MANUAL DE POLÍTICAS DE SEGURIDAD EMELNORTE

Este manual de políticas de seguridad es elaborado de acuerdo al análisis de riesgos y vulnerabilidades en las direcciones de la Empresa Eléctrica Regional Norte S.A. – EMELNORTE, por consiguiente el alcance de estas políticas, se encuentra sujeto a la empresa.

1 ACTIVOS

Toda adquisición de tecnología informática se efectuará a través del Departamento de Adquisiciones (Portal de Compras Públicas) previo a un requerimiento de usuario y la respectiva autorización del Director correspondiente, deberá constar en el presupuesto.

La adquisición de bienes informáticos, quedará sujeta a los lineamientos establecidos en esta política.

1.1 DE INFORMACIÓN

La Dirección de Tecnologías de la Información y Comunicación tiene como objetivo asegurar que la información recibe el nivel de protección adecuado. La información se debería clasificar para indicar la necesidad, las prioridades y el grado esperado de protección al manejar la información.

La información tiene diferentes grados de sensibilidad e importancia. Algunos elementos pueden requerir un grado adicional de protección o manejo especial. Se recomienda utilizar un esquema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas especiales de manejo.

La información que cada usuario mantiene en sus equipos es de su responsabilidad, la Dirección de Tecnologías de la Información y Comunicación, no se responsabilizará en caso de pérdida de la misma.

1.2 DE SOFTWARE, FÍSICOS Y SERVICIOS

La Dirección de Tecnologías de la Información y Comunicación, al planear las operaciones relativas a la adquisición de bienes informáticos y/o servicios, establecerá prioridades y en su selección deberá tomar en cuenta: estudio técnico, precio, calidad, experiencia, desarrollo tecnológico, estándares y capacidad, entendiéndose por:

Precio
Costo inicial, costo de mantenimiento y consumibles por el período estimado de uso de los equipos;

Calidad
Parámetro cualitativo que especifica las características técnicas de los recursos informáticos.

Experiencia
Presencia en el mercado nacional e internacional, estructura de servicio, la confiabilidad de los bienes y certificados de calidad con los que se cuente.

Desarrollo Tecnológico
Se deberá analizar su vida útil, su nivel tecnológico con respecto a la oferta existente y su permanencia en el mercado.

Capacidades
Se deberá analizar si satisface la demanda actual con un margen de holgura y capacidad de crecimiento para soportar la carga de trabajo del área.

Los Recursos Informáticos, Datos, Software, Red Corporativa y Sistemas de Comunicación Electrónica están disponibles exclusivamente para cumplir las obligaciones y propósito de la operación para la que fueron diseñados e implantados.

Todos los usuarios de dichos recursos deben saber que no tiene el derecho de confidencialidad en su uso.

El introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos, será motivo de sanción para los funcionarios, de acuerdo a la normativa vigente.

Perturbar el trabajo de los demás enviando mensajes o archivos que puedan inferir en el trabajo de otro usuario de la red, incurrirá en la aplicación de la sanción según la normativa vigente.

El diseminar “virus”, “gusanos”, “troyanos” y otros tipos de programas dañinos para los sistemas de procesos de la información, será motivo de sanción.

2 EQUIPOS DE CÓMPUTO

2.1 DE LA INSTALACIÓN

La instalación del equipo de cómputo, quedará sujeta a los siguientes lineamientos:

Los equipos para uso interno se instalarán en lugares adecuados, lejos de polvo y alto tráfico de personas.

Todo equipo de cómputo, que esté o sea conectado a la red de EMELNORTE, o aquel que en forma autónoma se tenga y que sea propiedad de la institución debe sujetarse a las normas y procedimientos de instalación que emite La Dirección de Tecnologías de la Información y Comunicación.

La Dirección de TIC’s deberá contar con un plano actualizado de las instalaciones eléctricas y de comunicaciones.

Las instalaciones eléctricas y de comunicaciones, estarán de preferencias fijas o en su defecto resguardadas del paso de personas o máquinas, y libres de cualquier interferencia eléctrica o magnética.

Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.

En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.

Los equipos informáticos mantendrán una estandarización en los nombres que se le asigne, cumpliendo con las necesidades de la Dirección de TIC's. El nombre no debe exceder de 15 caracteres.

