Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.
- **Procedimiento:** Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas del Partido, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del área donde ellos se aplican.
- **Área Crítica:** Es el área física donde se encuentra instalado el equipo de informática y telecomunicaciones que requiere de cuidados especiales y que son indispensables para el funcionamiento continuo de los sistemas de comunicación que están conectados.
- **Auditoria:** Llevar a cabo una inspección y examen independiente de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y procedimientos operativos y para recomendar cualquier cambio que se estime necesario.

- **Backup (copia de seguridad):** Los programas y/o técnicas de respaldo (backups), son las que permiten realizar una copia espejo de la información alojada en una base de datos, servidor y/o computadora personal, almacenándola en un dispositivo de almacenamiento masivo como disco duro externo u otro dispositivo de red destinado para este fin con el objetivo de realizar la recuperación de la información y evitar pérdidas de información críticas.

- **Bases de Datos: (Database).** Conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la posibilidad de relacionarlos y ordenarlos en base a diferentes criterios. Las bases de datos son uno de los grupos de aplicaciones de productividad personal más extendidos.
- **Control de acceso:** Técnica usada para definir el uso de programas o limitar la obtención y almacenamiento de datos a una memoria u dispositivo de almacenamiento. Es una característica o técnica en un sistema de comunicaciones que permite o niega el uso de algunos componentes o algunas de sus funciones.
- **Equipo de telecomunicaciones:** Todo dispositivo capaz de transmitir y/o recibir señales digitales o analógicas para comunicación de voz, datos y video, ya sea individualmente o de forma conjunta.
- **Equipo de informática:** Dispositivo con la capacidad de aceptar y procesar información con base en los programas establecidos o instrucciones previas, teniendo la oportunidad de conectarse a una red de equipos o computadoras para compartir datos y recursos, entregando resultados mediante despliegues visuales, impresos o audibles.
- **Enrutador/ROUTERS:** Es un dispositivo que proporciona conectividad a nivel de red. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un enrutador y que por tanto tiene prefijos de red distintos.
- **Firewall (cortafuegos):** Sistema instalado entre una red local e internet que asegura dicha red local y mantiene a los usuarios no autorizados fuera de la misma. Firewall en un sistema operativo, es un programa especializado en resguardar la información que se aloja en la computadora local de cualquier acceso remoto de tipo malicioso o ataques informáticos.
- **Internet:** Es una convergencia de conceptos computacionales para presentar y enlazar información que se encuentra dispersa a través de páginas Web en una forma fácilmente accesible.
- **Programas Freeware:** Programas/herramientas que se ofrecen al público sin ningún costo, pero que mantiene un copyright sobre ellos. Es decir se pueden usar sin problemas, pero no se pueden utilizar como parte de otros programas o modificarlos de ninguna manera.

- **Red informática:** Conjunto de ordenadores conectados directamente por cable, remotamente vía conmutadores de paquetes, o por otro procedimiento de comunicación.
- **Servidor:** Genéricamente, dispositivos de un sistema que resuelve las peticiones de otros elementos del sistema, denominados clientes. Computadora conectada a una red que pone sus recursos a disposición del resto de los integrantes de la red. Suele utilizarse para mantener datos centralizados o para gestionar recursos compartidos.
- **Antivirus:** Programa cuya finalidad es prevenir los virus informáticos así como curar los ya existentes en un sistema. Estos programas deben actualizarse periódicamente.
- **Dominio:** Sistema de denominación de hosts (estaciones de trabajo) en red, está formado por un conjunto de caracteres el cual identifica un sitio de la red accesible por un usuario.
- **Encriptar:** Cifrado. Tratamiento de un conjunto de datos, contenidos o no en un paquete, con el fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos. Hay muchos tipos de cifrado de datos, que constituyen la base de la seguridad de la red.
- **Gateway:** Es un punto de red que actúa como entrada a otra red.
- **Hardware:** Maquinaria. Componentes físicos de una computadora o de una red (a diferencia de los programas o elementos lógicos que los hacen funcionar).
- **Malware:** Cualquier programa cuyo objetivo sea causar daños a computadoras, sistemas o redes y, por extensión, a sus usuarios.
- **Software:** Se refiere a programas en general, aplicaciones, juegos, sistemas operativos, utilitarios, antivirus, etc. Lo que se pueda ejecutar en la computadora.
- **TI:** Tecnologías de la información
- **Ups:** Siglas en ingles de Uninterruptible Power Suply, es un aparato que incluye una batería que en caso que se vaya la electricidad, puede, por ejemplo, mantener una computadora funcionando lo suficiente para que el usuario pueda apagarla y guardar data importante.
- **Virus:** Programa que se duplica a sí mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas

# V. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## 1. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La dirección de Sistemas, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de una política de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con El Partido de la Unión por la Gente y los usuarios, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con nuestra misión y visión partidista.

Para El Partido de la Unión por la Gente , la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.
De acuerdo con lo anterior, esta política aplica a todo El Partido, a sus militantes, funcionarios, terceros, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa estarán determinados por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de El Partido.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios misionales del Partido
- Mantener la confianza de sus militantes, empleados y terceros.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros y militantes
- Garantizar la continuidad del negocio frente a incidentes.
- El Partido de la Unión por la Gente ha decidido definir, implementar, operar y mejorar de forma continua las políticas de seguridad de la Información, soportado en
  lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, militantes, proveedores, o terceros que se relacionen con El Partido de la Unión por la Gente .

