PLANEACIÓN Y DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA GOBERNACIÓN DE NARIÑO.

GOBERNACIÓN DE NARIÑO, 2015.

TABLA DE CONTENIDO

I- INTRODUCCIÓN

La Seguridad de la Información es importante tanto para los organizaciones, entidades públicas y privadas; de aquí que el Activo más importante en una institución es la INFORMACIÓN, por tal motivo es necesario tomar medidas para protegerla y salvaguardarla.

La organización, en este caso, la Gobernación de Nariño, debe implementar, establecer, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información SGSI, para preservar la confidencialidad, integridad y disponibilidad de la Información, para mantener los niveles de competitividad, de gestión pública y de conformidad legal necesarios para alcanzar las metas administrativas y, del plan departamental de desarrollo.

Es necesario, tener un control creando medios para la gestión del riesgo, incluyendo políticas, procedimientos, directrices, que se encuentran bajo el marco de referencia para la implementación del Sistema de Gestión de Seguridad de la Información, los cuales se basan en las normas internacionales NTC-ISO/IEC 27001 (Requisitos para conformar el SGSI) y la norma NTC/ISO IEC 17799 – 27002 (Implementación de SGSI), conocimientos obligatorios aplicados a los entes públicos departamentales, adoptando el modelo de seguridad de la información en el marco de la estrategia de Gobierno en Línea.

Por lo anterior, la Gobernación de Nariño dando cumplimiento al plan departamental de desarrollo 2012-2015 Nariño Mejor, especialmente en el eje Nariño Gobernable,

programa Desarrollo Institucional; promueve la modernización de la Entidad con base en la aplicación de procesos y procedimientos óptimos, apoyo de herramientas

tecnológicas y transformación de la cultura organizacional; y atendiendo al decreto 2693 de 2012 de MINTIC, se establecen los lineamientos de Gobierno en Línea y específicamente en el componente de elementos transversales, direccionados a las entidades públicas en la implementación de políticas en Seguridad de la Información, como mecanismos para disminuir el impacto de los riesgos potenciales en esta área.

II- OBJETO

Esta circular establece políticas, directrices, principios generales y prácticos para emprender, implementar, mantener y mejorar la gestión de la seguridad de la Información en la Gobernación de Nariño.

III- OBJETIVO

REDUCIR LOS RIESGOS DE: PÉRDIDA O DAÑO DE LA INFORMACIÓN, ACCESO NO AUTORIZADO A EQUIPOS Y/O SOFTWARE DEDICADO, POR MEDIO DE POLÍTICAS Y NORMAS DE USO.

IV- ALCANCE

Presentado a todos los funcionarios de la Gobernación de Nariño (sede principal) y sedes externas que prestan su servicio, y los cuales tienen acceso a la información, recursos propios de la entidad, ya sea equipos de cómputo, medios de almacenamiento externos (memorias USB, Discos Duros, etc.), y almacenamiento digital (correo electrónico, almacenamiento virtual).

V- RESPONSABILIDADES

Para alcanzar las metas propuestas en este Sistema de Gestión de Seguridad de la Información de la Gobernación de Nariño, es indispensable coordinar las actividades de Seguridad de la Información con representantes de todas partes de la Gobernación de Nariño, teniendo en cuenta roles y funciones laborales.

DIRECTORES O JEFES DE ÁREA

Directores o Jefes de Cada Área que conforman la Gobernación de Nariño:
Revisar con regularidad la implementación y el cumplimiento del proceso y procedimientos realizados con los Activos de la Información dentro de su área:

1. Establecer procedimientos para: manipulación, gestión, y destrucción (técnica, ambiental e industrial) de medios removibles.

2. Constituir manuales con procedimientos para la manipulación y almacenamiento de la información para evitar la divulgación no autorizada. Toda documentación de procedimientos debe ser protegida contra el acceso no autorizado.

3. Tener en cuenta la seguridad en oficinas (Recinto e Instalaciones), contra amenazas externas y ambientales.

4. Asumir y poner en práctica las estrategias proporcionadas por (Proceso Gestión TICs,) para prevenir la pérdida, daño, robo o compromiso de los activos de la información.

5. Identificar y documentar las reglas sobre el uso de la información y los activos asociados.

6. Establecer acuerdos para el intercambio de información y software entre Gobernación de Nariño (sede central) y partes externas; así mismo, realizar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información de la Gobernación de Nariño.

7. Implementar políticas y procedimientos para proteger información asociada con la interconexión de los sistemas de información de la Gobernación de Nariño.

8. Implementar normas para la clasificación de la Información en términos de su valor, requisitos legales, sensibilidad y criticidad para la organización.

9. Tener presente que los activos (equipos, información, software, etc.) no se deben retirar de su sitio sin autorización previa de (Proceso Gestión TICs.)

10. Todos los activos deben estar claramente identificados.

11. Precisar a todos los empleados y usuarios que deben devolver todos los activos a cargo al terminar su contrato, funciones o acuerdo.

12. Impulsar la política de escritorio limpio y pantalla limpia a los funcionarios a cargo.

13. Infundir la práctica de Respaldo de la Información; y el buen manejo de la información incluida en la Mensajería Electrónica (Correo Electrónico)

14. Exigir en cada dependencia la Política de Confidencialidad y no divulgación de la Información.

15. El jefe de cada dependencia debe implementar las políticas necesarias para recoger y almacenar su información, acordando mecanismos y tiempos para la realización del backup, y controlar el cumplimiento de este procedimiento.