El formato de nombres de los equipos de cómputo (computadores de escritorio, portátiles) sería el siguiente:

10IBATICSOP-16

10: ÁREA REFERENCIAL CÓDIGO PROVINCIAL
IBA: CIUDAD, CANTÓN DE UBICACIÓN DE LA EMPRESA O SUCURSAL
TIC: CORRESPONDE A LA DIRECCIÓN
SOP: ÁREA DE LA DIRECCIÓN
16: CUARTO OCTETO DE LA DIRECCIÓN IP

Para el caso de impresoras será el siguiente formato indicado:

10IBATICIMP-24

10: ÁREA REFERENCIAL CÓDIGO PROVINCIAL
IBA: CIUDAD, CANTÓN DE UBICACIÓN DE LA EMPRESA O SUCURSAL
TIC: CORRESPONDE A LA DIRECCIÓN, AREA O DEPARTAMENTO
IMP: INDICA QUE ES UNA IMPRESORA
24: CUARTO OCTETO DE LA DIRECCIÓN IP

Para el caso de cámaras de video vigilancia será el siguiente:

IBMATPB20-51

IBA: CIUDAD, CANTÓN DE UBICACIÓN DE LA EMPRESA O SUCURSAL
MAT: NOMBRE DE LA SUCURSAL

PB: UBICACIÓN FISICA
20: CUARTO OCTETO DE LA DIRECCIÓN IP
51: VLAN ASIGNADA

Los formatos para los nombres de los equipos informáticos debe actualizarse periódicamente por la Dirección de TIC's.

2.2 PARA EL MANTENIMIENTO

Es obligación de la Dirección de TIC's vigilar que el equipo de cómputo se use bajo las condiciones especificadas por el proveedor y de acuerdo a las funciones del área a la que se asigne.

Los empleados de la empresa al usar el equipo de cómputo, se abstendrán de consumir alimentos, fumar o realizar actos que perjudiquen el funcionamiento del mismo o deterioren la información almacenada en medios magnéticos, ópticos, o medios de almacenamiento removibles de última generación.

A la Dirección de TIC's corresponde la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física y su acondicionamiento específico a que tenga lugar. Para tal fin debe emitir las normas y procedimientos respectivos.

Los responsables la Dirección de Tecnologías de la Información y Comunicación son los únicos autorizados para realizar mantenimiento preventivo y correctivo, o para autorizar el mantenimiento por parte de terceros.

2.3 DE LA ACTUALIZACIÓN

La Dirección de TIC's es responsable de mantener versiones actualizadas de los sistemas usados en EMELNORTE, para ello se realizará un plan adecuado y a tiempo de las actualizaciones respectivas.

Todo equipo de cómputo (computadoras personales, estaciones de trabajo, supercomputadora y demás relacionados) y los de telecomunicaciones que sean

propiedad de la empresa debe procurarse sean actualizados tendiendo a conservar e incrementar la calidad del servicio que presta, mediante la mejora sustantiva de su desempeño.

2.4 DE LA RE-UBICACIÓN

La reubicación de los equipos de cómputo se realizará satisfaciendo las normas y procedimientos que para ello emita la Dirección de Tecnologías de la Información y Comunicación.

En caso de existir personal técnico de apoyo, este notificará de los cambios tanto físicos como de software que realice la Dirección de Tecnologías de la Información y Comunicación y al procedimiento de ALMACENAMIENTO, ASEGURAMIENTO E INVENTARIOS notificando también los cambios de los equipos para adjuntarlos al inventario.

El equipo de cómputo a reubicar se hará únicamente bajo la autorización del responsable, contando el lugar a donde se hará la ubicación con los medios necesarios para la instalación del equipo.

Es responsabilidad de cada usuario informar a la Dirección de TIC´s, mediante hojas de requerimiento la necesidad de reubicar los equipos para dar la asistencia correspondiente.

2.5 DE LA SEGURIDAD

Cada usuario es responsable de mantener sus claves de seguridad en secreto.

Los equipos de la Empresa sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

Cualquier falla en los computadores o en la red debe reportarse inmediatamente a la Dirección de Tecnologías de la Información y Comunicación para lograr evitar problemas serios como pérdida de la información o indisponibilidad de los servicios.

No deben usarse dispositivos de almacenamiento en cualquier computadora de la Empresa sin que previamente se haya verificado que están libres de cualquier tipo de virus.