## 1.1 Políticas

1. El Partido de la Unión por la Gente , protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se generan de los accesos otorgados a terceros (ej.: proveedores o militantes), o como resultado de un servicio de outsourcing.
2. El Partido de la Unión por la Gente , protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.
3. El Partido de la Unión por la Gente , protegerá su información de las amenazas originadas por parte del personal y/o usuarios.
4. El Partido de la Unión por la Gente, protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
5. El Partido de la Unión por la Gente , controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
6. El Partido de la Unión por la Gente, implementará control de acceso a la información, sistemas y recursos de red.
7. El Partido de la Unión por la Gente, garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
8. El Partido de la Unión por la Gente, garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
9. El Partido de la Unión por la Gente, garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
10. El Partido de la Unión por la Gente , garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

La Política de Seguridad y Privacidad de la Información, es la declaración general que representa la posición de la administración dEl Partido de la Unión por la Gente con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, militantes, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos del Partido y apoyan la implementación de la política de seguridad de la información, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

## 1.2 Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

El incumplimiento a la política de seguridad y privacidad de la información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, en cuanto a seguridad y privacidad de la Información se refiere.

## 2. IMPLEMENTACION

Las políticas y estándares de seguridad informática tienen por objeto establecer medidas y patrones técnicos de administración y organización de las Tecnologías de Información (TI) de todo el personal comprometido en el uso de los servicios informáticos proporcionados por el Área de TI en cuanto a la mejora y al cumplimiento de los objetivos institucionales.

También se convierte en una herramienta de difusión sobre las políticas y estándares de seguridad informática a todo el personal del Partido, facilitando una mayor integridad confidencialidad y confiabilidad de la información generada por el área de TI al personal, al manejo de los datos, al uso de los bienes informáticos disponibles, minimizando los riesgos en el uso de las tecnologías de información.

## 3. SEGURIDAD DE LA INFORMACIÓN DE LOS PROCESOS MISIONALES

En los procesos misionales se busca la protección y tratamiento de la información de acuerdo a la ley 1581 de 2012, la cual debe ser íntegra, estar disponible y ser confidencial, con el fin de garantizar la no expedición de la información sensible sin previa autorización del personal involucrado.
Para el Partido, es crucial proteger la información sensitiva, evitando que sea conocida por personas diferentes a aquellas que la requieren o que sea publicada de manera indiscriminada.
El Partido establece actividades para evitar el fraude, espionaje, sabotaje o vandalismo que puedan alterar la seguridad de la información, se cuenta con software de información en los procesos críticos, los cuales permiten una mejor administración y protección de la información.

Que información debe ser protegida:

- Información con datos de los senadores, representantes, gobernadores, alcaldes, concejales, diputados, ediles y demás militantes, del Partido.
- Información en los Sistemas (SIU, SIIGO, carpetas compartidas, entre otros que contengan información confidencial y datos sensibles).
- Oficios físicos, resoluciones.

- Archivo digital en disco duro o USB.
- Datos en las Bases de datos.

### 3.1 Amenazas asociadas al uso de la información

- Uso de las Contraseñas.
- Correo electrónico y mensajería instantánea.
- Virus Informáticos y SPAM.
- INTERNET.
- Conexiones Públicas (cafés internet) y Spyware (SW espía).
- Phishing (suplantación identidad)
- Hackers (Acceso no Autorizado)
- Dispositivos móviles

### 3.2 Actividades de seguridad

- Bloquear y proteger las unidades cuando no estén siendo utilizadas (guardar bajo llave).
- No colocar medios removibles cerca de fuentes electromagnéticas (Imanes).
- Marcar los medios indicando su contenido.
- Destruir siempre los medios de almacenamiento removibles antes de de desechados.
- Realizar inventario de los contenidos de los medios extraíbles con frecuencia, eliminando datos que no sean necesarios almacenar en estos.

## 4. CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

**Política:** La Oficina de TI. Tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas.

## 5. CLÁUSULA DE CUMPLIMIENTO

1. La Oficina de TI realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática.
2. La Oficina de TI podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos.
3. Los jefes y responsables de los procesos establecidos en el Partido deben apoyar las revisiones y el cumplimiento de las políticas y estándares de seguridad informática.

# VI. LINEAMIENTOS DE SEGURIDAD

## 1. Generales

1. Cada una de las áreas funcionales del Partido, deberá elaborar los planes de contingencia que correspondan a las actividades críticas que realicen a través de los sistemas de información.
2. Los presentes lineamientos deberán ser divulgados por el área de informática a través de la Secretaria General, a todo el personal involucrado que utilice equipos y programas informáticos.
3. El área de Tecnología Informática (TI), podrá accesar a la información de un usuario cuando se presuma alguna falta grave que amerite una sanción o investigación.
4. Cuando a un usuario se le esté realizando un proceso de investigación por alguna falta o negligencia y este, para realizar sus funciones, requiera tener acceso a la información y a las operaciones que se realicen en El Partido, el área de Tecnología Informática (TI) podrá restringirle el acceso a los equipos informáticos de su área.

El área de Tecnología Informática (TI), es la responsable de brindar servicio directo al usuario, en lo que respecta al equipamiento, instalación, actualización, cambio de lugar y programación informática, con el fin de permitirle el uso de los equipos, de la infraestructura de red y servicios asociados a ellos, en forma eficaz y eficiente.

