POLITICAS DE SEGURIDAD DE LA INFORMACION

Contenido

POLITICAS DE SEGURIDAD DE LA INFORMACION

INTRODUCCION

La Dirección Nacional de Tecnologías de la Información, es la dependencia responsable de establecer normas, estándares, políticas y metodologías en lo relacionado a redes, sistemas operativos, equipos, bases de datos, desarrollo de sistemas y comunicaciones informáticas, tanto para la Fiscalía General del Estado como para las entidades con las que comparte sistemas informáticos; definir criterios y velar por el cumplimiento de los mecanismos de disponibilidad, seguridad y acceso a la información que administra la Institución.

Asimismo, tiene a su cargo asegurar el buen funcionamiento de los sistemas informáticos, que sirvan a los procesos técnicos y administrativos internos; desarrollar nuevas aplicaciones, a través de un análisis constante de las necesidades de usuarios, por medio de desarrollo interno o externo, entre otras.

Por lo expuesto y en base a las atribuciones legales y reglamentarias que tiene esta dirección se presentan a continuación las **POLITICAS SOBRE SEGURIDAD DE LA INFORMACIÓN,** contenidas en los siguientes términos:

1.- RESPONSABILIDAD DEL USUARIO Y CONCEPTOS GENERALES

1. El sistema informático multiusuario y/o conectado por red a la Fiscalía General Del Estado, requiere unas medidas de seguridad que garanticen la privacidad de la información frente a posibles intrusiones internas (usuarios que comparten un mismo sistema) o externas (usuarios procedentes de otros sistemas).

2. La protección del sistema no sólo es tarea del administrador sino también de sus usuarios.

3. Por útiles y/o herramientas de trabajo puede entenderse a todos los elementos puestos a disposición del funcionario o empleado por parte de la Fiscalía, directamente vinculados con la prestación de servicios, bien por resultar imprescindibles para su desenvolvimiento o bien por facilitarla.

4. Dentro de las Tecnologías de la Información a la Comunicación que mantiene la Fiscalía de la República como herramientas de trabajo tendríamos –entre otras- a los teléfonos, telefax, correo electrónico, las computadoras y todas sus partes integrantes y accesorias, las impresoras, fotocopiadoras y escáneres, el acceso y navegación en Internet, las diferentes aplicaciones y recursos Informáticos que se puedan facilitar mediante la intranet institucional, las bases de datos, los programas, documentos, archivos y carpetas de archivos subidos en la red de la Fiscalía.

5. El mal uso de los útiles y las herramientas de la institución y la inobservancia de las normas contenidas en esta política por parte de los funcionarios y empleados de la Fiscalía General Del Estado será sancionado de conformidad con el régimen disciplinario vigente y las infracciones informáticas establecidas en el Código Penal atendiendo a la gravedad de la violación.

2.- SEGURIDAD FISICA

2.1.- EQUIPAMIENTO

1. Los equipos de la Institución sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.
2. No se permite fumar, comer o beber mientras se está usando una estación de trabajo.
3. Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).
4. Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso.
5. La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportado a la Dirección Nacional de Tecnologías de la Información inmediatamente detectado el incidente.
6. Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño.
7. Cualquier falla en los computadores o anomalía en la red debe reportarse inmediatamente al personal de la Dirección Nacional de Tecnologías de la Información, para evitar posibles problemas serios como pérdida de la información o indisponibilidad de los servicios.
8. Debe respetarse y no modificar la configuración de hardware y software establecida por la Dirección Nacional de Tecnologías de la Información.
9. Ningún equipo que pertenece a la Institución puede moverse o ser reubicado sin permiso. Para llevar un equipo fuera de la Institución se requiere una autorización escrita emitida por parte del Director Nacional de Tecnologías de la Información o un funcionario encargado.
10. Los **gabinetes** (armarios del cableado estructurado) donde se ubican los switches deben ser protegidos y no deben ser obstruidos para tener libre acceso.

2.2.- CABLEADO ELECTRICO

1. Ante un corte del suministro de energía eléctrica debe apagarse los equipos, hasta que se normalice el fluido eléctrico.

2.3.- CONTROL DE ACCESO FÍSICO A OFICINAS Y ZONAS RESTRINGIDAS

1. El personal podrá permanecer en las instalaciones de la Institución durante el **horario autorizado.** Se deberá establecer un procedimiento de autorización para el personal que deba permanecer fuera de su horario habitual de trabajo.
2. Únicamente los funcionarios de la Dirección Nacional de Tecnologías de la Información tienen acceso al **área del centro de cómputo** donde se encuentran los servidores, los switches de comunicaciones y demás equipamiento crítico.

3. Ninguna persona sin autorización previa podrá ingresar al área del **centro de cómputo,** para reducir el riesgo de accidentes y actividades fraudulentas.
4. Toda persona que ingrese a las áreas restringidas, debe registrarse y requerirá autorización para ingresar.
5. Cualquier **persona ajena a la Institución** que necesite ingresar al centro de cómputo deberá anunciarse con un funcionario de la dirección, un personal de sistemas lo escoltará desde la puerta hacia el interior del centro de cómputo y lo acompañará durante el transcurso de su tarea, hasta que ésta concluya.