Los usuarios de PCs son responsables de realizar periódicamente el respaldo de los datos guardados en sus PCs, para evitar pérdidas de información.

Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño.

El personal que utiliza un computador portátil que contenga información confidencial de la Empresa, debe protegerlo y evitar el acceso a la información de personas no autorizadas.

Para prevenir el acceso no autorizado, utilice contraseñas difíciles de predecir y además debe configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además, cada vez que deba ausentarse de su oficina debe activar el protector de pantalla manualmente.

Para prevenir el ataque de virus, no está permitido el uso de módems de internet de cualquier operadora en los equipos de EMELNORTE que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la red interna de la Empresa.

Debe respetarse y no modificar la configuración de hardware y software establecida por la Dirección de Tecnologías de la Información y Comunicación.

Está terminantemente prohibido hacer copias o usar software de EMELNORTE para fines personales.

Los usuarios no deben copiar a un dispositivo de almacenamiento externo, el software de las computadoras de la Empresa, sin la aprobación previa de la Dirección de Tecnologías de la Información y Comunicación.

No debe utilizarse software descargado de Internet o software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que

esté aprobado su uso por la Dirección de Tecnologías de la Información y Comunicación.

Se prohíbe estrictamente la instalación de software no autorizado, sin que haya sido previamente aprobado por la Dirección de Tecnologías de la Información y Comunicación, con el fin de prevenir la introducción de virus informáticos.

El internet es estrictamente para uso de las actividades propias de la Empresa y su uso será autorizado por la Presidencia Ejecutiva.

Queda totalmente prohibido, sacar los equipos de computación de la Empresa sin previa autorización por parte del director de cada dependencia. En caso de ser necesario sacar los mismos, se debe llenar el formulario de movilización de equipos y entregar al personal de seguridad.

3 COMUNICACIONES Y OPERACIONES

3.1 PROCEDIMIENTOS Y RESPONSABILIDADES

El objetivo de la Dirección de Tecnologías de la Información y Comunicación es asegurar la operación correcta y segura de los servicios de procesamiento de información.

Se deberían establecer todas las responsabilidades y los procedimientos para la gestión y operación de todos los servicios de procesamiento de información. Esto incluye el desarrollo de procedimientos operativos apropiados.

Cuando sea conveniente, se debería implementar la separación de funciones para reducir el riesgo de uso inadecuado deliberado o negligente del sistema.

3.2 PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA

La Dirección de Tecnologías de la Información y Comunicación pretende minimizar el riesgo de fallas en los sistemas.

Se requieren una previa planificación y preparación para garantizar la disponibilidad de la capacidad y los recursos adecuados para entregar el desempeño requerido del sistema.

Es necesario hacer proyecciones de la capacidad futura para reducir el riesgo de sobrecarga del sistema.

Los requisitos operativos de los sistemas nuevos se deberían establecer, documentar y probar antes de su aceptación y uso.

3.3 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS Y MÓVILES

La Dirección de Tecnologías de la Información y Comunicación busca proteger la integridad del software y de la información.

Se requieren precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no autorizados.

El software y los servicios de procesamiento de información son vulnerables a la introducción de códigos maliciosos tales como virus de computador, gusanos en la red, caballos troyanos y bombas lógicas. Los usuarios deberían ser conscientes de los peligros de los códigos maliciosos. Los directores deberían, cuando sea apropiado, coordinar con la dirección de TIC’s los controles para evitar, detectar y retirar los códigos maliciosos y controlar los códigos móviles.

Se encuentra prohibida la conexión de equipos móviles, que no sean de la empresa, a la red interna de EMELNORTE, a menos de que exista la respectiva autorización de la Presidencia Ejecutiva.

3.4 RESPALDO

La Dirección de Tecnologías de la Información y Comunicación pretende mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.

Se deberían establecer procedimientos de rutina para implementar la política y la estrategia de respaldo acordada para hacer copias de la seguridad de los datos y probar sus tiempos de restauración.

El personal responsable de mantener los servicios informáticos operativos, deberá sacar respaldos de la información de forma mensual y almacenarlos en un lugar seguro.

3.5 SEGURIDAD EN LAS REDES

La Dirección de Tecnologías de la Información y Comunicación busca asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

La gestión segura de las redes, las cuales pueden sobrepasar las fronteras de la organización, exige la consideración cuidadosa del flujo de datos, las implicaciones legales, el monitoreo y la protección.

