MINISTERIO DE EDUCACIÓN NACIONAL
Oficina de Tecnología y Sistemas de Información

POLÍTICAS Y PROCEDIMIENTOS PARA LA GESTIÓN DE LA SEGURIDAD Y LA CONSERVACIÓN DE LA INFORMACIÓN EN EL MINISTERIO DE EDUCACIÓN

Documento de Políticas de Seguridad Informática - Versión Vigencia 2009

Versión 1 - Diciembre de 2008
Versión 2 – Marzo de 2009

1 INTRODUCCIÓN

El proceso de gestión de la seguridad de tecnología de información y comunicaciones, tiene como objetivo garantizar la protección de activos ante daños, destrucción, uso no autorizado, robos; mantener la integridad de los datos de manera oportuna, precisa confiable y completa; apoyar el logro de las metas organizacionales, mediante la contribución de la tecnología y que se realice un uso eficiente de los recursos disponibles en el procesamiento de la información.

La gestión de la seguridad de la información es fundamental debido a que la información se ha convertido en un importante activo en la operación del Ministerio de Educación Nacional y del sector educativo en general, Las organizaciones del sector requieren para su operación normal contar con los recursos de cómputo y el acceso a la información de manera permanente e inmediata, la ausencia de esta capacidad por motivos de riesgos no controlados o contingencias de fuerza mayor pondrán el peligro el desempeño del Ministerio de Educación Nacional y de otras entidades del sector y del Gobierno Nacional, así como la posible generación de traumatismos en las actividades diarias del personal del sector y de los ciudadanos que hacen uso de los diferentes servicios con los que ya cuentan o bien en medio digital o bien presencial, pero facilitado intensamente por las Tecnologías de Información y Comunicaciones (TIC), en los diferentes procesos que apoyan los servicios que actualmente brinda el sector educativo a la ciudadanía.

Las políticas de seguridad de tecnología de información son agentes fundamentales para la concientización de los funcionarios, para la prestación adecuada de servicios y para la administración de los activos informáticos en un entorno moderno en el cual se utilizan tecnologías modernas, en un ambiente dinámico en el que la seguridad es fundamental para la protección ante amenazas de diferente tipo.

La política de seguridad informática determina la manera como debe actuar un servidor público en el Ministerio de Educación Nacional, para gestionar la información y los recursos tecnológicos y busca generar compromiso y autocontrol en las personas que laboran en el Ministerio de Educación, para reconocer y administrar este importante activo de que disponen: la información.

La política de seguridad informática incluye componentes de gestión de activos, gestión de usuarios, gestión de la infraestructura computacional, disposición adecuada de servicios de información entre otros.

Las políticas registradas en este documento son de carácter obligatorio para todos los servidores públicos, funcionarios del Ministerio de Educación Nacional, contratistas, terceros participantes de convenios que el Ministerio ha celebrado con personas jurídicas, usuarios y visitantes que hacen uso de medios tecnológicos dispuestos por la entidad para el desarrollo de los procesos, servicios y proyectos consignados en el Sistema Integrado de Gestión y en especial en el macroproceso de Gestión de Tecnología.

2 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Políticas sobre el acceso:

2.1 Política 1. Seguridad para los servicios informáticos

i.) Alcance

Servidores públicos (funcionarios y contratistas) que tienen acceso a la red y a los servicios informáticos disponibles

ii.) Objetivo

Proteger a la entidad del uso inadecuado de los medios electrónicos por parte de los servidores públicos (funcionarios y contratistas) así como protegerse de las amenazas propias de internet y que están al alcance de los usuarios.

iii.) Descripción

El correo electrónico institucional y los sistemas de mensajería instantánea que la entidad disponga a los servidores públicos y contratistas, deberán ser usados únicamente para las funciones asignadas a cada funcionario y para las actividades contratadas en caso de los contratistas. Los funcionarios deben abstenerse de utilizar este medio para actividades de índole personal y para la participación en foros y comunidades en las que actúen a título personal y no como servidores públicos. En caso de que se requiera la participación en nombre de la entidad, sólo se podrá usar el coreo institucional siempre y cuando exista una autorización del jefe inmediato. La entidad se reserva el derecho de acceder y develar todos los mensajes enviados por este medio, para cualquier propósito. Para este efecto, el servidor aceptará estas condiciones de uso de los servicios disponibles. Las cuentas de correo electrónico se asignarán de manera individual a cada servidor y se identificará plenamente con el nombre y apellido del servidor público. No se crearán cuentas con nombres genéricos, se exceptúan los buzones institucionales, los cuales serán administrados por los funcionarios responsables de los proyectos. La entidad se reserva el derecho de asignar los nombres de las cuentas de usuario y la descripción, de acuerdo a las políticas de administración de correo electrónico. Para las personas naturales vinculadas mediante convenio con un tercero, tendrán en la descripción el nombre de la entidad contratista, para diferenciarlas de los funcionarios y contratistas de prestación de servicios del Ministerio. Los servidores públicos deben abstenerse de utilizar versiones escaneadas de firmas hechas a mano, para enviar correos o cualquier otro tipo de comunicación electrónica, en su nombre o de otra persona.

El uso de Internet y de las facilidades disponibles a los servidores públicos se llevará a cabo en el marco de las políticas de uso de Internet, definidas por la entidad. La navegación en sitios no seguros de Internet, tales como sitios de

descarga de música, videos, sitios para adultos, archivos ejecutables, entre otros y que atenten contra la seguridad de la red está prohibida.

La entidad dispondrá de un sistema de antivirus que garantiza la defensa ante amenazas de código malicioso que afecte el desempeño de los recursos informáticos con que cuenta la entidad. Es responsabilidad de los usuarios informar oportunamente acerca de una sospecha de infección por un virus, recepción de SPAM o comportamiento anómalo por causas desconocidas, a la mesa de ayuda de la Oficina de Tecnología; ante estas situaciones de riesgo, deberá abstenerse de usar su computador y desconectarlo físicamente de la red.

iv.) Responsables

Funcionarios públicos y contratistas

v.) Sanciones

El incumplimiento de esta política conllevará a la suspensión de la cuenta de acceso a la red, y de la notificación al superior inmediato, con copia a la Subdirección de Talento Humano.