16. Investigar al personal que va a ser contratado y hacer un control y seguimiento de la información que va a manipular.

17. Definir y documentar los roles y responsabilidades de los empleados, contratistas, y usuarios de terceras partes.

18. Se debe desarrollar e implementar periodos de registros donde se pueda evidenciar las actividades de los usuarios, excepciones, eventos de seguridad de la información; esto con el fin de facilitar investigaciones futuras, monitoreo y control de acceso al sistema.

19. Todos los funcionarios deben recibir capacitaciones sobre las políticas y procedimientos de la SGSI.

20. Se debe exigir a los empleados en general, emplear activamente el SGSI de acuerdo con las políticas y procedimientos durante y después de la terminación del contrato, cambio de empleados o cambio de funciones.

21. Exhortar a los empleados que sean conscientes de las amenazas y riesgos, con respecto a la Seguridad de la Información.

22. Permitir a los usuarios consultar los procedimientos operativos (documentados).

23. Hacer un análisis y posterior reporte de las posibles Debilidades en la Seguridad de la Información.

24. Debe existir un proceso formal disciplinario para emprender acciones legales contra empleados que hayan cometido alguna violación al SGSI.

25. Se recomienda gestionar una Auditoría Interna para la gestión de la seguridad de la información y su implementación debe ser revisada independientemente.

26. Toda la información (copias de seguridad) y activos, deben estar en custodia en una parte designada por la Gobernación de Nariño.

27. Organizar perímetros de seguridad para proteger las áreas que contienen información, el acceso a estas áreas sólo es para personal autorizado.

FUNCIONARIOS Y USUARIOS

Usuarios (Servidores Públicos en General) de la Gobernación de Nariño. El usuario debe atender todas las pautas o normas, impartidos desde (Proceso Gestión TICs.) y los Jefes de cada Área:

a) Todo empleado debe hacer uso diligente del SGSI, de acuerdo a las políticas y procedimientos planteados. Esto se debe aplicar cuando haya cambio de funciones, durante y después de la vigencia del contrato.

b) El no cumplimiento o desacato del SGSI, puede acarrear sanciones de índole legal.

c) Etiquetar toda la información, ya sea carpetas o archivos; con nombres claros o que haga alusión a su contenido, para una futura búsqueda exitosa.

d) Hacer Copias de Seguridad con regularidad, con el fin de proteger la información contra su pérdida o daño.

e) Ejercer buen uso de las contraseñas, tanto de Windows como las de software dedicado.

f) No usar programas que no tengan licencia, o que sean obtenidos fuera de (Proceso Gestión TICs.)

g) Tener precaución contra las amenazas externas y ambientales que puedan influir en los lugares de trabajo, e instalación eléctrica y cableado estructural.

h) A quienes tengan a cargo equipos de cómputo de la Gobernación de Nariño o utilicen equipos personales en las instalaciones de la Gobernación de Nariño, deben estar atentos para prevenir la pérdida, daño o robo de estos; los equipos deben estar en un lugar privilegiado para su protección, reduciendo los riesgos de amenazas y peligros del entorno, y las oportunidades para darse un acceso no autorizado.

i) El usuario debe tener un pacto de confidencialidad y no divulgación de la información que maneja, esto con el fin de que no pueda comprometer a la Gobernación de Nariño en difamación, acoso, suplantación de identidad, envío de cartas de cadena, adquisición de elementos sin autorización, etc.

j) El trabajador no está autorizado para hacer cambios o modificaciones a los paquetes de software instalado en el equipo; todos los cambios se autorizan y realizan estrictamente desde (Proceso Gestión TICs.)

k) Los Equipos de Reproducción (Impresoras, Fotocopiadoras, Scaner) deben estar ubicados en lugares con acceso controlado; por tanto, cualquier documento confidencial o sensible, se debe retirar inmediatamente del equipo. Igualmente tener precaución con el uso de papel reciclado.

l) Tener precaución cuando se hace uso de impresoras en red, considerar que el no tener en claro la dirección de red o nombre de la impresora, la impresión

puede hacerse en otro lugar, exponiendo la información contenida en la impresión.

m) Todos los activos deben estar claramente identificados; por tanto, cada funcionario esta en el deber de examinar y registrar los activos a cargo.

n) Todos los empleados y usuarios deben devolver todos los activos que están a su cargo al terminar su empleo, contrato o acuerdo.

o) El empleado o contratista debe informar a (Proceso Gestión TICs.), cualquier debilidad de seguridad de la Información observada o que se sospecha en los sistemas o servicios.

VI- TERMINOLOGÍA Y COMPLEMENTOS

1- LA INFORMACIÓN COMO ACTIVO DE LA ENTIDAD

La información es uno de los activos más valiosos de una organización, por lo tanto: la Información de propiedad de la Gobernación de Nariño, sus medios de almacenamiento y procesamiento, son considerados críticos para el cumplimiento de los procesos y objetivos de la Entidad.