## 2. Seguridad Institucional

**Política:** Toda persona que ingresa como usuario nuevo al Partido para manejar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el presente manual.

### 2.1 Usuarios nuevos

Todo el funcionario nuevo en El Partido, deberá ser notificado ante el proceso de TI (Tecnologías de la información); para asignarle los derechos correspondientes (Equipo de cómputo, Creación de usuario en el servidor (Perfil en el servidor) o en caso de retiro anular y cancelar los derechos otorgados como usuario informático.

### 2.2 Obligaciones de los usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir con las Políticas y estándares de seguridad informática para usuarios en el presente manual.

### 2.3 Capacitación en seguridad informática

Todo funcionario nuevo en El Partido deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática, según sea el área operativa y en función de las actividades que se desarrollan; de la misma forma las sanciones en que pueden incurrir en caso de incumplimiento.

### 2.4 Sanciones

Se consideran violaciones graves el hurto, daño, divulgación de información reservada o confidencial, o ser encontrado culpable de delito informático.

## 3. Seguridad física y del medio ambiente

**Política:** Para el acceso a los sitios y áreas restringidas se debe notificar a la oficina de TI para la autorización correspondiente, así proteger la información y los bienes informáticos.

### 3.1 Protección de la información y de los bienes informáticos

1. El cableado de red, se instalará físicamente separado de cualquier otro tipo de cables, llámese a estos de corriente o energía eléctrica, para evitar interferencias.
2. Los servidores, sin importar al dominio o grupo de trabajo al que estos pertenezcan, con problemas de hardware, deberán ser reparados localmente, de no cumplirse lo anterior, deberán ser retirados sus medios de almacenamiento.
3. Los equipos o activos críticos de información y proceso, deberán ubicarse en áreas aisladas y seguras, protegidas con un nivel de seguridad verificable y manejable por el administrador y las personas responsables de TI.
4. El usuario o funcionario deberán reportar de forma inmediata al proceso de TI (tecnologías de la información) cuando se detecte riesgo alguno real o potencial equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.
5. El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.

## 3.2 Controles generales

1. En ningún momento se deberá dejar información sensible de hurto, manipulación o acceso visual, sin importar el medio en el que esta se encuentre, de forma que pueda ser alcanzada por terceros o personas que no deban tener acceso a esta información.
2. El suministro de energía eléctrica debe hacerse a través de un circuito exclusivo para los equipos de cómputo, o en su defecto el circuito que se utilice no debe tener conectados equipos que demandan grandes cantidades de energía.
3. El suministro de energía eléctrica debe estar debidamente polarizado, no siendo conveniente la utilización de polarizaciones locales de tomas de corriente, sino que debe existir una red de polarización.
4. Las instalaciones de las áreas de trabajo deben contar con una adecuada instalación eléctrica, y proveer del suministro de energía mediante una estación de alimentación ininterrumpida o UPS para poder proteger la información.
5. Las salas o instalaciones físicas de procesamiento de información deberán poseer información en carteles, sobre accesos, alimentos o cualquier otra actividad contraria a la seguridad de la misma o de la información que ahí se procesa.
6. Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información del Partido que se encuentre almacenada en los equipos de cómputo que tengan en su estación de trabajo.

## 3.3 Controles de acceso físico

1. Cualquier persona que tenga acceso a las instalaciones del Partido, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y/o herramientas que no sean propiedad del Partido;

en el área de recepción o portería, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.

2. La oficina de tecnologías de la información deberá llevar el registro del mantenimiento que se realizan a los equipos de cómputo. Se debe establecer los periodos de mantenimiento preventivo.
3. Dentro de las instalaciones, habrá un espacio dedicado única y exclusivamente al área de servidores, la cual se mantiene separado mediante una división de pared y protegido su acceso bajo llave. Cualquier actividad anómala, efectuada dentro de las instalaciones físicas de procesamiento de información será cancelada en el momento en que se constatase la actividad.

# VII. LINEAMIENTOS DE EQUIPOS

## 1. Instalación de equipos

1. Todo el equipo de informática (computadoras, estaciones de trabajo, accesorios y partes), que esté conectado a la red del Partido, aquel que en forma autónoma se tenga y sea propiedad del Partido, deberá de sujetarse a las configuraciones de la red que se conectan.
2. La protección física y uso adecuado de los equipos es responsabilidad de quienes en un principio se les asigna.

## 2. Atención de fallas o problemas con hardware y software

1. El equipo de cómputo, periférico o accesorio de tecnología de información que sufra algún desperfecto, daño por maltrato, descuido o negligencia por parte del usuario responsable, se le levantara un reporte de incumplimiento de políticas de seguridad.
2. El reporte para la atención de fallas o problemas menores de los equipos informáticos, se hará por vía telefónica o correo electrónico.
3. El área de Tecnología Informática (TI) atenderá las fallas o problemas de los equipos informáticos que estén o no con mantenimiento preventivo o correctivo, documentará la causa de la falla, emitirá un diagnóstico y dará las recomendaciones a los usuarios de las posibles soluciones para la rehabilitación o reparación de los equipos.
4. La atención de fallas o problemas podrá realizarse en el lugar de trabajo dependiendo del problema presentado y de la factibilidad para solucionarlo.