También pueden ser necesarios los controles adicionales para proteger la información sensible que pasa por las redes públicas.

3.6 MANEJO DE LOS MEDIOS

La Dirección de Tecnologías de la Información y Comunicación trata de evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio.

Estos medios se deberían controlar y proteger de forma física.

Se deberían establecer procedimientos operativos adecuados para proteger documentos, medios de computador (por ejemplo cintas, discos), datos de entrada/salida y documentación del sistema contra divulgación, modificación, remoción y destrucción no autorizadas.

3.7 MONITOREO

La Dirección de Tecnologías de la Información y Comunicación pretende detectar actividades de procesamiento de la información no autorizadas.

Se deberían monitorear los sistemas y registrar los eventos de la seguridad de la información. Los registros de operador y la actividad de registro de fallas se deberían utilizar para garantizar la identificación de los problemas del sistema de información.

Una organización debería cumplir todos los requisitos legales pertinentes que se aplican a sus actividades de monitoreo y registro.

Debería emplearse el monitoreo del sistema para verificar la eficacia de los controles adoptados y revisar el cumplimiento de un modelo de política de acceso.

4 CONTROL DE ACCESO

4.1 GESTIÓN DEL ACCESO DE LOS USUARIOS

Todos los usuarios con acceso a un sistema de información o a una red informática, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.

Ningún usuario recibirá un identificador de acceso a la Red de Comunicaciones, Recursos Informáticos o Aplicaciones hasta que no acepte formalmente la Política de Seguridad vigente.

Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el responsable de la información.

La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.

Los identificadores para usuarios temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.

Cada usuario, dispondrá de un identificador único, el cual se corresponde con la cuenta de usuario.

A cada identificador de usuario corresponderá una, y solo una persona física.

Todas aquellas operaciones realizadas por un usuario, serán siempre atribuidas al identificador utilizado que se hubiere identificado ante el sistema de información.

La Dirección de TIC's, realizará mensualmente, la actualización de usuarios, en coordinación con la Dirección de Talento Humano.

4.2 RESPONSABILIDAD DE LOS USUARIOS

Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.

Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.

Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su

contraseña e informar a su jefe inmediato y éste reportar al responsable de la administración de la red.

El Usuario debe utilizar una contraseña compuesta por un mínimo de ocho caracteres constituida por una combinación de caracteres alfabéticos, numéricos y especiales.

La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos.

En caso que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.

En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 15 días. Caso contrario, se le podrá denegar el acceso y se deberá contactar con el jefe inmediato para solicitar al administrador de la red una nueva clave.

Proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.

Guardar por tiempo indefinido la máxima reserva y no se debe emitir al exterior datos de carácter personal contenidos en cualquier tipo de soporte.

Utilizar el menor número de listados que contengan datos de carácter personal y mantener los mismos en lugar seguro y fuera del alcance de terceros.

Cuando entre en posesión de datos de carácter personal, se entiende que dicha posesión es estrictamente temporal, y debe devolver los soportes que contienen los datos inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos.

Los usuarios sólo podrán crear ficheros que contengan datos de carácter personal para un uso temporal y siempre necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco de la computadora de trabajo y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

Los usuarios deben notificar a su jefe inmediato cualquier incidencia que detecten que afecte o pueda afectar a la seguridad de los datos de carácter personal: pérdida de listados y/o dispositivos de almacenamiento, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos.

Los usuarios únicamente introducirán datos identificativos y direcciones o teléfonos de personas en las agendas de contactos de las herramientas ofimáticas.

4.3 A LAS REDES

La Dirección de Tecnologías de la Información y Comunicación es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.

La Dirección de Tecnologías de la Información y Comunicación es la responsable de difundir el reglamento para el uso de la red y de procurar su cumplimiento.

Dado el carácter unipersonal del acceso a la Red de EMELNORTE, la Dirección de Tecnologías de la Información y Comunicación verificará el uso responsable, de acuerdo con el Reglamento para el uso de la red.

El acceso lógico a equipo especializado de cómputo (servidores, enrutadores, switches, bases de datos, equipo de supercómputo centralizado y distribuido, etc.) conectado a la red es administrado por la Dirección de Tecnologías de la Información y Comunicación.