2.4.- CONTROL DE APLICACIONES EN ESTACIONES DE TRABAJO

1. Los usuarios deben asumir que todo el software de la Institución está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales. Así también está prohibida la instalación de software que no haya adquirido la Institución.
2. No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Director de Informática o un delegado.
3. Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el Director de Informática o un delegado.
4. Debe utilizarse un programa antivirus para examinar todo software que venga de fuera de la Institución.
5. No deben usarse diskettes u otros medios de almacenamiento en cualquier computadora de la Institución a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.

2.5.- CONTROL DE DATOS EN LAS APLICACIONES

1. Los datos de entrada y salida a los diferentes sistemas propios o adquiridos son validados en cada sistema e ingresados solo desde las estaciones de trabajo que poseen los permisos de acceso necesarios de cada usuario final.
2. Los datos de salida de los diferentes sistemas utilizados en la Institución son restringidos con controles lógicos de acuerdo a los permisos de acceso, es responsabilidad del usuario final salvaguardar la información.
3. Todas las aplicaciones y sus archivos poseen controles de acceso es responsabilidad del usuario final conservarlos.

2.6.- CICLO DE VIDA DE LAS APLICACIONES DESARROLLADAS O ADQUIRIDAS

1. Las **aplicaciones se actualizarán** cuando exista el reporte de algún mal funcionamiento o por un nuevo requerimiento del usuario final.
2. Debe existir un documento formal de solicitud de cambios, donde quede reflejado el motivo y la solicitud del cambio, allí se agregarán los requerimientos de seguridad

necesarios, definidos por el responsable de la información y el administrador de sistemas. La documentación de los cambios debe incluir:

a. sistema que afecta,
b. fecha de la modificación,
c. desarrollador que realizó el cambio,
d. funcionario que solicitó el cambio,
e. descripción global de la modificación.

3. Este documento se utilizará para actualizar la documentación del desarrollo y de los distintos manuales generados.
4. Todo nuevo desarrollo o modificación deber estar probado y aprobado por los usuarios del mismo antes de su instalación en el ambiente de trabajo.
5. Las modificaciones en los sistemas adquiridos, solo se realizarán por personal técnico de la Empresa a la que le pertenece el producto.

3.- SEGURIDAD LÓGICA#

3.1.- ASPECTOS GENERALES

1. Las estaciones de trabajo desatendidas deben ser bloqueadas por sus usuarios**.**
2. Cuando un funcionario es despedido o renuncia a la Institución, debe desactivarse su cuenta antes de que deje el cargo.
3. Los privilegios otorgados a los usuarios deben ser ratificados cada año. El encargado de la Dirección Nacional de Tecnologías de la Información debe bloquear la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un funcionario cesa en sus funciones.

3.2.- IDENTIFICACION DE USUARIOS

1. Para **ingresar a un usuario** al sistema (**dar de alta**) debe exigirse los siguientes datos:
   a. nombres y apellidos completo,
   b. identificación única e irrepetible del usuario,
   c. unidad administrativa a la que pertenece,
   d. permisos de acceso.
2. Cada cuenta de usuario debe contar con los permisos mínimos y necesarios que le permitan desempeñar su tarea.
3. Debe restringirse el acceso al sistema o la utilización de recursos en un **rango de horario definido**, teniendo en cuenta que:
   a. las cuentas de los usuarios no deben poder acceder al sistema en horarios no laborales, de acuerdo al grupo al que pertenezcan,
   b. durante las vacaciones o licencias las cuentas de usuarios deben desactivarse,
   c. en días feriados las cuentas de usuarios administrativos, deben permanecer desactivadas.

3.3.- AUTENTICACIÓN EN LA RED

1. Todo usuario, para **el ingreso a la red (inicio de sesión)** debe registrar su credencial de acceso:
   a. nombre de usuario,
   b. contraseña,
   c. dominio.

2. Mientras el usuario está **ingresando su contraseña**, esta no debe ser mostrada por pantalla o visualizada al ser digitada.