## 3. Mantenimiento de equipos

1. El área de Tecnología Informática (TI), coordinará y verificará que los servicios de mantenimiento preventivo y correctivo para los equipos de informática propiedad del Partido, sean ejecutados según la orden de compra y/o contrato de servicio o quien el área de Tecnología Informática (TI) asigne para prestar estos servicios.

2. Queda estrictamente prohibido dar mantenimiento preventivo y correctivo al equipo de informática que no es propiedad del Partido.
3. Únicamente el personal autorizado por el Área de TI podrá llevar a cabo el mantenimiento preventivo y correctivo de los equipos informáticos.
4. Los usuarios deberán asegurarse de respaldar en copias o backups la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en él equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

5. Cualquier falla efectuada en las aplicaciones o sistema, por la manipulación errónea de archivos, posterior mantenimiento deberá ser notificada y reparada por el personal técnico encargado en dicha función.

## 4. Actualización de equipos

1. El área de Tecnología Informática (TI), es la responsable de proponer los proveedores al Partido para la actualización de los equipos de informática y red.
2. Todo agregado o adhesión de repuestos que incremente la vida útil del equipo informático, debe de ser reportado al encargado de manejo de inventarios del área Administrativa y Financiera.

## 5. Pérdida de equipos

1. El funcionario que tengan bajo su responsabilidad o asignado algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de hurto, extravío o pérdida del mismo.
2. El funcionario deberá de informar de inmediato al proceso de TI y almacén la desaparición, hurto o extravío de equipos de cómputo, periféricos o accesorios bajo su responsabilidad.

## 6. Protección y ubicación del equipo

1. Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del proceso de TI, en caso de requerir este servicio deberá solicitarlo mediante el debido formato y con mínimo un día de anterioridad.
2. El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones asignadas dentro del Partido.
3. Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
4. Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro diferente aquella que contiene el sistema operativo.
5. Mientras se opera el equipo de cómputo, no se deberán consumir alimentos ni ingerir líquidos.
6. Se debe evitar colocar objetos encima del equipo cómputo o tapar las salidas de ventilación del monitor o de la CPU.
7. Se debe mantener el equipo informático en un lugar limpio y sin humedad.
8. El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar la reubicación de cables al personal de TI.

9. Cuando se requiera realizar cambios múltiples de los equipos de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, éstos deberán ser notificados con tres días de anticipación al proceso de TI.
10. Queda terminantemente prohibido que el usuario o funcionario distinto al personal de TI abra o destape los equipos de cómputo.

# VIII. CONTROLES DE ACCESOS FÍSICOS

**Política:** Los usuarios y funcionarios deberán proteger la información utilizada en la infraestructura tecnológica del Partido. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna del partido, a otras redes externas como Internet.

1. Los usuarios y funcionarios del Partido que hagan uso de equipos de cómputos, deben conocer y aplicar las medidas para la prevención de código malicioso (malware) y/o virus.
2. TI establece las políticas y procedimientos administrativos para regular, controlar y describir el acceso de visitantes o funcionarios no autorizados a las instalaciones de cómputo restringidas.
3. Cuando un funcionario no autorizado o un visitante requieran la necesidad de ingresar al sitio donde se encuentren los servidores, debe solicitar mediante comunicado interno debidamente firmado y autorizado por el Jefe inmediato de su área o dependencia y para un visitante se debe solicitar la visita con anticipación la cual debe traer el visto bueno de la Secretaría General, y donde se especifique tipo de actividad a realizar, y siempre contar con la presencia de un funcionario del proceso de TI.
4. El proceso de Tecnologías de la Información deberá llevar un registro escrito de todas las visitas autorizadas al Centro de Cómputo restringido.
5. Todo equipo informático ingresado al Centro de Cómputo restringido deberá ser registrado en el libro de visitas en portería.
6. Cuando se vaya a realizar un mantenimiento en algunos de los equipos del Centro de Cómputo restringido, se debe dar aviso con anticipación a los usuarios para evitar traumatismos.
7. El proceso de Tecnologías de la Información deberá solicitar a la Dirección Administrativa y Financiera, los equipos de protección para las instalaciones contra incendios, inundaciones, sistema eléctrico de respaldo, UPS.

## 1. Acceso a las áreas críticas

1. La oficina de sistemas, identificará las áreas críticas o de acceso restringido para el personal.
2. El director o coordinador de cada área, será el responsable de autorizar o no el ingreso de personal a las áreas consideradas críticas y deberá informarlo por escrito al área de sistemas.

## 2. Acceso al equipo de informática

1. El funcionario a quien se le asigne un equipo será el responsable de su custodia y buen uso del mismo y responderá a su extravió o daño no justificable.
2. Dada la naturaleza de los sistemas operativos y su conectividad en red, el área de Tecnología Informática (TI), tiene la facultad de accesar a cualquier equipo de informática que esté conectado en la red aun cuando no esté bajo la responsabilidad directa del área.