En el uso y manejo de la Información hay que tener en cuenta las siguientes normas:

1-1. Toda información sensible para la Gobernación de Nariño debe estar protegida desde su recolección, seguido por su proceso y, hasta su almacenamiento o publicación. Toda la información deben estar en custodia en una parte designada por la Gobernación de Nariño.

1-2. Tener presente la papelera de reciclaje. Cuando se haya eliminado archivos, es conveniente “vaciar la papelera de reciclaje” cuándo se finalice la jornada; puesto que, cualquier persona puede recuperar estos archivos y obtener información; además, el acumular mucha información en la papelera, hace que el disco duro del equipo se llene inadvertidamente.

1-3. Las carpetas o archivos compartidos, deben estar restringidos para quienes no tengan autorización de su lectura o edición. Esta restricción se hace mediante permisos otorgados por parte del usuario dueño de estos archivos o carpetas. Lo mismo ocurre con los equipos compartidos, el usuario es

responsable de informar a (Proceso Gestión TICs.) si su equipo está en modo compartido, este modo es base para una intrusión desde un equipo externo pudiendo causar daño o robo de información.

1-4. Queda totalmente prohibido difundir información propia de la Gobernación de Nariño sin autorización a otros funcionarios internos o externos.

1-5. No se permite alterar o manipular información que vaya en contra de la Gobernación de Nariño.

1-6. Es necesario etiquetar toda la información, ya sea carpetas o archivos de diferente extensión; con nombres claros o que haga alusión a su contenido, para que en un futuro su búsqueda sea precisa.

1-7. Cuando el funcionario se ausente del puesto de trabajo, es su deber bloquear la sesión de trabajo para no dar pie a la sustracción de información no autorizada.

1-8. Cada funcionario es responsable de hacer copias de respaldo con regularidad, con el fin de proteger la información contra su pérdida o daño. Cuando sea necesario hacer un reseteo total del equipo, (Proceso Gestión TICs.) tiene la tarea de extraer la información de la partición distinta a (C:) del disco duro.

1-9. Todos los empleados y usuarios de terceras partes que tengan acceso a información sensible de la Gobernación de Nariño, deben firmar un acuerdo de confidencialidad y no divulgación.

1-10. Tener un control especial en áreas de acceso, despacho y/o carga donde pueda entrar personal no autorizado, esto con el fin de evitar el acceso no autorizado a la información.

1-11. Toda clase de información que se ponga al servicio público o dentro de la Gobernación de Nariño debe ser verificada y aprobada por el jefe dueño de la información.

1-12. Cuando se necesite hacer publicaciones con información externa, esta tiene que ser verificada. Los directores o jefes de área deben garantizar que se utilizan fuentes acreditadas.

1-13. Tomar precauciones para que la información no sea interceptada por ningún medio.

1-14. El usuario no debe registrar datos personales o datos de la entidad en ningún software, aplicación o portal web desconocido, esto con el fin de evitar su recolección y un uso posterior sin autorización.

1-15. No tener conversaciones de carácter confidencial en lugares públicos, ni oficinas abiertas, como tampoco en lugares de reunión, o donde no se tenga la seguridad que no están escuchando.

2- PANTALLA LIMPIA

Es la Protección de las computadoras, notebook, u otros dispositivos, mediante un bloqueo de pantalla o desconexión cuando no están en uso. Toda vez que el funcionario se ausente del lugar de trabajo debe dejar bloqueado su equipo, con el fin de proteger el acceso a la información de las aplicaciones y/o servicios de la Gobernación de Nariño. El protector de pantalla y/o Fondo de Pantalla debe estar fijado según (Proceso Gestión TICs.)

Cuando el funcionario se ausente de su lugar de trabajo, el equipo debe bloquearse por medio del protector de pantalla y una contraseña, así mismo, cuando se finalice una sesión de trabajo, el equipo debe apagarse, y cuando se encienda este, se debe introducir la contraseña de inicio.

Se debe configurar el equipo para que después de cierto tiempo de inactividad, el equipo cierre las sesiones de aplicaciones y Windows, y por ende cerrar las conexiones de red.

El usuario no debe guardar archivos en el escritorio de Windows, ya que puede incurrir en accesos no autorizados por la facilidad de encontrarlos; además estos archivos no son recuperables cuando se hace un formateo del equipo, por este motivo debe guardarse la información en otra partición.

3- ESCRITORIO LIMPIO

Es la protección de los papeles o documentos y dispositivos removibles de almacenamiento de información, conservados y manipulados en estaciones de trabajo (escritorio, oficina, etc.) de accesos no autorizados, pérdida y/o daño de la información durante y fuera de las horas normales de trabajo. Es así que, al finalizar la jornada de trabajo, el funcionario debe guardar en un lugar seguro, los documentos y medios que contengan información sensible para la Gobernación de Nariño.

Cuando no se esté utilizando algún medio de almacenamiento electrónico o escrito, se recomienda guardarlos en un sitio seguro bajo llave, especialmente cuando la oficina está vacía.

Retirar inmediatamente los documentos de impresoras o fotocopiadoras; evitar usar estos equipos sin autorización.

4- RESPALDO DE INFORMACIÓN y/o COPIAS DE SEGURIDAD

(Proceso Gestión TICs.) es el responsable de realizar el procedimiento de Backup de las Bases de Datos de los servidores del data center, según está estipulado en el ** Documento de Gestión de Procesos de “Copias de Seguridad” **.