3.4.- LAS CONTRASEÑAS (PASSWORDS)

1. Las contraseñas deben incluir mayúsculas, minúsculas, números y caracteres especiales.
2. La longitud mínima de una contraseña no debe ser menor de 8 caracteres.
3. La **fecha de expiración** de las contraseñas es de 30 días. El sistema exigirá automáticamente el cambio, una vez cumplido el plazo.
4. La contraseña **no deberá contener** el nombre de la empresa, el nombre del usuario, o palabras que sean asociadas con el usuario.
5. Se bloqueará la cuenta de red de todo usuario que haya intentado **acceder al sistema en forma fallida** por más de **cinco** veces consecutivas.
6. Se debe controlar que la contraseña ingresada sea **diferente a las últimas diez utilizadas**.
7. Si un usuario **olvida su contraseña**, solicitará a un técnico de soporte informático, el cual realizara el procedimiento para eliminar la contraseña, y permitirá que el usuario ingrese una nueva desde su terminal la próxima vez que ingrese a la red.
8. No se debe compartir la contraseña a ningún usuario o administrador de la red, el compartir expone al usuario a las consecuencias por las acciones que otros hagan con esa contraseña.
9. El usuario no debe guardar su contraseña en una forma legible y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada.
10. La contraseña inicial emitida a un nuevo usuario o a un usuario cuyo equipo ha sido reparado, sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.
11. Las contraseñas predefinidas que traen los equipos nuevos tales como switchs, firewalls, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.
12. Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la Institución.
13. Para cambiar la contraseña de un usuario ausente, solo el Jefe inmediato o su Director puede solicitar borrar la contraseña, para que se pueda registrar otra.
14. Por ningún concepto y bajo ninguna circunstancia un usuario puede usar la credencial de acceso de otro usuario.
15. Cuando un usuario ha sido reubicado de su puesto de trabajo es responsabilidad del Director de Recursos Humanos o si el cambio es interno del Director de la unidad administrativa, notificar los movimientos de personal a la Dirección Nacional de Tecnologías de la Información, con la finalidad de realizar el intercambio de información y permisos de acceso lógicos a los sistemas de los usuarios involucrados.

4.- SEGURIDAD DE COMUNICACIONES

4.1.- ASPECTOS GENERALES

1. Es política de la Institución no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones será supervisado

ocasionalmente en caso de ser necesario para actividades de mantenimiento, seguridad o auditoría. Puede ocurrir que el personal técnico vea el contenido de un mensaje de un empleado individual durante el curso de resolución de un problema.

2. Los empleados y funcionarios de la Institución no deben interceptar las comunicaciones o divulgar su contenido, tampoco deben ayudar a otros para que lo hagan así también se hacen responsables del buen uso de sus redes de comunicación. La Institución se compromete a respetar los derechos de sus empleados, incluyendo su privacidad.
3. De manera consistente con prácticas aceptadas, la Institución procesa datos estadísticos sobre el uso de los sistemas de comunicación. Como ejemplo, los reportes de la central telefónica, que contienen detalles sobre el número llamado su duración, la hora en que se efectuó, etc.

4.2.- LA INFORMACION

1. Por Políticas Generales se prohíbe la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información propietaria de la Institución.
2. El Fiscalía General Del Estado es el único propietario de toda la información que se derive de cualquier actividad o trabajo de investigación que realicen los funcionarios.

4.3.- USO DE LOS SISTEMAS DE COMUNICACIÓN

1. Se debe promover el uso responsable de las comunicaciones, en particular el teléfono, el correo electrónico, sistema de comunicación interna (COMUNICATOR) y el fax. Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, se deben considerar como propiedad de la Institución y no propiedad de los usuarios de los servicios de comunicación.
2. Los sistemas de comunicación de la Institución generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del funcionario ni con las actividades de la Institución.
3. Se debe prohibir el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.
4. La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la Institución y en tal sentido deben usarse las horas no laborables.

4.4.- CONEXIONES EXTERNAS

1. La conectividad a Internet se debe otorgar para propósitos relacionados con las actividades de la Institución. Los usuarios no autorizados deben ser imposibilitados de conectarse al exterior.
2. Cada vez que se establezca una vía de comunicación con terceros (personal de mantenimiento externo, proveedor de servicios de Internet, etc.), los mecanismos de transmisión y las responsabilidades de las partes deberán fijarse por escrito.

3. El uso de Internet debe ser monitoreado periódicamente. Si existe alguna razón para creer que la seguridad está siendo violada o existe algún abuso en particular, personal designado puede revisar el contenido de las comunicaciones de Internet.
4. El acceso casual a los mensajes de correo electrónico por los administradores y similares, se considera una violación a la política de seguridad de la información. Sin embargo, la Dirección Nacional de Tecnologías de la Información tiene el derecho de examinar cualquier información, sin previo consentimiento o notificación del funcionario, en caso que se considere que se está utilizando inadecuadamente el equipamiento del Fiscalía General Del Estado.

4.5.- EL CORREO ELECTRONICO

1. Los mensajes de correo electrónico deben ser considerados como documentos formales y deben respetar todos los lineamientos referentes al uso inapropiado del lenguaje.
2. Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.
3. El correo electrónico no debe ser utilizado para enviar **cadenas de mensajes**, no debe relacionarse con actividades ilegales y no éticas o para mensajes no relacionados con los propósitos de la Institución.
4. El tamaño máximo de un archivo adjunto en un mensaje de correo electrónico es de 5 MB, y no debe ser de tipo EXE, BAT, COM, PPS, entre otros. Esta definición se utiliza tanto para enviar como para recibir mensajes.