2.2 Política 2. Seguridad para usuarios terceros

i.) Alcance

Personas naturales y jurídicas que usen recursos propios o dispongan recursos para el desarrollo de actividades en el Ministerio de Educación Nacional y que tengan acceso a la red y a los recursos o servicios informáticos disponibles

ii.) Objetivo

Garantizar que los recursos informáticos habilitados por terceros en el desarrollo de actividades requeridas, cumplan con los requerimientos de seguridad de la información de manera que no se incurra en riesgos por el uso de estos recursos en la entidad.

iii.) Descripción

Cuando se requiera utilizar recursos informáticos u otros elementos de propiedad del Ministerio de Educación Nacional para el funcionamiento de recursos que no sean propios de la entidad y que deban ubicarse en sus instalaciones, los recursos serán administrados por la Oficina de Tecnología.

Los dueños de los recursos informáticos que no sean propiedad de la entidad y deban ser ubicados y administrados por ésta, deben garantizar la legalidad del recurso para su funcionamiento. Adicionalmente debe definir un documento de acuerdo oficial entre las partes.

Los usuarios terceros tendrán acceso a los recursos informáticos, que sean estrictamente necesarios para el cumplimiento de su función, servicios que deben ser aprobados por quien será el jefe inmediato o coordinador, que a su vez

será un funcionario de la planta de la entidad. En todo caso deberán firmar el acuerdo de buen uso de los recursos informáticos.

La conexión entre sistemas internos de la entidad y otros de terceros debe ser aprobada y certificada por la Oficina de Tecnología con el fin de no comprometer la seguridad de la información interna de la entidad.

Los equipos de usuarios terceros que deban estar conectados a la Red, deben cumplir con todas las normas de seguridad informática vigentes en la Entidad.

Como requisito para interconectar las redes de la entidad con las de terceros, los sistemas de comunicación de terceros deben cumplir con los requisitos establecidos por la entidad. La entidad se reserva el derecho de monitorear estos sistemas de terceros sin previo aviso para evaluar la seguridad de los mismos. La entidad se reserva el derecho de cancelar y terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos establecidos por la entidad.

iv.) Responsables

Funcionarios públicos y contratistas y sus jefes inmediatos y delegados de firmas o entidades externas y sus interventores

v.) Sanciones

El no cumplimiento de esta política conllevará la limitación en el uso de la red y la notificación oficial al interventor y a su jefe inmediato

2.3 Política 3. Seguridad física y del entorno

i.) Alcance

Servidores públicos (funcionarios y contratistas) que tienen acceso a la red y a los servicios informáticos disponibles y Personas naturales y jurídicas que usen recursos propios o dispongan recursos para el desarrollo de actividades en el Ministerio de Educación Nacional y que tengan acceso a la red y a los recursos o servicios informáticos disponibles

ii.) Objetivo

Garantizar que el acceso físico a las instalaciones de operación de equipos de cómputo y de telecomunicaciones se realiza bajo medidas de seguridad que permitan que únicamente el personal autorizado pueda manipular o tener contacto con los equipos activos y sensibles para la operación.

iii.) Descripción

La Entidad deberá contar con los mecanismos de control de acceso tales como puertas de seguridad, sistemas de control con tarjetas inteligentes, sistema de alarmas y circuitos cerrados de televisión en las dependencias que la entidad considere críticas.

Los visitantes de las oficinas de la entidad deben ser escoltados durante todo el tiempo por un empleado autorizado, asesor o contratista. Esto significa que se requiere de un escolta tan pronto como un visitante entra a un área controlada y hasta que este mismo visitante sale del área controlada. Todos los visitantes requieren una escolta incluyendo clientes, antiguos empleados y miembros de la familia del trabajador.

Siempre que un trabajador se de cuenta que un visitante no escoltado se encuentra dentro de áreas restringidas de la entidad, el visitante debe ser inmediatamente cuestionado acerca de su propósito de encontrarse en área restringida e informar a las responsables de la seguridad del edificio.

Los centros de cómputo o áreas que la entidad considere criticas, las cintotecas deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada permanentemente por el personal que labora cotidianamente en estos lugares.

Toda persona que se encuentre dentro de la entidad deberá portar su identificación en lugar visible.

En los centros de cómputo o áreas que la entidad considere criticas deberán existir elementos de control de incendio, inundación y alarmas.

Los centros de computo o áreas que la entidad considere criticas deberán estar demarcados con zonas de circulación y zonas restringidas.

Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.

Todos los computadores portátiles y equipos de comunicación deben registrar su ingreso y salida y no deben abandonar la entidad a menos que esté acompañado por la autorización respectiva y la validación de supervisión de la Oficina de Tecnología.

Todos los visitantes deben mostrar identificación con fotografía y firmar antes de obtener el acceso a las áreas restringidas controladas por la entidad.

Los equipos de microcomputadores (PCs, servidores, equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa de la Oficina de Tecnología

Los funcionarios públicos se comprometen a NO utilizar la red regulada de energía para conectar equipos eléctricos diferentes a su equipo de cómputo, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras y en general cualquier equipo que generen caídas de la energía.

Los particulares en general, entre ellos, los familiares de los servidores públicos, no están autorizados para utilizar los recursos informáticos de la entidad

iv.) Responsables

Funcionarios de la Oficina de Tecnología, funcionarios públicos y contratistas y sus jefes inmediatos y delegados de firmas o entidades externas y sus interventores

v.) Sanciones

El incumplimiento de esta política conllevará a notificación al superior inmediato, con copia a la Subdirección de Talento Humano, en el caso de terceros, esto conllevará una nota solicitando explicación al representante legal de la firma a la que pertenece el contratista y en caso de manipulación indebida puede tener efectos penales, de igual manera se notificará a los interventores.