Cuando se necesite una copia de la Base de Datos, se debe contar con la respectiva autorización del Jefe Inmediato y la aprobación de (Proceso Gestión TICs.).

Cada funcionario, es el único responsable de hacer copias de respaldo de la información que maneja, esto debe hacerse con regularidad con el fin de proteger la información contra su pérdida o daño. Este respaldo lo puede hacer por diferentes medios de almacenamiento: CD-ROM, DVD, Discos Duros Externos, Memorias USB, Correo Electrónico (Correo Personal, no Institucional), alojamiento de archivos multiplataforma en la nube (Adrive, Dropbox, Google Drive, OneDrive, Mega, etc.)

Cada medio de almacenamiento físico (CD-ROM, DVD, Discos Duros Externos, Memorias USB) deben estar correctamente etiquetado, para evitar su divulgación accidental, modificación, remoción o destrucción no autorizada. Cuando un medio ya no es utilizado, este debe ser un medio irrecuperable (destrucción total). Para estas tareas debe existir un registro de control de actividades.

Cuando sea necesario hacer un formateo total del equipo, (Proceso Gestión TICs.) tiene la tarea de extraer la información de la partición distinta a (C:) del disco duro; para que posteriormente, se vuelva a copiar la información en el equipo recién formateado.

El usuario tiene el deber de guardar toda su información en la partición (D:) puesto que cuando se necesite hacer el formateo del disco duro se hace en la partición (C:) donde se encuentra alojado el sistema operativo, quedando a salvo la información contenida en la partición (D:). Cuando se hace un formateo de disco, quiere decir que se borra definitivamente toda la información que contenga la partición (C:)

donde se encuentra instalado el sistema operativo. Es por eso que se hace la aclaración de que se debe guardar la información en (D:).

Cuando ya se tengan las copias de respaldo, se debe hacer un cronograma para poner a prueba regularmente su funcionalidad.

5- USO DE SOFTWARE-PROGRAMAS-APLICATIVOS:

El Personal de (Proceso Gestión TICs.) está autorizado y capacitado para realizar cualquier configuración e instalación de software; por tanto:

5-1. Se prohíbe la instalación y utilización de software (programas), temporales ni permanentes, que no sean autorizados por (Proceso Gestión TICs.).

5-2. Se debe establecer criterios de aceptación para nuevos sistemas de información, nuevas actualizaciones y nuevas versiones.

5-3. Restringir y controlar estrictamente el uso de programas utilitarios (Unlocker, Norton Partition Magic, Easy Recovery, Spyware Terminator, Hiren Boot CD, CCleaner, Tune up, etc.) que pueden anular los controles del sistema y de la aplicaciones.

5-4. Controlar el uso de código móvil con previa autorización; código móvil hace referencia a: comandos JavaScript, VBScript, Applets Java, controles Activex, animaciones Flash, películas Shockwave, macros en documentos office.

5-5. Se prohíbe la instalación de aplicativos propios de la Gobernación de Nariño en equipos externos a la entidad.

5-6. Se prohíbe copiar archivos, programas, modificación de aplicativos, utilización personal o de terceros de estos; que sean propiedad de la Gobernación de Nariño.

5-7. Se aconseja verificar la validaciones en las aplicaciones para detectar cualquier tergiversación de la información por errores de procesamiento o de actos intencionales.

5-8. Cuando haya desarrollo de software, se debe establecer y aplicar las reglas correspondientes para este (ejecución en diferentes sistemas, conexión por diferentes dominios, perfiles de usuario diferentes en S.O., compiladores y/o editores, entrada de al código fuente de código malicioso); además, durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de seguridad.

5-9. Para las pruebas, se deben seleccionar, proteger y controlar los datos de prueba.

5-10. Cuando se contrate un desarrollo externo, este debe estar supervisado y tener un seguimiento de la actividad de desarrollo.

5-11. Cuando se desarrolle un programa o aplicativo, ya sea por encargo o autorización, la propiedad intelectual pertenece a la Gobernación de Nariño.

5-12. Se debe restringir el acceso a códigos fuentes de aplicaciones o software dedicado.

5-13. Cuando un aplicativo se encuentre en fase de prueba, (Proceso Gestión TICs.), es el único encargado de realizar estas pruebas, y de lanzar la aplicación para su servicio en la Gobernación de Nariño.

5-14. Se prohíbe copiar, duplicar, vender cualquier aplicativo o programa que posee licencia de propiedad de la Gobernación de Nariño; esto se convierte en piratería y se extiende al hurto, lo cual tiene efectos penales.

5-15. Cuando se utilice software libre se debe tener soporte del sitio WEB en donde se especifique el tipo de licencia que posee.

5-16. Las claves de acceso a los aplicativos los da (Proceso Gestión TICs.). Es responsabilidad de cada funcionario la confidencialidad de la clave y la información contenida y procesada por el aplicativo.

5-17. Tener especial cuidado con el manejo de certificados y firmas digitales; el uso inadecuado de estos elementos conducirá al levantamiento de cargos legales.

5-18. El cancelar una cuenta de acceso o suspensión de permisos, se aplica cuando ésta no se esta utilizando, o si se utiliza con fines distintos al institucional, o existe sospecha de fraude.

5-19. La información consignada en el aplicativo debe ser corroborada en su totalidad (actualizada y exacta).