## 3. Acceso local a la red

1. El área de Tecnología Informática (TI), es la responsable de proporcionar a los usuarios el acceso a los recursos informáticos que estén o no en red.
2. Dado el carácter unipersonal del acceso a la red, El área de Tecnología Informática (TI), verificará, a través de visitas periódicas a los usuarios, el uso responsable de los recursos informáticos que se comparten en la red.
3. El acceso a equipo especializado en informática (servidores, enrutadores, bases de datos, etc.) conectado a la red será administrado únicamente por el área de Tecnología Informática (TI).
4. Todo el equipo de informática que este o sea conectado a la red, o aquellos que en forma autónoma se tengan y que sean propiedad del Partido, deberán sujetarse a los procedimientos de acceso que emita el área de Tecnología Informática (TI).

## 4. Acceso remoto

1. El área de Tecnología Informática (TI), será la responsable de proporcionar los servicios de acceso a los recursos informáticos del Partido, disponibles a través de la red.
2. Los usuarios de estos servicios deberán sujetarse a las configuraciones y especificaciones ya instaladas y no podrán hacer cambios a éstas.

## 5. Acceso a los sistemas de información

1. La instalación y uso de los sistemas de información se regirán por lo establecido en la definición de políticas y procedimientos de controles generales en los sistemas de información de las normas técnicas de control interno específicas del Partido.

2. El control de acceso a cada sistema de información será determinado por la dirección o coordinación del área responsable de generar y procesar los datos, sobre la base de los niveles de responsabilidad asignados a cada funcionario para su lugar de trabajo.
3. La creación de nuevas cuentas con acceso a los sistemas de información deberá ser solicitado vía correo electrónico o por escrito, esta solicitud deberá contener el nombre del funcionario, nivel de acceso a la información (solo consulta, ingreso, modificación de datos, etc.). área que solicita, y firma de jefe inmediato así como la autorización de la Secretaría General cuando se requiera.

## 6. Acceso a internet

1. La Secretaría General, será la responsable de autorizar la información a publicar en el sitio Web Institucional.
2. El área de Tecnología Informática (TI), en coordinación con el área de Comunicaciones, será la responsable de actualizar las veces que sea necesario hacerlo, la información que se publique en el sitio web institucional.
3. Los accesos a las páginas web a través de los equipos autorizados, deben utilizarse responsablemente y no descargar programas o información que pueda dañar a los programas y equipos propiedad del Partido
4. Los servicios de internet estarán sujetos a la disponibilidad en la infraestructura de red de datos del Partido.
5. El servicio de internet no deberá utilizarse para navegar por páginas con información obscena o para enviar correos electrónicos que dañen la integridad moral de las personas y/o la imagen reputacional del partido. El mal uso del internet será sancionado con la suspensión del servicio. El tiempo de la sanción será determinado de acuerdo a lo estipulado en el reglamento interno de trabajo del Partido, sin perjuicio de las sanciones laborales que correspondan.
6. Se proporcionará acceso a internet a los funcionarios del Partido y a los que las jefaturas determinen que es necesario para su desarrollo laboral, de igual forma la cuenta de correo institucional.
7. El área de Tecnología Informática (TI), no se hará responsable por problemas externos de conectividad y comunicación por parte del proveedor del servicio, sin embargo se comunicará con el proveedor para hacer el reclamo respectivo.
8. Los usuarios del servicio de navegación en Internet, al utilizar el servicio están aceptando que:
    - Serán sujetos de monitoreo de las actividades que realiza en Internet, saben que existe la prohibición al acceso de páginas no autorizadas, saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
    - Saben que existe la prohibición de descarga de software sin la autorización de la Oficina de TI.

# IX. CONTROLES DE ACCESO LÓGICO

**Política:** Cada usuario o funcionario es responsable de los mecanismos de control de acceso que le sean proporcionado; esto es, de su "ID" login de usuario y contraseña necesarios para acceder a la red interna de información y a la infraestructura tecnológica del Partido, por lo que se deberá mantener de forma confidencial. El permiso de acceso a la información que se encuentra en la infraestructura tecnológica del Partido, debe ser proporcionado por el dueño de la información, con base en el principio de "Derechos de Autor" el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

1. Todos los usuarios de servicios de información son responsables por el usuario y contraseña que recibe para el uso y acceso de los recursos.
2. Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por la Oficina de TI, antes de poder usar la infraestructura tecnológica del Partido,
3. Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del Partido, a menos que se tenga el visto bueno del dueño de la información y de la Oficina de TI y la autorización de su Jefe inmediato.
4. Cada usuario que acceda a la infraestructura tecnológica del Partido debe contar con un identificador de usuario (ID) único y personalizado, por lo cual no está permitido el uso de un mismo ID por varios usuarios.
5. Los usuarios y funcionarios son responsables de todas las actividades realizadas con su identificador de usuario (ID). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tiene prohibido utilizar el ID de otros usuarios.
6. Todo cambio en roles, funciones o cargo que requiera asignar al usuario atributos para acceso a diferentes prestaciones de la infraestructura tecnológica en El Partido, debe ser notificado a la oficina de TI por el Jefe inmediato.

## 1. Administración de privilegios

Cualquier cambio en los roles y responsabilidades de los usuarios deberán ser notificados a la oficina de TI para el cambio de privilegios.

## 2. Equipos desatendidos

Los usuarios deberán mantener sus equipos de cómputo con controles de acceso y con las contraseñas previamente instaladas autorizadas por la Oficina de TI.

### 3. Administración y uso de contraseñas

1. La asignación de contraseñas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.
2. Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá acudir a la Oficina de TI para que se le proporcione una nueva.
3. Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso o dejarlas en un lugar donde personas no autorizadas puedan descubrirlas.
4. Sin importar las circunstancias, las contraseñas nunca se deben compartir o ser reveladas.