2.4 Política 4. Escritorio limpio

i.) Alcance

Servidores públicos (funcionarios y contratistas) que tienen acceso a la red y a los servicios informáticos disponibles y personas naturales y jurídicas que usen recursos propios o dispongan recursos para el desarrollo de actividades en el Ministerio de Educación Nacional y que tengan acceso a la red y a los recursos o servicios informáticos disponibles

ii.) Objetivo

Garantizar que los medios magnéticos y físicos que contienen información propia de la entidad, se encuentran resguardados en los escritorios de los miembros de la comunidad que labora en la entidad.

iii.) Descripción

Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD, Memorias USB y otros dispositivos de almacenamiento, con fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información durante el horario normal de trabajo y fuera del mismo. Los dispositivos de almacenamiento deben ser guardados bajo llave, especialmente aquellos en los que se hayan realizado copias de respaldo de archivos magnéticos.

iv.) Responsables

Todos los funcionarios públicos y contratistas y sus jefes inmediatos y delegados de firmas o entidades externas y sus interventores

v.) Sanciones

El incumplimiento de esta política conllevará a notificación al superior inmediato, con copia a la Subdirección de Talento Humano, en el caso de terceros, esto conllevará una nota solicitando explicación al representante legal de la firma a la que pertenece el contratista y en caso de manipulación indebida puede tener efectos penales, de igual manera se notificará a los interventores.

2.5 Política 5. Acceso a la información

i.) Alcance

Servidores públicos (funcionarios y contratistas) que tienen acceso a la red y a los servicios informáticos disponibles y personas naturales y jurídicas que usen recursos propios o dispongan recursos para el desarrollo de actividades en el Ministerio de Educación Nacional y que tengan acceso a la red y a los recursos o servicios informáticos disponibles

ii.) Objetivo

Garantizar que la información, como bien público, sea dispuesta a los funcionarios, usuarios y ciudadanos, según las necesidades del Sistema Integrado de Gestión de la Entidad, de manera que se pueda utilizar efectivamente, de manera segura y sin afectación a la calidad y confiabilidad de la misma.

iii.) **Descripción**

Todos los funcionarios públicos, contratistas, funcionarios de las secretarías de educación, funcionarios de las instituciones de educación superior, deberán tener acceso sólo a la información necesaria para el desarrollo de sus actividades, según los procesos definidos en el Sistema Integrado de Gestión SIG. En el caso de terceros externos al Ministerio de Educación Nacional, deberán contar con una solicitud de autorización diligenciada por el responsable de la dependencia que lidera los procesos, mediante solicitud a la Oficina de Tecnología y haciendo uso de los mecanismos que para ello ésta defina.

El otorgamiento de acceso a la información está regulado mediante las normas y procedimientos definidos para tal fin.

Todas las prerrogativas para el uso de los sistemas de información que el Ministerio de Educación Nacional pone al servicio de sus servidores públicos, deberán terminar inmediatamente después de que el trabajador cesa de prestar sus servicios.

Los contratistas, proveedores o terceras personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones convenidas y aprobadas.

Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la Entidad, la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal de la Entidad.

Mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica se efectuará un seguimiento a los accesos realizados por los usuarios a la información de la Entidad, con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución.

iv.) Responsables

Todos los funcionarios públicos y contratistas y sus jefes inmediatos y delegados de firmas o entidades externas y sus interventores

v.) Sanciones

El incumplimiento de esta política conllevará a notificación al superior inmediato, con copia a la Subdirección de Talento Humano, en el caso de terceros, esto conllevará una nota solicitando explicación al representante legal de la firma a la que pertenece el contratista y en caso de manipulación indebida puede tener efectos penales, de igual manera se notificará a los interventores.

Políticas sobre los recursos:

2.6 Política 6. Seguridad de la información

i.) Alcance

Servidores públicos (funcionarios y contratistas) que tienen acceso a la red y a los servicios informáticos disponibles y personas naturales y jurídicas que usen recursos propios o dispongan recursos para el desarrollo de actividades en el Ministerio de Educación Nacional y que tengan acceso a la red y a los recursos o servicios informáticos disponibles

ii.) Objetivo

Garantizar los servidores públicos realicen una gestión segura y confiable de la información de que disponen.

iii.) Descripción

Los servidores públicos del Ministerio de Educación Nacional son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Entidad y por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

Los servidores públicos no deben suministrar cualquier información de la entidad a ningún ente externo sin las autorizaciones respectivas.

Todo servidor público que utilice los recursos informáticos, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

Los servidores públicos del Ministerio de Educación Nacional deben firmar y renovar cada año, un acuerdo de cumplimiento de la seguridad de la información, la confidencialidad, el buen manejo de la información. Después de que el trabajador deja de prestar sus servicios a la Entidad, se compromete a

entregar toda la información respectiva de su trabajo realizado. Una vez retirado el funcionario o contratista, debe comprometerse a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la entidad, directamente o través de terceros. Así mismo, los funcionarios públicos que detecten el mal uso de la información están en la obligación de reportar el hecho al grupo de control interno disciplinario.

Como regla general, la información de políticas, normas y procedimientos de seguridad se deben revelar únicamente a funcionarios y entes externos que lo requieran, de acuerdo con su competencia y actividades a desarrollar según el caso respectivamente.

iv.) Responsables

Todos los funcionarios públicos y contratistas y sus jefes inmediatos y delegados de firmas o entidades externas y sus interventores

v.) Sanciones

El incumplimiento de esta política conllevará a notificación al superior inmediato, con copia a la Subdirección de Talento Humano, en el caso de terceros, esto conllevará una nota solicitando explicación al representante legal de la firma a la que pertenece el contratista y en caso de manipulación indebida puede tener efectos penales, de igual manera se notificará a los interventores.