5-20. Se prohíbe el acceso de terceras personas a los aplicativos, si se da el caso, este acceso debe ser autorizado e identificado por (Proceso Gestión TICs.).

5-21. En un equipo de cómputo no debe existir más de una sesión de trabajo configurado en Windows.

5-22. Cuando se trate de mantenimiento, el ingreso remoto a los equipos debe hacerse única y exclusivamente desde (Proceso Gestión TICs.).

5-23. La reinstalación del Sistema Operativo (S.O.) se hace cuando exista un requisito o exigencia para hacerlo, por ejemplo: requisitos exigentes por parte de aplicaciones.

5-24. El usuario del sistema debe registrar las fallas por medio de las asistencias técnicas para que (Proceso Gestión TICs.) tome las medidas necesarias para su arreglo.

5-25. (Proceso Gestión TICs.) es el único encargado de instalar y actualizar software de detección de códigos maliciosos (antivirus), y además, es el delegado de manejar las políticas de Firewall del sistema.

5-26. Es conveniente que siempre se haga una verificación de la presencia de códigos malicioso antes de abrir los archivos que se encuentran en medios de almacenamiento (CD-ROM, USB,), en carpeta de DESCARGA, archivos compartidos por red, archivos adjuntos del correo electrónico.

6- USO DE HARDWARE (EQUIPOS DE ESCRITORIO Y PORTÁTILES)

Cada funcionario es responsable por los equipos a cargo (responsabilidad de manejo, control, protección, administración y uso), sean personales o equipos a cargo, registrados y asignados por parte de la Gobernación de Nariño.

A continuación se presentan directrices para la conservación de dichos dispositivos:

6-1. Conservar el orden y la limpieza en el escritorio.

6-2. Tratar en lo posible de no ingerir alimentos sólidos, ni bebidas cerca o sobre los equipos, ya que son causales de daño y deterioro de los equipos.

6-3. Los periféricos (teclado y mouse) deben ser tratados de la mejor manera posible.

6-4. Cuando se esté trabajando en un archivo de Excel, Word, PowerPoint, Pdf, etc., tratar en lo posible de guardar continuamente para evitar inconvenientes de pérdida de información.

6-5. Efectuar el proceso correcto de apagado de los equipos (no dejar sesiones abiertas, ni reinicio del equipo)

6-6. Los equipos están destinados principalmente para realizar trabajos propios de la entidad y no para hacer trabajos de tipo personal (universidad, especializaciones, etc.); además, no pueden ser usados para hacer pruebas de configuración o manipulación de archivos, los únicos calificados para esto son (Proceso Gestión TICs.).

6-7. Está prohibido el desconectar o conectar hardware, intercambiar elementos entre equipos; igualmente, no se puede alterar las conexiones de red; con el fin de no entorpecer el desempeño de la red.

6-8. Cuando un equipo es dado de baja, de debe verificar todos los elementos del equipo (medios de almacenamiento) para asegurar que se haya eliminado cualquier software licenciado y datos sensibles.

6-9. Se debe proteger el cableado estructural contra interceptaciones, interferencia o daño, igualmente el cableado eléctrico.

6-10. Identificar los tomas con corriente regulada, conectar sólo los equipos de cómputo a estos puntos; queda prohibido conectar equipos diferentes en estos puntos; así mismo, hacer buen uso de las fuentes UPS, mantenerlas con carga activa y enchufar los elementos necesarios (Monitor, CPU, periféricos).

6-11. El servicio de Impresión y Fotocopia es exclusivo de la entidad, se prohíbe su uso para fines personales o negocio.

6-12. Las comunicaciones telefónicas deben ser breves, para evitar la congestión de las líneas y facilitar la comunicación; queda prohibido las llamadas personales que tengan que ver con negocios particulares, instalar o conectar cualquier tipo de teléfono sin previa autorización de (Proceso Gestión TICs.).

6-13. El (Proceso Gestión TICs.) es el único encargado de instalar y configurar equipos para videoconferencia, presentaciones con videobeam. Este servicio debe ser solicitado con al menos tres días de anticipación.

6-14. El uso del circuito de cámaras está autorizado únicamente por la “Secretaria General”; por tanto, cualquier verificación de video o consulta, debe ser solicitada a esta dependencia. El incumplimiento de esta política traerá sanciones de carácter disciplinario.

6-15. Aplicar las medidas preventivas de seguridad a los activos que se encuentran fuera de las instalaciones de la Gobernación de Nariño.

6-16. El usuario del hardware debe registrar las fallas por medio de las asistencias técnicas para que (Proceso Gestión TICs.) tome las medidas necesarias para su arreglo y así reportar al usuario las fallas y posibles causas.

7- USO DE INTERNET:

El servicio de Internet en la Gobernación de Nariño, se presta para la investigación y búsqueda de nuevos conocimientos que tengan relación con las labores que cada funcionario desempeña, lo que contribuye al mejoramiento personal y/o profesional; por tanto:

7-1. El uso inadecuado de este servicio (actividades ilegales) que interfiera o que atente contra la ética y la buena imagen de la Gobernación de Nariño, se considera una falta, y está sujeto a las sanciones correspondientes.