### 4. Controles para otorgar, modificar y retirar accesos a usuarios

1. Todo usuario debe quedar registrado, en Usuarios y Roles del directorio activo del Partido. La creación de un nuevo usuario y/o solicitud para la asignación de otros roles, deberá venir acompañado del reporte debidamente firmado por el Jefe de Área.
2. La oficina de TI será la responsable de ejecutar los movimientos de, bajas o cambios de perfil de los usuarios.

## X. SOFTWARE

### 1. Adquisición

1. El área de Tecnología Informática (TI), establecerá los mecanismos de sustitución de sistemas y programas informáticos.
2. El área de Tecnología Informática (TI), será la encargada de recomendar la adquisición de programas informáticos de vanguardia, de acuerdo con lo estipulado en los lineamientos sobre especificaciones técnicas para la adquisición de equipos y programas de informática del Partido.
3. El área de Tecnología Informática (TI), será la encargada de asesorar y apoyar técnicamente para mantener actualizado los estándares de configuración de los sistemas operativos, programas comerciales, base de datos y comunicaciones.
4. Para la adquisición de nuevas licencias o actualizaciones de sistemas operativos, programas comerciales, base de datos y comunicaciones, equipos, accesorios y repuestos informáticos, será el área de Tecnología Informática (TI) quien proporcione la asesoría y opinión técnica, además de autorizar la adquisición de lo descrito anteriormente.
5. Los usuarios y funcionarios que requieran la instalación de software que sea propiedad del Partido, deberán justificar su uso y solicitar su autorización al proceso TI con el visto bueno de su Jefe inmediato, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que será usado.

6. Se considera una falta grave que los usuarios o funcionarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red del Partido, que no esté autorizado por TI.
7. En el proceso de reinstalar un programa el personal de TI debe borrar completamente la versión instalada para luego proceder a instalar la nueva versión que desea, esto siempre y cuando no sea una actualización del mismo.

## 2. Instalación de software

1. Corresponde al área de sistemas, la instalación y supervisión del software básico para cualquier tipo de equipo informático.
2. El área de Tecnología Informática (TI), es la responsable de brindar asesoría y supervisión para la instalación de software informático y de telecomunicaciones.
3. El área de Tecnología Informática (TI), será responsable que en los equipos de informática, de telecomunicaciones y en dispositivos basados en sistemas informáticos, únicamente se instalen software con licenciamiento propiedad del Partido y acorde a los derechos que la licencia lo indique.
4. La instalación y uso de paquetes y programas informáticos gratuitos (freeware) o sin costo alguno para El Partido, será autorizado por el área de Tecnología Informática (TI), respetando la ley de propiedad intelectual.
5. El área de Tecnología Informática (TI), proporcionara asesoría y apoyo técnico por medio de la instalación de versiones actualizadas, que ayuden a solventa problemas detectados o modificaciones que contribuyen a mejorar la utilización de los equipos informáticos para las áreas.
6. Se prohíbe la instalación de programas que no posean su licencia de software, juegos u otro programa informático que no tengan relación con las funciones y actividades que el funcionario desempeñe en su lugar de trabajo. El área de Tecnología Informática (TI), monitoreara su cumplimiento. El área de TI realiza periódicamente un inventario físico de los programas y software instalados en cada uno de los computadores del Partido.
7. Está prohibida la instalación de software que pudiera poner en riesgo los recursos o la información del Partido. El no cumplimiento de este numeral será sancionado de acuerdo al reglamento interno de trabajo vigente.
8. Para proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan como mínimo de software de seguridad (antivirus, vacunas, firewall software, etc.), u otros.
9. La protección y manejo de los sistemas y programas informáticos, corresponde a las personas o grupos que se les asigna y les compete notificar cualquier problema de estos a su jefe inmediato, quien deberá informar al área de sistemas para proporcionar una solución oportuna a dicho problema.

## 3. Actualización de software

1. Corresponde a la Secretaría General a través del área de Tecnología Informática (TI) autorizar cualquier adquisición y actualización de software.
2. Las actualizaciones del software de uso común las llevará a cabo el área de Tecnología Informática (TI), y se hará de acuerdo a las necesidades del Partido.

## 4. Auditoría del software instalado

1. El área de Tecnología Informática (TI), será la responsable de realizar la auditoria de software instalado.
2. El área de Tecnología Informática (TI), realizará, al menos una vez al año, revisiones de los equipos informáticos, para asegurar que los programas instalados, cuenten con las licencias vigentes.
3. Los funcionarios, cuyas computadoras cuenten con software instalado de versión de prueba, en caso de necesitar licencia válida, deberá presentar la necesidad y justificación para adquisición del software al área de sistemas a través de la Secretaría General o a través del Jefe inmediato.