2.7 Política 7. Seguridad en recursos informáticos

i.) Alcance

Servidores públicos (funcionarios y contratistas) que tienen acceso a la red y a los servicios informáticos disponibles y personas naturales y jurídicas que usen recursos propios o dispongan recursos para el desarrollo de actividades en el Ministerio de Educación Nacional y que tengan acceso a la red y a los recursos o servicios informáticos disponibles

ii.) Objetivo

Garantizar que cada uno de los recursos informáticos es suscetible de ser administrado y de establecer las condiciones de seguridad con las que debe operar para que sea elemento activo de un esquema integral de seguridad informática de la entidad.

iii.) Descripción

Todos los recursos informáticos deben cumplir como mínimo con lo siguiente:

Administración de usuarios: Establece cómo deben ser utilizadas las claves de ingreso a los recursos informáticos. Establece parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar

su contraseña y los períodos de vigencia de las mismas, entre otras.

Rol de Usuario: Los sistemas operacionales, bases de datos y aplicativos deberán contar con roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles. También deben permitir que un rol de usuario administre el Administración de usuarios.

Plan de auditoria: Hace referencia a las pistas o registros de los sucesos relativos a la operación.

Las puertas traseras: las puertas traseras son entradas no convencionales a los sistemas operacionales, bases de datos y aplicativos. Es de suma importancia aceptar la existencia de las mismas en la mayoría de los sistemas operacionales, bases de datos, aplicativos y efectuar las tareas necesarias para contrarrestar la vulnerabilidad que ellas generan.

El control de acceso a todos los sistemas de computación de la entidad debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicas para cada usuario.

Las palabras claves o contraseñas de acceso a los recursos informáticos, que designen los servidores públicos del Ministerio de Educación Nacional son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.

Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.

Se prohíbe tener identificaciones de usuario genéricos basados en sus funciones de trabajo. Las identificaciones de usuario deben únicamente identificar individuos específicos.

Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a el.

El nivel de superusuario de los sistemas críticos debe tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del sistema.

Toda la información del servidor de base de datos que sea sensible, crítica o valiosa debe tener controles de acceso y sometida a procesos de ciframiento para garantizar que no sea inapropiadamente descubierta, modificada, borrada o no recuperable.

Antes de que un nuevo sistema se desarrolle o se adquiera, los subdirectores, jefes de oficina, en conjunto con el asesor de seguridad informática, deberán definir las especificaciones y requerimientos de seguridad necesarios.

La seguridad debe ser implementada por diseñadores y desarrolladores del sistema desde el inicio del proceso de diseño de sistemas hasta la conversión a un sistema en producción.

Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad y en cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.

iv.) Responsables

Todos los funcionarios públicos y contratistas y sus jefes inmediatos y delegados de firmas o entidades externas y sus interventores. Los responsables por el esquema de seguridad de la entidad y de los equipos de desarrollo de los sistemas de información de la Oficina de Tecnología.

v.) Sanciones

El incumplimiento de esta política conllevará a notificación al superior inmediato, con copia a la Subdirección de Talento Humano, en el caso de terceros, esto conllevará una nota solicitando explicación al representante legal de la firma a la que pertenece el contratista.

2.8 Política 8. Seguridad en redes y comunicaciones

i.) Alcance

Funcionarios de la Oficina de Tecnología y sus terceros personas naturales y jurídicas contratistas e interventores.

ii.) Objetivo

Garantizar que la operación de las redes de telecomunicaciones de area local o de área amplia se realice en condiciones de seguridad para el intercambio de información y para las comunicaciones efectivas entre personas, entre entidades y entre sistemas de información y entre elementos activos de transmisión de datos.

iii.) **Descripción**

Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Entidad, deberán ser consideradas y tratadas como información confidencial.

La red de amplia cobertura geográfica a nivel nacional e internacional debe estar dividida en forma lógica por diferentes segmentos de red, cada uno separado con controles de seguridad perimetral y mecanismos de control de acceso.

Todas las conexiones a redes externas de tiempo real que accedan a la red interna de la entidad, debe pasar a través de los sistemas de defensa electrónica que incluyen servicios de cifrado y verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.

Todo intercambio electrónico de información o interacción entre sistemas de información con entidades externas deberá estar soportado con un acuerdo, convenio o documento de formalización.

Los computadores del Ministerio de Educación Nacional que se conectarán de manera directa con computadores de entidades externas, conexiones seguras deberán tener previa autorización de la Oficina de Tecnología.

Toda información secreta y/o confidencial que se transmita por las redes de comunicación del Ministerio de Educación Nacional e internet deberá estar cifrada

iv.) Responsables

Servidores públicos de la Oficina de Tecnología y sus terceros contratistas e interventores.

v.) Sanciones

El incumplimiento de esta política conllevará a notificación al superior inmediato, con copia a la Subdirección de Talento Humano, en el caso de terceros, esto conllevará una nota solicitando explicación al representante legal de la firma a la que pertenece el contratista.

2.9 Política 9. Seguridad de los recursos humanos

i.) Alcance

Servidores públicos (funcionarios y contratistas) que tienen acceso a la red y a los servicios informáticos disponibles y personas naturales y jurídicas que usen recursos propios o dispongan recursos para el desarrollo de actividades en el Ministerio de Educación Nacional y que tengan acceso a la red y a los recursos o servicios informáticos disponibles

ii.) Objetivo

Garantizar que los recursos humanos que tienen acceso a los recursos tecnológicos dispuestos por la entidad, están identificados y controladas sus actuaciones de manera que contibuyan a mantener un ambiente seguro para el beneficio de todos los servidores públicos y de la gestión de la entidad

iii.) Descripción

Todos los funcionarios y contratistas del Ministerio de Educación Nacional, deberán contar con un control biométrico de acceso a las instalaciones del Ministerio y a aquellas consideradas críticas por razones de seguridad. Adicionalmente deberán portar un carnet que los identifique plenamente. Sus datos serán consignados en una base de datos única de registro de usuarios, con la cual se realizarán las validaciones necesarias para que los usuarios accedan.

iv.) Responsables

Todos los funcionarios públicos y contratistas y sus jefes inmediatos y delegados de firmas o entidades externas y sus interventores. Los responsables por el esquema de seguridad de la entidad y de los equipos de desarrollo de los sistemas de información de la Oficina de Tecnología.

v.) Sanciones

El incumplimiento de esta política conllevará a notificación al superior inmediato, con copia a la Subdirección de Talento Humano, en el caso de terceros, esto conllevará una nota solicitando explicación al representante legal de la firma a la que pertenece el contratista.