7-2. (Proceso Gestión TICs.), posee el derecho de filtrar el contenido de la red, con el fin de que este servicio no interfiera con el buen desempeño de los trabajadores. En el caso en que un funcionario tenga la necesidad de consultar algún contenido que se encuentre restringido, se debe diligenciar la solicitud correspondiente, dirigida a (Proceso Gestión TICs.)

7-3. Está prohibido la descarga de Software (programas) desde internet por motivos de seguridad (virus, spyware, malware, etc.). Dado el caso en que el funcionario necesite hacer la descarga, se debe contar con la autorización de (Proceso Gestión TICs.) Así mismo, se debe tener en cuenta los derechos de propiedad intelectual, derechos de autor, marcas registradas, etc., de cualquier información que se apropie de internet, atendiendo a las disposiciones legales que esto amerita, tanto a nivel nacional como internacional, sin que se tenga que comprometer el nombre de la Gobernación de Nariño.

7-4. Está totalmente prohibido la descarga de contenido de tipo sexual, nudismo, violencia, pedofilia, pornografía infantil, o cualquier tipo de actividad pornográfica, que vaya en contra de los principios y valores de la Gobernación de Nariño; el no cumplimiento de esta política, será causa justificada para efectuar una Sanción Disciplinaria.

7-5. Está prohibido la utilización de aplicaciones de mensajería instantánea externa (Chat Outlook, Yahoo Messenger, Chat de Facebook, Skype, WhatsApp Web, Line Web); además, el funcionario no puede acceder a servicios web para mirar videos vía Streaming u Online (Youtube, Vimeo, Dailymotion), emisoras de radio virtuales (Real audio, MusicMatch, Oozic Player).

7-6. Toda información que involucre algún tipo de comercio o información de este tipo, y que se transmita por redes públicas debe estar protegida contra actividades fraudulentas, dispuestas por contratos y divulgación o modificación no autorizada.

7-7. La información involucrada en las transacciones en línea debe estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración, divulgación, duplicación o repetición no autorizada del mensaje.

7-8. La información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no autorizada.

8- USO DE LA INTRANET:

Las normas de conducta del uso de INTERNET, se aplican al uso de la INTRANET, además de estas normas, se deben tener en cuenta las siguientes políticas:

8-1. Quienes hacen uso de la Intranet, deben ser funcionarios (registrados) de la Gobernación de Nariño. El registro debe hacerse previa solicitud a (Proceso Gestión TICs.)

8-2. Las cuentas de acceso son personales e intransferibles.

8-3. Las Publicaciones no pueden ser de fuentes externas a la Gobernación de Nariño, o que sean obtenidas sin autorización de (Proceso Gestión TICs.), quien verifica la licencia de copia.

8-4. La información que se pone a disposición de los funcionarios debe estar protegida para evitar la modificación no autorizada y divulgación a fuentes externas.

9- MENSAJERÍA O CORREO ELECTRÓNICO:

El uso del correo institucional es esencial para el desarrollo laboral de cada cargo, facilitando la comunicación y conectividad, con el beneficio de la rapidez y efectividad en las comunicaciones que este medio brinda, aplicado a la Gobernación de Nariño. Por tanto:

9-1. Todo funcionario tiene el deber de leer y responder oportunamente los correos y requerimientos que se envían por este medio. Es obligación del funcionario revisar su correo por lo menos una vez al día, ya que, el fin de este medio de comunicación implementado por la Gobernación de Nariño es tener una comunicación y conectividad constante con sus empleados, por medio de informaciones y directrices administrativas.

El correo institucional lleva consigo el nombre de la Entidad (narino.gov), por tanto, se prohíbe su uso para fines distintos de la Gobernación de Nariño. A continuación se enumeran algunas actividades que van en contra del fin principal del Correo Institucional:

a) Difundir al interior o exterior de la Gobernación de Nariño material fotográfico que contengan escenas de sexo explícito o implícito, nudismo, violencia, pornografía de cualquier tipo, o cualquier otra situación que atente contra la buena moral de la sociedad.

b) Enviar información que no haya sido requerida por los destinatarios, o archivos de dudosa procedencia.

c) Enviar información que maltrate o desconozca los derechos de cualquier persona, incluyendo su derecho a la intimidad, origen étnico, orientación sexual, calumnias, falsos testimonios, etc.

d) Queda totalmente prohibido el correo SPAM o cadenas de correo tanto al interior o exterior de la Gobernación de Nariño que no tengan que ver con alguna función de la Gobernación de Nariño; ya que esto afecta el

rendimiento de la red; además, es foco de inseguridad informática (virus, spyware, malware, etc.) para los usuarios; esta prohibición se extiende para quien utilice el correo para hacer promociones o propagandas comerciales, información política, promoción de actividades no lícitas; y por último, usar el correo institucional para envío de tarjetas de felicitaciones o algún motivo especial de carácter personal.

e) Restringir el envío automático de correos a direcciones externas.

9-2. La utilización del servicio de Correo Electrónico, permite disminuir costos; por lo cual, se hace necesario aclarar que no todo lo recibido por este medio debe imprimirse, puesto que esto genera un costo adicional para la Gobernación de Nariño, y se atenta contra la política de reciclaje.