## 5. Software propiedad del Partido

1. Todo programa adquirido por El Partido sea por desarrollo interno, compra, donación o cesión, es propiedad del Partido y mantendrá los derechos que la ley de propiedad Intelectual le confiera.
2. Todos los programas, bases de datos, sistemas operativos, interfaces, desarrollados con recursos del Partido, se mantendrán como propiedad del Partido respetando la propiedad intelectual del mismo.
3. El software disponible en cada equipo informático es propiedad del Partido, quedando prohibida su distribución y reproducción.
4. Los códigos fuentes de los sistemas de información, deberán estar en el área de Tecnología Informática (TI) para efectos de custodia y control.
5. El área de Tecnología Informática (TI), en coordinación con el área Administrativa y Financiera, a través del sistema de inventario del Partido, podrá verificar el registro de las licencias, sistemas y programas informáticos propiedad del Partido.
6. Es obligación de todos los usuarios que manejen información, mantener el respaldo correspondiente de la misma, ya que se considerara como un activo del Partido que debe preservarse.
7. Corresponderá al Partido, el promover y difundir los mecanismos para realizar el respaldo de los datos y los sistemas de información existente, de acuerdo a las políticas para la ejecución de backup y recuperación de información, según lo estipulado en las políticas y procedimientos de los Controles Generales de los Sistemas de Información de las Normas Técnicas de Control Interno Especificas del Partido.
8. Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de del Partido deberán estar debidamente resguardados.

### 6. Controles contra virus o software malicioso

1. Los usuarios del Partido deben verificar que la Información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software de antivirus autorizado por el proceso de TI.
2. Todos los archivos de computadoras que sean proporcionados por personal externo o interno como programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.
3. Ningún funcionario, empleado o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización del proceso de TI.
4. Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y notificará al proceso de TI para la revisión y erradicación del virus.
5. Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sea implantadas por TI en: Antivirus, Outlook, office, Navegadores u otros programas.
6. Debido a que algunos virus son extremadamente complejos, ningún usuario o funcionario del Partido, distinto al personal del proceso TI deberá intentar erradicarlos de las computadoras.

## XI. USO DE DISPOSITIVOS EXTRAÍBLES

1. El uso de los quemadores externos o grabadores de disco compacto es exclusivo para backups o copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.
2. El funcionario que tengan asignados estos tipos de dispositivos serán responsables del buen uso de ellos.
3. Si algún área por requerimientos muy específicos del tipo de aplicación o servicios de información tengan la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por TI con el respectivo visto bueno de la Dirección Administrativa y Financiera.
4. Todo funcionario del Partido deberá reportar al proceso de TI el uso de memorias, USB asignadas para su trabajo y de carácter personal y responsabilizarse por el buen uso de ellas.

# XII. UTILIZACIÓN DE RECURSOS DE REDES

1. Corresponde al área de sistemas el administrar, mantener y actualizar la infraestructura de la red del Partido.
2. Los usuarios del Partido no deben tener acceso físico y/o manipulación de los servidores, switches, routers, puntos y elementos activos de red y las bases de datos que almacenan información privilegiada y transacciones propias del Partido. Estas acciones serán realizadas única y exclusivamente por el personal de la Oficina de TI autorizados para realizar estas labores.
3. Se prohíbe a los usuarios del Partido, transmitir, acceder o recibir vía Internet, haciendo uso de las redes o equipos de cómputo del Partido información con contenido que pudiera ser discriminatorio, ofensivo, obsceno, amenazante, intimidante o destructivo para cualquier individuo u organización. Ejemplos de contenido inaceptable incluyen, entre otros, comentarios en general o imágenes con contenido sexual, discriminación racial, otro tipo de comentarios o imágenes que pudieran ofender a algún individuo con base en su raza, edad, orientación sexual, creencias religiosas, orientación política, nacionalidad, limitaciones físicas o cualquier otra característica especial protegida por la ley.
4. Los recursos disponibles a través de la red, serán de uso exclusivo para asuntos relacionados con las actividades del puesto de trabajo y del lugar donde está asignado.

# XIII. USO DEL CORREO ELECTRÓNICO

1. Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe re-direccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa al Partido, a menos que cuente con la autorización del proceso de TI.
2. Los usuarios y funcionarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad del Partido. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.
3. Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan encriptados y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y responsabilidades.
4. Queda prohibido falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.
5. Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

# XIV. SUPERVISIÓN Y EVALUACIÓN

1. Es responsabilidad del área de Tecnología Informática (TI), la supervisión y evaluación de los sistemas de información que involucren aspectos de seguridad lógica y física, las cuales deberá realizarse cada año.
2. Los sistemas de información institucional deben estar bajo monitoreo y actualización permanente.
3. Los usuarios del Partido deben conservar los registros o la información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial.
4. Las actividades que realicen los usuarios serán registradas y podrán ser objeto de auditoría.

## 1. Identificación incidentes

1. El usuario que detecte o tenga conocimiento de la posible ocurrencia de un incidente de seguridad informática deberá reportarlo al proceso de TI lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.
2. Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización competente, el usuario deberá notificar a TI.
3. Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información del Partido debe ser reportado al proceso de TI.

## 2. Logs de aplicaciones sensibles

1. Todas las aplicaciones de producción que manejen información sensible del Partido, deben generar logs que muestren cada modificación, incorporación y borrado de la información. Esto incluye modificaciones a los sistemas de producción y modificaciones a los sistemas fuente.
2. Los sistemas que manejen información valiosa, sensible o crítica deben además contener y activar forzosamente el log sobre todos los eventos o procesos relacionados con la seguridad de acceso a los mismos. Ejemplo: Varios intentos de contraseña, intentos de uso de privilegios no autorizados, entre otros. Los logs de procesos relevantes deben de proveer información suficiente para soportar auditorías y contribuir a la eficiencia y cumplimiento de medidas de seguridad.
3. Todos los comandos emitidos por los operadores de sistemas deben ser rastreables o identificables para especificar su uso individual.
4. El período que debe activarse y depurarse un log es por lo menos cada mes.