2.10 Política 10. Seguridad en el desarrollo y mantenimiento de los sistemas de información

i.) Alcance

Funcionarios de la Oficina de Tecnología y sus terceros (personas naturales y jurídicas) contratistas e interventores.

ii.) Objetivo

Incorporar las políticas de seguridad de la información en el software y las aplicaciones desarrolladas o adquiridas por la Oficina de Tecnología del Ministerio de Educación, de manera que se garantice la operación segura de los sistemas de información y éstos contribuyan a la gestión de la entidad en un ambiente confiable y auditable, para el mejoramiento continuo.

iii.) Descripción

Todas las políticas de seguridad deben ser tenidas en cuenta en el desarrollo de los sistemas de información y en su mantenimiento.

Los sistemas de información deberán contar desde su diseño con un capítulo de administración de usuarios, roles, perfiles autenticación y autorizaciones y auditoría de eventos con el fin de establecer las autorizaciones y el alcance de las actuaciones de cada usuario en el uso de las funcionalidades de los sistemas de información.

Todo el software que se adquiera, o que se solicite desarrollar con un proveedor o con una casa de software deberá observar las políticas de seguridad del Ministerio de Educación Nacional y deberá formar parte de las herramientas de seguridad informática.

Los Sistemas de Información del Sector educativo deben propender por compartir un directorio único de usuarios activos a nivel nacional, con el fin de reducir los mecanismos de autenticación disponibles y concentrar el ingreso de los usuarios en un solo punto de acceso (Single sign on). Dada la complejidad de este enfoque la recomendación es que se realice de manera gradual, sin afectar el normal funcionamiento de los procesos y sin afectar las actividades de servicio a los usuarios.

iv.) Responsables

Servidores públicos de la Oficina de Tecnología y sus terceros contratistas e interventores.

v.) Sanciones

El incumplimiento de esta política conllevará a notificación al superior inmediato, con copia a la Subdirección de Talento Humano, en el caso de terceros, esto conllevará una nota solicitando explicación al representante legal de la firma a la que pertenece el contratista.

2.11 Política 11. Software utilizado

i.) Alcance

Servidores públicos (funcionarios y contratistas) que tienen acceso a la red y a los servicios informáticos disponibles y personas naturales y jurídicas que usen recursos propios o dispongan recursos para el desarrollo de actividades en el Ministerio de Educación Nacional y que tengan acceso a la red y a los recursos o servicios informáticos disponibles

ii.) Objetivo

Garantizar que el software utilizado por todos los equipos de cómputo propiedad del Ministerio de Educación Nacional, y de aquellos que no siendo de su propiedad, hagan parte de la red telemática de la entidad, observen las condiciones adecuadas de seguridad, propiedad y desempeño necesarios para que la operación de la entidad en sus medios tecnológicos sea segura.

iii.) Descripción

Todo software que utilice el Ministerio de Educación Nacional será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Entidad o reglamentos internos.

Todo el software de manejo de datos que utilice el Ministerio de Educación Nacional dentro de su infraestructura informática, deberá contar con las técnicas más avanzadas de la industria para garantizar la integridad de los datos.

Debe existir una cultura informática al interior de la Entidad que garantice el conocimiento por parte de los funcionarios y contratistas y las implicaciones que tiene el instalar software ilegal en los computadores del Ministerio de Educación Nacional.

El Ministerio de Educación Nacional contará con un inventario de las licencias de software que permita su adecuada administración y control evitando posibles sanciones por instalación de software no licenciado. Las responsabilidades legales o penales que surjan por la instalación de software de manera ilegal serán asumidas por los funcionarios responsables de cada equipo.

Por ningún motivo los funcionarios, contratistas o terceros estarán autorizados a instalar software en los equipos asignados y de propiedad del Ministerio de Educación Nacional.

Existirá una reglamentación de uso para los productos de software instalado en demostración en los computadores del Ministerio de Educación Nacional.

iv.) Responsables

Todos los funcionarios públicos y contratistas y sus jefes inmediatos y delegados de firmas o entidades externas y sus interventores. Los responsables por el esquema de seguridad de la entidad y de los equipos de desarrollo de los sistemas de información de la Oficina de Tecnología.

v.) Sanciones

El incumplimiento de esta política conllevará a notificación al superior inmediato, con copia a la Subdirección de Talento Humano, en el caso de terceros, esto conllevará una nota solicitando explicación al representante legal de la firma a la que pertenece el contratista.

2.12 Política 12. Actualización de Hardware

i.) Alcance

Servidores públicos (funcionarios y contratistas) que tienen acceso a la red y a los servicios informáticos disponibles y personas naturales y jurídicas que usen recursos propios o dispongan recursos para el desarrollo de actividades en el Ministerio de Educación Nacional y que tengan acceso a la red y a los recursos o servicios informáticos disponibles.

ii.) Objetivo

Garantizar que la actualización del hardware propiedad de la entidad y comprometido en la prestación de los servicios, se encuentre debidamente actualizado, en firmware, software de administración, software operativo y en parches de seguridad, de manera que garantice su operación de manera segura y confiable.

iii.) Descripción

Cualquier cambio que se requiera realizar en los equipos de cómputo de la entidad (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización de la Oficina de Tecnología.

La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado.