9-3. Prestar atención cuando se envían archivos adjuntos innecesarios o archivos adjuntos que tengan un peso considerable; esto hace que se afecte el desempeño de la red. Igualmente se recomienda borrar archivos con más de 30 días de antigüedad que no sean utilizados, esto se recomienda para que el usuario optimice el uso del espacio del servidor de correo y posteriores grabaciones de copias de seguridad, conservando el número mínimo de mensajes almacenados.

9-4. Tener precaución cuando se envía un correo, puede caer en equivocación y enviar por error un mensaje a un destinatario diferente.

9-5. El cancelar una cuenta de correo se aplica: cuando la cuenta no se esta utilizando, o se utiliza con fines distintos al institucional.

10- POLÍTICA DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN:

Se debe realizar una evaluación de las personas que estarán autorizadas para entregar o recibir la información, según sea el caso, y para esto se debe presentan los siguientes lineamientos:

10-1. La información escrita o verbal debe estar controlado por los superiores dueños de esta.

10-2. La persona quien recibe la información no obtendrá derecho alguno, de ningún tipo, sobre la información, ni tampoco, ningún derecho de utilizarla, excepto para el objeto del acuerdo firmado.

10-3. El trabajador debe mantener la información confidencial en estricta reserva y no revelar ningún dato a otra parte externa que no sea la Gobernación de Nariño, sin el consentimiento previo de la fuente.

10-4. Se debe dar un trato especial a la información confidencial que es recibida directa o indirectamente, no debe utilizarse sin previo estudio y autorización.

10-5. No manipular, usar, explotar, o divulgar la información confidencial a personas o entidades que no estén implicadas en su proceso, esto debe hacerse con autorización escrita.

10-6. La divulgación o mal uso de la información se convierte en infracción y es causal de sanciones.

11- GESTIÓN DE CONTRASEÑAS

El uso de contraseñas en equipos de cómputo (Inicio de Sesión en Windows) es de carácter obligatorio, y es el usuario quien define que clase de contraseña se va a registrar en el S.O.; si el usuario cree pertinente pedir indicaciones para esta tarea, puede pedir asesoría en (Proceso Gestión TICs.)

La Oficina de Gestión TICs, entrega un usuario y contraseña para la administración del correo personal institucional; así mismo, se entrega usuario y contraseña para acceder a software y plataformas web. Esta entrega se hace previa solicitud a (Proceso Gestión TICs.) y verificación de la identidad.

Cada funcionario es responsable de manejar la confidencialidad de la identificación, por esto se recomienda que las cuentas de usuario y contraseñas no sean entregadas a nadie diferente al usuario. Las contraseñas no deben contener datos personales, deben contener letras mayúsculas, minúsculas, números, y algún símbolo especial.

Ningún usuario debe utilizar el nombre de usuario y contraseña de otro funcionario para acceder a los servicios personales (Correo electrónico, equipos de cómputo, y servicios en general).

Cuando al funcionario se le cancela o termina el contrato, o es reasignado de lugar de trabajo, es obligación de (Proceso Gestión TICs.) anular la contraseña, usuarios de correo electrónico y aplicaciones web.

Se debe hacer un seguimiento del ciclo de vida del acceso del usuario (desde el registro hasta cuando se cancele la cuenta).

Los usuarios deben firmar una declaración escrita donde esté contenido los derechos de acceso y de uso, y confidencialidad de las contraseñas personales; en (Proceso Gestión TICs.) no debe existir registros escritos, archivos, software o dispositivos donde estén registradas las contraseñas.

Implementar controles de autenticación para las conexiones externas basadas en la red privada virtual VPN.

12- USO DE LA RED

13-1. Implementar políticas de seguridad para el uso de los servicios de la red de datos ya que los usuarios sólo deben tener acceso a los servicios para cuyo uso están específicamente autorizados.

13-2. Se debe considerar un mecanismo para la identificación automática de los equipos en lo que se refiere a la autenticación de conexiones de equipos y ubicaciones específicas.

13-3. Implementar un componente o módulo de red para realizar un diagnóstico remoto y protección de puertos de configuración.

13-4. La red debe estar separada o segmentada por medio de VLAN´s (Redes Virtuales Locales), debe existir diferentes grupos de servicios, información, usuarios y sistemas de información.

13-5. Debe existir un control de conexión para redes compartidas que sean externas (fuera de la sede central de la Gobernación de Nariño).

13-6. Identificar los eventos que pueden ocasionar interrupciones en los servicios y procesos de la entidad, junto con los riesgos identificados de dichas interrupciones, así como sus consecuencias para la seguridad de la información.

VII- ANEXOS

A- DELITOS INFORMÁTICOS

TIPOS DE DELITOS INFORMÁTICOS:

- Virus.
- Gusanos.
- Bomba lógica o cronológica.
- Sabotaje informático.
- Piratas informáticos o hackers.
- Acceso no autorizado a sistemas o servicios.
- Reproducción no autorizada de programas informáticos de protección legal.
- Manipulación de datos de entrada y/o salida.
- Manipulación de programas.
- Fraude efectuado por manipulación informática.

LEGISLACIÓN ACTUAL:

Ley 1273 de 2009 (enero 5) Diario Oficial No. 47.223 de 5 de enero de 2009 CONGRESO DE LA REPÚBLICA DE COLOMBIA.