Durante este período, el administrador del sistema y/o dueño de la información, se debe asegurar que éste no sea modificado, y cerciorarse de que no sea leído por personal no autorizado. Estos aspectos son importantes para la corrección de errores, auditorías o brechas de seguridad.

5. Para evitar conductas inapropiadas, crear un sentido de responsabilidad del usuario, y permitir una administración adecuada de los sistemas, todas las actividades de los usuarios que afecten producción deben ser trazables desde el log. Las aplicaciones y otros manejadores de Bases de Datos, deben tener logs para las actividades de los usuarios y estadísticas relacionadas a estas actividades que les permitan identificar y detectar alarmas de posibles problemas o mal uso, y que reflejen eventos misionales de la institución sospechosos. El objetivo es que todos los movimientos que se realizan dentro de las operaciones críticas o sensibles del partido, sean registrados, para detectar y reducir el riesgo de violación o fraudes. Estas herramientas sirven como evidencia y apoyo para la detección de la fuente del problema ocasionado, identificando sus posibles causas y posibles soluciones.

# XV. POLÍTICA Y REGLAMENTO PARA LA OPERACIÓN DEL SITIO WEB

1. El Partido entiende el sitio web como un medio de comunicación en todo lo relativo a contenidos e imagen gráfica, entendidos estos como: el carácter institucional del Partido y la comunicación externa e interna, reconoce y asume el valor de este espacio virtual como herramienta de promoción, comunicación y apoyo permanente a todos sus procesos.
    a) La Oficina de TI como proceso de gestión tecnológica tiene la responsabilidad de garantizar la integridad de la información.
    b) Está prohibido la publicación de información privada o sensible sin la respectiva autorización del personal involucrado.
    c) Todos los contenidos que aparecen en la página Web, son responsabilidad del área que los emite.
2. Antes de publicar la información en la página web se debe verificar la redacción y ortografía.
3. El nombre de dominio *"www.partidodelau.com"* y todos aquellos que sirvan para acceder de forma directa al sitio oficial son de propiedad exclusiva del Partido. La indebida utilización de los mismos supondría una infracción de los derechos conferidos por su registro y será perseguido por los medios previstos en la Ley.
4. Quedan exceptuados de esta protección aquellos archivos o programas de computador que no sean de propiedad del Partido y de acceso gratuito o aplicaciones que tienen el carácter de dominio público por voluntad de sus autores.

5. Cualquier link o vínculo a páginas externas al Partido, deberá ser autorizado por la Oficina de Informática y la Secretaria General.
6. Toda solicitud para realizar cambios o publicaciones en la página web debe estar sustentada por un comunicado escrito o correo electrónico.

# XVI. CONTROLES PARA LA GENERACIÓN Y RESTAURACIÓN DE COPIAS DE SEGURIDAD (BACKUPS)

Se deberán considerar como mínimo los siguientes aspectos:

1. Establecer como medida de seguridad informática la necesidad de realizar copias de respaldo o backups periódicamente de los equipos de cómputo administrativos y servidores.
2. Cada funcionario es responsable directo de la generación de sus backups o copias de respaldo de su información, asegurándose de validar la copia. También puede solicitar asistencia técnica para la restauración de un backups.
3. Conocer y manejar el software utilizado para la generación y/o restauración de copias de respaldo, registrando el contenido y su prioridad.
4. Contar con almacenamiento interno o externo de las copias de respaldo, o verificar si se cuenta con custodia para ello.
5. Las copias de seguridad o Backups, se deben realizar al menos una vez a la semana, periódicamente el proceso de TI realizará un seguimiento del cumplimiento de este procedimiento y registrará en el formato de Copias de Seguridad.

# XVII. DEFINIR PLANES DE CONTINGENCIA ANTE DESASTRES

**Definición:** Se entiende por PLAN DE CONTINGENCIA los procedimientos alternativos a la operación normal en una organización, cuyo objetivo principal es permitir el continuo funcionamiento y desarrollo normal de sus operaciones, preparándose para superar cualquier eventualidad ante accidentes de origen interno o externo, que ocasionen pérdidas importantes de información. Estos deben prepararse de cara a futuros sucesos.

1. Asegurar, recuperar o restablecer la disponibilidad de las aplicaciones que soportan los procesos de misión crítica y las operaciones informáticas que soportan los servicios críticos del Partido, ante el evento de un incidente o catástrofe parcial y/o total.
2. Disponer de plataformas computacionales, comunicaciones e información necesarias para soportar las operaciones definidas como de misión crítica de negocio en los tiempos esperados y acordados.
3. Tener en existencia equipos informáticos de respaldo o evidencia de los proveedores, de la disponibilidad de equipos y tiempos necesarios para su instalación, en préstamo, arriendo o sustitución.
4. Actualización periódica del plan de recuperación ante desastre de acuerdo con los cambios en plataformas tecnológicas (hardware, software y comunicaciones), para reflejar permanentemente la realidad operativa y tecnológica de la compañía.
5. Disponer de copias de respaldo (externas) para restablecer las operaciones en las áreas de misión crítica definidas.