Los equipos de microcomputadores (PC, servidores, LAN etc.) no deben moverse o reubicarse sin la aprobación previa del administrador, jefe o coordinador del área involucrada y el movimiento lo realizará únicamente el personal autorizado de la Oficina de Tecnología

iv.) Responsables

Todos los funcionarios públicos y contratistas y sus jefes inmediatos y delegados de firmas o entidades externas y sus interventores. Los responsables por el esquema de seguridad de la entidad y del soporte técnico a los equipos de cómputo y en especial el personal de la Oficina de Tecnología.

v.) Sanciones

El incumplimiento de esta política conllevará a notificación al superior inmediato, con copia a la Subdirección de Talento Humano, en el caso de terceros, esto conllevará una nota solicitando explicación al representante legal de la firma a la que pertenece el contratista.

Políticas sobre los procesos de gestión:

2.13 Política 13. Administración de cambios

i.) Alcance

Servidores públicos (funcionarios y contratistas) que tienen acceso a la red y a los servicios informáticos disponibles y personas naturales y jurídicas que usen recursos propios o dispongan recursos para el desarrollo de actividades en el Ministerio de Educación Nacional y que tengan acceso a la red y a los recursos o servicios informáticos disponibles y ue soliciten estudiar cambios en los sistemas de información.

ii.) Objetivo

Garantizar que la gestión de cambios que afecten la operación y el servicio de los recursos tecnológicos, cumpla con los requerimientos de seguridad definidos en este manual de políticas de seguridad informática, de manera que siempre se garantice un ambiente seguro y confiable para la operación y el servicio.

iii.) Descripción

Todo cambio (creación y modificación de programas, consultas, funcionalidades y reportes) que afecte los recursos informáticos, debe ser requerido por los usuarios de la información, los analistas de la información o los ingenieros de desarrollo de los sistemas de información y aprobado formalmente por el responsable de la administración del mismo, al nivel de jefe inmediato o a quienes estos formalmente deleguen. El responsable de la administración de los accesos tendrá la facultad de aceptar o rechazar la solicitud.

Bajo ninguna circunstancia un cambio puede ser aprobado, realizado e implantado por la misma persona o área, o sin el cumplimiento de los procedimientos o sin el diligenciamiento de los formatos previstos para este efecto.

Para la administración de cambios se efectuará el procedimiento correspondiente definido por la Oficina de Tecnología del Ministerio de Educación Nacional, de acuerdo con el tipo de cambio solicitado en la plataforma tecnológica.

Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.

Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

iv.) Responsables

Todos los funcionarios públicos y contratistas y sus jefes inmediatos y delegados de firmas o entidades externas y sus interventores. Los responsables por el esquema de seguridad de la entidad y del soporte técnico a los equipos de cómputo y en especial el personal de la Oficina de Tecnología que tiene acceso a los recursos tecnológicos y a los elementos que conforman el software al servicio de los sistemas de información.

v.) Sanciones

El incumplimiento de esta política conllevará a notificación al superior inmediato, con copia a la Subdirección de Talento Humano, en el caso de terceros, esto conllevará una nota solicitando explicación al representante legal de la firma a la que pertenece el contratista.

2.14 Política 14. Almacenamiento y respaldo

i.) Alcance

Servidores públicos (funcionarios y contratistas) que tienen acceso a la red y a los servicios informáticos disponibles y personas naturales y jurídicas que usen recursos propios o dispongan recursos para el desarrollo de actividades en el Ministerio de Educación Nacional y que tengan acceso a la red y a los recursos o servicios informáticos disponibles

ii.) Objetivo

Garantizar que las copias de seguridad de la información, así como el almacenamiento en disco activo e histórico se realice de la manera más adecuada, protegiendo a la entidad de pérdida de información significativa para los procesos de gestión, para dar respuesta a peticiones de terceros y para garantizar que la información oficial tenga un ciclo de vida adecuado según los requerimientos legales ante exigibilidades de entidades de control o de otras instancias del estado.

iii.) Descripción

La información que es soportada por la infraestructura de tecnología informática del Ministerio de Educación Nacional deberá ser almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad.

Debe existir una definición formal de la estrategia de generación, retención y rotación de las copias de respaldo.

La entidad definirá la custodia de los respaldos de la información que se realizará externamente con una compañía especializada en este tema.

El almacenamiento de la información deberá realizarse interna y/o externamente a la Entidad, esto de acuerdo con la importancia de la información para la operación del Ministerio de Educación Nacional.

La Oficina de Tecnología en consulta con el área generadora de la información definirá la estrategia a seguir para el respaldo de la información.

Los funcionarios públicos son responsables de los respaldos de su información en los microcomputadores, siguiendo las indicaciones técnicas dictadas por la Oficina de Tecnología. La Oficina de Tecnología será la autorizada para realizar el seguimiento y control de esta política y de definir los mecanismos de apoyo a los usuarios para que su información sea respaldada correcta y oportunamente.

iv.) Responsables

Todos los funcionarios públicos y contratistas y sus jefes inmediatos y delegados de firmas o entidades externas y sus interventores. Los responsables por el esquema de seguridad de la entidad y del soporte técnico a los equipos de cómputo y en especial el personal de la Oficina de Tecnología que tiene acceso a los recursos tecnológicos y a los elementos que conforman el esquema de respaldo y de almacenamiento de la información.

v.) Sanciones

El incumplimiento de esta política conllevará a notificación al superior inmediato, con copia a la Subdirección de Talento Humano, en el caso de terceros, esto conllevará una nota solicitando explicación al representante legal de la firma a la que pertenece el contratista.

2.15 Política 15. Administración de la seguridad

i.) Alcance

Servidores públicos (funcionarios y contratistas) que tienen acceso a la red y a los servicios informáticos disponibles y personas naturales y jurídicas que usen recursos propios o dispongan recursos para el desarrollo de actividades en el Ministerio de Educación Nacional y que tengan acceso a la red y a los recursos o servicios informáticos disponibles

ii.) Objetivo

Garantizar que exista una administración de la seguridad que se realice en forma permanente, con el liderazgo de la Oficina de Tecnología y con la participación de todos los actores involucrados en la disposición y uso de los recursos tecnológicos, de manera costo-efectiva y confiable y que permita un ambiente seguro de operación, en un esquema de mejoramiento continuo y permanente.

iii.) Descripción

La evaluación de riesgos de seguridad para los recursos informáticos en producción se debe ejecutar al menos una vez cada dos años. Todas las mejoras, actualizaciones, conversiones y cambios relativos asociados con estos recursos deben ser precedidos por una evaluación del riesgo.

