Procedimiento sobre seguridad de la información en la Procuraduría General de la República.

Este documento está amparado en la Política sobre Seguridad de la Información y tiene como propósito brindar el detalle sobre seguridad de la información en la PGR, el documento se divide en 6 procedimientos los que se detallan a continuación.

1. Procedimiento para asignación y uso de equipo de cómputo a usuarios de la PGR

1.1. La Institución establece en sus presupuestos anuales el monto correspondiente para la dotación de equipo de cómputo y software necesario para que cada usuario realice su labor operativa.
1.2. A cada usuario se le asigna un equipo de cómputo, la responsabilidad sobre el uso del equipo es del usuario. Si ocurre algún imprevisto (robo, deterioro, perdida), el usuario debe hacerlo saber de manera inmediata al departamento de control de Bienes.
1.3. A los Procuradores, Abogados Asistentes, Analistas de Sistemas y Jefes de Departamento se les asigna un equipo de cómputo portátil.
1.4. Al personal administrativo se le asignará equipo de cómputo estacionario.
1.5. Si un funcionario como parte de su trabajo debe salir del país y requiere trasladar el equipo de cómputo asignado puede hacerlo, siempre y cuando sea una gira laboral estrictamente.
1.6. El software establecido para cada equipo de cómputo depende del perfil de funcionario y los procesos que deba realizar.

Los perfiles establecidos son:

- Secretarias
- Asistentes Administrativos
- Asistentes Abogados
- Procuradores
- Coordinadores de Área
- Jefes Administrativos
- Diseñadores de Software

- Soporte Técnico

1.6.1. La instalación de software en los equipos de cómputo es responsabilidad absoluta del personal del núcleo de informática de la PGR.

1.6.2. El proceso específico para instalación de software es el siguiente:

1.6.2.1. Instalación de software en equipo nuevo, que se entrega a un usuario:

- El soportista técnico revisa el equipo e instala todos los componentes que garanticen el buen funcionamiento del equipo.
- El soportista técnico revisa el perfil del usuario para determinar el software que requiere.
- Se verifica con el encargado de custodia de licencias la disponibilidad de las mismas.
- El encargado de custodia, entrega y registra las licencias correspondientes.
- El soportista instala lo que corresponda y hace las pruebas necesarias.
- El soportista asigna en el sistema de gestión de incidencias el equipo al usuario e imprime la boleta de entrega.

1.1.1.2. Instalación de software en equipo que se encuentra asignado:

- El usuario registra un incidente solicitando la instalación del software.
- El soportista técnico recibe la solicitud y verifica el perfil de usuario además verifica con el encargado de custodia de licencias la disponibilidad de licencias, si se trata de software de uso libre se debe verificar si es software permitido en la PGR.
- Si al perfil de usuario no le corresponde la licencia, el soportista técnico consulta al encargado del Núcleo de Informática sobre la necesidad de la instalación.
- El encargado del Núcleo de Informática verifica con el superior inmediato del solicitante sobre la necesidad del software solicitado y brinda la autorización si es requerido.

2. Procedimiento de seguridad de la información.

2.1. Los usuarios deben apegarse al uso de los sistemas de información definidos en la Institución para la generación de escritos y oficios, todos esos documentos se generan y almacenan en la plataforma creada por Informática para ese fin.

2.2. Todos los equipos de los usuarios finales cuentan con la herramienta de protección como es el antivirus corporativo.

2.3. El acceso a internet y descargas de información están regulados por los firewalls respectivos.

2.4. La información adicional a escritos y oficios que genere el usuario debe quedar en una carpeta denominada c:\NombreUsuario, la cual se respaldará de manera automática (según la política de respaldo de información institucional). En esa carpeta no es permitido el respaldo de información personal (fotos, videos, otros documentos).

2.5. Los documentos relacionados a la labor sustantivan como son: notificaciones, adjuntos, escritos y otros, se almacenan en la plataforma de gestión de documentos Visión2020.

2.6. La PGR cuenta con un sistema para recibir documentos firmados digitalmente, cualquier documento que sea remitido a la PGR firmado digitalmente se recibe únicamente mediante la plataforma web denominada "Ventanilla Electrónica".

3. Procedimiento definición y uso de contraseñas.

3.1. Todo funcionario de la PGR cuanta con contraseñas para ingresar a la plataforma tecnológica.
3.2. El cambio de contraseñas se realiza cada 6 meses.
3.3. Todas las contraseñas de usuario de sistema de información están integradas con la contraseña general (active directory).
3.4. Las contraseñas deben ser tratadas con carácter confidencial.
3.5. Las contraseñas de ninguna manera podrán ser transmitidas mediante servicios de mensajería electrónica instantánea ni vía telefónica.
3.6. El usuario debe evitar revelar contraseñas en cuestionarios, reportes o formularios.
3.7. El usuario debe evitar activar o hacer uso de la utilidad de recordar clave o recordar Password de las aplicaciones.
3.8. La responsabilidad del uso de las contraseñas es responsabilidad única del usuario.

4. Procedimiento para el uso de dispositivos de almacenamiento externo.

4.1. El uso de dispositivos de almacenamiento externo está permitido en la PGR.
4.2. Es responsabilidad del usuario final el uso que le dé a la información que trasiega en los dispositivos externos de almacenamiento.
4.3. El Núcleo de Informática concientizará a los funcionarios, de la institución sobre los riesgos asociados con el uso de los medios de almacenamiento externo, tanto para los sistemas de información como para la infraestructura tecnológica de la institución.
4.4. El Núcleo de Informática mediante el software de protección institucional velará para que los dispositivos de almacenamiento utilizados por los usuarios finales estén libres de software malicioso, espía o virus para lo cual realizará de manera automática una verificación de dichos dispositivos cada vez que sea conectado a un equipo de cómputo de la Institución.

Procedimiento para el uso de conexiones remotas

4.5. El uso de conexiones remotas está permitido solo por medios de redes privadas virtuales (en inglés, Virtual Private Network (VPN).
4.6. El acceso remoto solo es permitido desde equipo institucional.
4.7. Es responsabilidad del Núcleo de Informática restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se permitirá los accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con lo que determine el departamento de Recursos Humanos.
4.8. Es responsabilidad del usuario mantener la confidencialidad y protección de la información a la que tienen acceso fuera de las instalaciones Institucionales.
4.9. Es responsabilidad del usuario dar aviso al Núcleo de Informática sobre cualquier posible abuso o intento de violación tanto de los accesos como de las credenciales entregadas.

5. Procedimiento uso de convenios

5.1. Los accesos a los diferentes convenios (Asamblea Legislativa, Registro Nacional, Hacienda, Ministerio de Justicia etc), se habilitarán mediante solicitud de la jefatura inmediata al encargado del Núcleo de Informática.