POR MEDIO DE LA CUAL SE MODIFICA EL CÓDIGO PENAL, SE CREA UN NUEVO BIEN JURÍDICO TUTELADO – DENOMINADO "DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS" – Y SE PRESERVAN INTEGRALMENTE LOS SISTEMAS QUE UTILICEN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, ENTRE OTRAS DISPOSICIONES.

CAPITULO PRIMERO: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.

Artículo 269A: El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de presión de cuanta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.

Artículo 269B: El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

INTERCEPTACIÓN DE DATOS INFORMÁTICOS.

Artículo 269C: El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

DAÑO INFORMÁTICO.

Artículo 269D: El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

USO DE SOFTWARE MALICIOSO.

Artículo 269E: El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

VIOLACIÓN DE DATOS PERSONALES.

Artículo 269F: El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.

Artículo 269G:

- El que, con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) mese y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.
- En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.
- La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA

Artículo 269H: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1- Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2- Por servidor público en ejercicio de sus funciones.

3- Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vinculo contractual con este.

4- Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5- Obteniendo provecho para sí o para un tercero.

6- Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7- Utilizando como instrumento a un tercero de buena fe.

8- Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO SEGUNDO: De los atentados informáticos y otras infracciones

HURTO POR MEDIOS INFORMATICOS
Artículo269I:

- El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una res de

sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

- Artículo 239. Hurto. El que se apodere de una cosa mueble ajena, con el propósito de obtener provecho para sí o para otro, incurrirá en prisión de dos (2) a seis (6) años.

- Artículo 240. Hurto calificado. La pena será prisión de tres (3) a ocho (8) años.

TRANSFERENCIA NO CONSENTIDA DE ACTIVOS

Artículo 269J:

- El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

- Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

CIRCUNSTANCIAS DE MAYOR PUNIBILIDAD

- Artículo 2º. Adiciónese al artículo 58 del Código Penal con un numeral 17, así:

  Articulo 58. Circunstancias de mayor punibilidad. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera:

  17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos

B- MEDIOS MÓVILES

- Cuando se hace uso de dispositivos móviles (notebooks, tablets, phablets, Smartphones, ebook) se debe garantizar la seguridad de la información contenida en estos.

- Tener precaución cuando se trabaje en espacios libres, donde se vea implicado en hurto, sustracción, el medio ambiente, entorno meteorológico, instalaciones eléctricas, etc.

- Tener políticas SGSI aplicadas a la utilización de equipos móviles

- Tener cuidado cuando se utilicen dispositivos móviles en lugares públicos, salas de reuniones y otras áreas sin protección fuera de las instalaciones de la Gobernación de Nariño.

- Es conveniente realizar copias de respaldo de la información continuamente, contenida en estos dispositivos, para evitar pérdida de información por alguna eventualidad.

- Tener cuidado con estos dispositivos por robo, uso en transporte, olvido en habitaciones de hoteles, centros de conferencias y sitios de reuniones.

C- TRABAJO REMOTO

Se autoriza esta actividad si las disposiciones de seguridad son adecuadas, poseen los controles y políticas de seguridad de la organización:

- Seguridad física en cuanto a la edificación y entorno local propuesto para el trabajo remoto.

- Requisitos de seguridad de comunicación, acceso remoto a los sistemas internos de la Gobernación de Nariño, tipo de información a tratar.

- Acceso no autorizado a la información o recursos por parte de otras personas que usan o comparten el mismo espacio (familiares y/o amigos).

- Restricciones en la configuración de la red física o inalámbrica del lugar de trabajo.

- Licenciamiento de software desde la organización de la Gobernación de Nariño para las estaciones de trabajo de propiedad privada de los empleados, contratistas o usuarios de terceras partes.

- Poseer protección antivirus y requisitos de firewall.

- Por parte del trabajador, debe existir disposición de equipo adecuado y medios de almacenamiento para las actividades de trabajo remoto.

- Definición del trabajo a realizar, horas laborales, confidencialidad de la información.

- Disposición de equipo de comunicación red.

- Precaución de acceso de familiares y visitantes a la estación de trabajo (equipo de cómputo)

- Soporte en software y hardware de la estación de trabajo

- Disposición de pólizas de seguro.

- Revocación de autoridad y derechos de acceso, si es el caso devolución del equipo al final de las actividades de trabajo remoto.

D- ADMINISTRACIÓN PARTICIONES DE DISCO DURO

Es conveniente crear particiones por razones de seguridad, ya que se crean unidades independientes, de forma que si tenemos que formatear una de ellas por algún motivo tendremos nuestros datos a salvo en la otra unidad. Por lo general en un disco duro existe dos particiones C: y D:

En la partición C: se encuentra ubicado todo el sistema operativo Windows, en esta partición se encuentra ubicado la carpeta de “mis documentos” y escritorio; cuando sea necesario formatear esta unidad dado el caso por infección de virus, desconfiguración de sistema, daño en el registro, se procede a borrar todos los datos existentes en esta unidad, con el fin de instalar nuevamente el S.O. sin fallo alguno. Por esta razón es conveniente guardar toda la información en la partición D: ya que esta no se ve afectada cuando se tenga que hacer un formateo del disco C:

Firma en Original

Ing. Brenda E. Rivas M.
Prof. Universitario
Proceso Gestión TIC´S

Proyectó:
Ing. JAVIER GIOVANNI JOJOA ORBES
Proceso Gestión TIC´S