Cualquier brecha de seguridad o sospecha en la mala utilización en el Internet, la red corporativa o Intranet, los recursos informáticos de cualquier nivel (local o corporativo) deberá ser comunicada por el funcionario que la detecta, en forma inmediata y confidencial a la Oficina de Tecnología.

Los servidores públicos del Ministerio de Educación Nacional que realicen las labores de administración del recurso informático son responsables por la implementación, permanencia y administración de los controles sobre todos los recursos. La implementación debe ser consistente con las prácticas establecidas por la Oficina de Tecnología.

La Oficina de Tecnología divulgará, las políticas, estándares y procedimientos en materia de seguridad informática. Efectuará el seguimiento al cumplimiento de las políticas de seguridad y reportará a la dirección, los casos de incumplimiento con copia a la oficina de control interno.

iv.) Responsables

Todos los funcionarios públicos y contratistas y sus jefes inmediatos y delegados de firmas o entidades externas y sus interventores. Los responsables por el esquema de seguridad de la entidad y del soporte técnico a los equipos de cómputo y en especial el personal de la Oficina de Tecnología que tiene acceso a los recursos tecnológicos y a los elementos que conforman el software al servicio de los sistemas de información.

v.) **Sanciones**

El incumplimiento de esta política conllevará a notificación al superior inmediato, con copia a la Subdirección de Talento Humano, en el caso de terceros, esto conllevará una nota solicitando explicación al representante legal de la firma a la que pertenece el contratista.

2.16 Política 16. Contingencia

i.) Alcance

Servidores públicos (funcionarios y contratistas) que tienen acceso a la red y a los servicios informáticos disponibles y personas naturales y jurídicas que usen recursos propios o dispongan recursos para el desarrollo de actividades en el Ministerio de Educación Nacional y que tengan acceso a la red y a los recursos o servicios informáticos disponibles

ii.) Objetivo

Garantizar una capacidad contingente de operación de los servicios más críticos para prestar un servicio aún en condiciones críticas de fuerza mayor o desastre en alguno de los centros de cómputo y que afecten gravemente los recursos comprometidos en la prestación del servicio. La gestión debe ser realizada con mecanismos contingentes preferiblemente activos, de tal forma que ante una contingencia se pueda reaccionar de manera inmediata, de no ser así por decisiones de costos o de oportunidad, la Oficina de Tecnología dispondrá de procedimientos de recuperación y recobro ante fallas de fuerza mayor.

iii.) **Descripción**

La Oficina de Tecnología del Ministerio de Educación Nacional debe preparar, actualizar periódicamente y probar en forma regular un plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, explosión, terrorismo, inundación u otras circunstancias de fuerza mayor

iv.) Responsables

Todos los funcionarios públicos y contratistas y sus jefes inmediatos y delegados de firmas o entidades externas y sus interventores. Los responsables por el esquema de seguridad de la entidad y del soporte técnico a los equipos de cómputo y en especial el personal de la Oficina de Tecnología que tiene acceso a los recursos tecnológicos y a los elementos que conforman el software al servicio de los sistemas de información.

v.) Sanciones

El incumplimiento de esta política conllevará a notificación al superior inmediato, con copia a la Subdirección de Talento Humano, en el caso de terceros, esto conllevará una nota solicitando explicación al representante legal de la firma a la que pertenece el contratista.

2.17 Política 17. Auditoría

i.) Alcance

Servidores públicos (funcionarios y contratistas) que tienen acceso a la red y a los servicios informáticos disponibles y personas naturales y jurídicas que usen recursos propios o dispongan recursos para el desarrollo de actividades en el

Ministerio de Educación Nacional y que tengan acceso a la red y a los recursos o servicios informáticos disponibles

ii.) Objetivo

Garantizar condiciones suficientes y adecuadas para realizar labores de auditaje al uso, a los datos registrados, al procesamiento realizado y al servicio prestado por parte de los sistemas de información que el Ministerio de Educación Nacional; a través de la Oficina de Tecnología, en quien ha delegado de manera única la prestación de servicios tecnológicos a usuarios internos y externos, ha puesto a disposición del sector. De esta manera se crearán y mantendrán las condiciones para que puedan ser verificados, auditados por áreas internas o externas en funciones de control y/o auditaje, todos los servicios de información y la infraestructura que los presta.

iii.) **Descripción**

Todos los sistemas automáticos que operen y administren información sensitiva, valiosa o crítica para el Ministerio de Educación Nacional, o para las entidades del sector, tales como lo son los sistemas de aplicación en producción, sistemas operativos, sistemas de bases de datos y telecomunicaciones deben generar pistas (adición, modificación, borrado) de auditoria.

Todos los archivos de auditorias deben proporcionar suficiente información para apoyar el monitoreo, control y auditorias.

Todos los archivos de auditorias de los diferentes sistemas deben preservarse por periodos definidos según su criticidad y de acuerdo a las exigencias legales para cada caso.

Todos los archivos de auditorias deben ser custodiados en forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personas autorizadas; los usuarios que no estén autorizados deben solicitarlos al área encargada de su administración y custodia.

Todos los computadores de la Entidad deben estar sincronizados y tener la fecha y hora exacta para que el registro en la auditoria sea correcto.

iv.) Responsables

Todos los funcionarios públicos y contratistas y sus jefes inmediatos y delegados de firmas o entidades externas y sus interventores. Los responsables por el esquema de seguridad de la entidad y del soporte técnico a los equipos de cómputo y en especial el personal de la Oficina de Tecnología que tiene acceso a los recursos tecnológicos y a los elementos que conforman el software al servicio de los sistemas de información.

v.) Sanciones

El incumplimiento de esta política conllevará a notificación al superior inmediato, con copia a la Subdirección de Talento Humano, en el caso de

terceros, esto conllevará una nota solicitando explicación al representante legal de la firma a la que pertenece el contratista.

Políticas sobre la confidencialidad y la propiedad:

2.18 Política 18. Confidencialidad

i.) Alcance

Servidores públicos (funcionarios y contratistas) que tienen acceso a la red y a los servicios informáticos disponibles y personas naturales y jurídicas que usen recursos propios o dispongan recursos para el desarrollo de actividades en el Ministerio de Educación Nacional y que tengan acceso a la red y a los recursos o servicios informáticos disponibles

ii.) Objetivo

Garantizar el respeto por la confidencialidad de la información y realizar un tratamiento especial con el fin de proteger derechos de los individuos y de las entidades que solicitan servicios al Ministerio de Educación Nacional o que son sujeto de las actuaciones de control propias de la prestación de los servicios educativos en el territorio nacional.

iii.) **Descripción**

Los servidores públicos del Ministerio de Educación Nacional, mantendrá el uso restringido de información considerada como de carácter confidencial, tal como información individual de personas naturales, contemplada en la ley de habeas data y otras disposiciones; de igual manera, la información de trámites no será de uso público hasta que el resultado del trámite no haya sido público y en general se mantendrá la responsabilidad de administrar la información de manera confidencial cuando se requiera.

iv.) Responsables

Todos los funcionarios públicos y contratistas y sus jefes inmediatos y delegados de firmas o entidades externas y sus interventores. Los responsables por el esquema de seguridad de la entidad y del soporte técnico a los equipos de cómputo y en especial el personal de la Oficina de Tecnología que tiene acceso a los recursos tecnológicos y a los elementos que conforman el software al servicio de los sistemas de información.

v.) Sanciones

El incumplimiento de esta política conllevará a notificación al superior inmediato, con copia a la Subdirección de Talento Humano, en el caso de terceros, esto conllevará una nota solicitando explicación al representante legal de la firma a la que pertenece el contratista.

2.19 Política 19. Propiedad de los recursos

i.) Alcance

Servidores públicos (funcionarios y contratistas) que tienen acceso a la red y a los servicios informáticos disponibles y personas naturales y jurídicas que usen recursos propios o dispongan recursos para el desarrollo de actividades en el Ministerio de Educación Nacional y que tengan acceso a la red y a los recursos o servicios informáticos disponibles

ii.) Objetivo

Garantizar el respeto a la propiedad de los activos de la entidad y de terceros, observando las políticas necesarias para que su operación se realice de manera segura y confiable.

iii.) **Descripción**

Todos los recursos que sean propiedad del Ministerio de Educación Nacional, deberán observar las políticas de seguridad de la entidad sin excepción alguna. Por ninguna razón, recursos que no son propiedad de la entidad, harán parte activa del sistema de seguridad, en todo caso la Oficina de Tecnología se reservará la administración de cualquier bien tecnológico o informático que se use en el Ministerio de Educación Nacional.

iv.) Responsables

Todos los funcionarios públicos y contratistas y sus jefes inmediatos y delegados de firmas o entidades externas y sus interventores. Los responsables por el esquema de seguridad de la entidad y del soporte técnico a los equipos de cómputo y en especial el personal de la Oficina de Tecnología que tiene acceso a los recursos tecnológicos y a los elementos que conforman el software al servicio de los sistemas de información.

v.) Sanciones

El incumplimiento de esta política conllevará a notificación al superior inmediato, con copia a la Subdirección de Talento Humano, en el caso de terceros, esto conllevará una nota solicitando explicación al representante legal de la firma a la que pertenece el contratista.

2.20 Política 20. Propiedad intelectual

i.) Alcance

Servidores públicos (funcionarios y contratistas) que tienen acceso a la red y a los servicios informáticos disponibles y personas naturales y jurídicas que usen recursos propios o dispongan recursos para el desarrollo de actividades en el Ministerio de Educación Nacional y que tengan acceso a la red y a los recursos o servicios informáticos disponibles

ii.) Objetivo

Garantizar el respeto a la propiedad intelectual de los activos de la entidad y de terceros, observando las políticas necesarias para que su operación se realice de manera segura y confiable.

iii.) **Descripción**

El Ministerio de educación Nacional cumplirá ateniéndose a las disposiciones legales los lineamientos de protección de la propiedad intelectual de terceros y exigirá el cumplimiento de sus derechos de propiedad intelectual y patrimonial sobre los sistemas de información de su propiedad, de manera que no se incurra en ninguna transgresión a los derechos de terceros o propios del Ministerio de Educación Nacional. Estas disposiciones incluyen, la adquisición de licencias de uso de manera legal, el respeto por las condiciones de uso, instalación, divulgación e intercambio de piezas de software de terceros, de acuerdo con las condiciones de licenciamiento que se pacten con los propietarios de los derechos o de sus representantes. En ningún caso se aceptará que un equipo que sea propiedad del Ministerio de Educación Nacional, cuente con software ilegal o que ponga en riesgo el cumplimiento de las disposiciones de respeto por la propiedad intelectual del software.

iv.) Responsables

Todos los funcionarios públicos y contratistas y sus jefes inmediatos y delegados de firmas o entidades externas y sus interventores. Los responsables por el esquema de seguridad de la entidad y del soporte técnico a los equipos de cómputo y en especial el personal de la Oficina de Tecnología que tiene acceso a los recursos tecnológicos y a los elementos que conforman el software al servicio de los sistemas de información.

v.) Sanciones

El incumplimiento de esta política conllevará a notificación al superior inmediato, con copia a la Subdirección de Talento Humano, en el caso de terceros, esto conllevará una nota solicitando explicación al representante legal de la firma a la que pertenece el contratista.