Todo el equipo de cómputo que esté o sea conectado a la Red de EMELNORTE, o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, debe de sujetarse a los procedimientos de acceso que emite La Dirección de Tecnologías de la Información y Comunicación.

La Dirección de Tecnologías de la Información y Comunicación, será la responsable de cambiar periódicamente las claves de acceso a la red inalámbrica.

La Dirección de Tecnologías de la Información y Comunicación, deberá mantener respaldos de las configuraciones de servidores, enrutadores, switches, bases de datos, etc.

4.4 AL SISTEMA OPERATIVO, LAS APLICACIONES, INFORMACIÓN

El manejo de información administrativa que se considere de uso restringido deberá ser cifrado con el objeto de garantizar su integridad.

Tendrá acceso a los sistemas administrativos solo el personal de EMELNORTE o persona que tenga la autorización por La Dirección de Tecnologías de la Información y Comunicación.
Los servidores de bases de datos administrativos son dedicados, por lo que se prohíben los accesos de cualquiera, excepto para el personal la Dirección de Tecnologías de la Información y Comunicación.

El control de acceso a cada sistema de información de EMELNORTE será determinado por la unidad responsable de generar y procesar los datos involucrados.

Toda salida de información (en soportes informáticos o por correo electrónico) sólo podrá ser realizada por personal autorizado y será necesaria la autorización formal del responsable del área del que proviene.

4.5 COMPUTACIÓN MÓVIL Y TRABAJO REMOTO

La Dirección de Tecnologías de la Información y Comunicación es la responsable de proporcionar el servicio de acceso remoto y computación móvil, las normas de acceso a los recursos informáticos disponibles.

Para el caso especial de los recursos de cómputo a terceros deberán ser autorizados por la Dirección de Tecnologías de la Información y Comunicación.

El usuario de estos servicios deberá sujetarse al Reglamento de Uso de la Red de EMELNORTE y en concordancia con los lineamientos generales de uso de Internet.

El acceso remoto que realicen personas ajenas a la institución deberá cumplir las normas establecidas por la Dirección de Tecnologías de la Información y Comunicación.

El acceso a los servicios se realizará mediante conexiones seguras, las mismas que serán configuradas previamente por la Dirección de TIC’s y asignará un usuario y contraseña para su correcto uso.

4.6 A LA WEB

La Dirección de Tecnologías de la Información y Comunicación es la responsable de instalar y administrar el o los servidor(es) de Internet. Es decir, sólo se permiten servidores de páginas autorizados por la Dirección de Tecnologías de la Información y Comunicación.

La Dirección de Tecnologías de la Información y Comunicación deberá emitir las normas y los requerimientos para la instalación de servidores de páginas locales, de bases de datos, del uso de la Intranet institucional, así como las especificaciones para que el acceso a estos sea seguro.

Los accesos a las páginas de Web a través de los navegadores deben sujetarse a las normas que previamente se manifiestan en el Reglamento de acceso a la red de EMELNORTE.

A los responsables de los servidores de Web corresponde la verificación de respaldo y protección adecuada.
Toda la programación involucrada en la tecnología Web deberá estar de acuerdo con las normas y procedimientos establecidas por La Dirección de Tecnologías de la Información y Comunicación.

El material que aparezca en la página de Internet de EMELNORTE deberá ser aprobado para su publicación por la Presidencia Ejecutiva, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).

Con referencia a la seguridad y protección de las páginas, así como al diseño de las mismas deberá referirse a las consideraciones de diseño de páginas electrónicas establecidas por la Dirección de Tecnologías de la Información y Comunicación.

5 SOFTWARE

Todo el personal que accede a los Sistemas de Información de EMELNORTE debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.

5.1 DE LA ADQUISICIÓN

En concordancia con la política de la institución, la Dirección de Tecnologías de la Información y Comunicación es la encargada en la entidad de establecer los lineamientos para adquisición de sistemas informáticos.
En los proyectos que ejecutan las diferentes áreas de EMELNORTE deberán presupuestarse los recursos necesarios para la adquisición de sistemas de información licenciados o el desarrollo de sistemas de información a la medida.

Corresponderá a la Dirección de Tecnologías de la Información y Comunicación establecer las normas para el tipo de licenciamiento, cobertura, transferibilidad, certificación y vigencia.

La Dirección de Tecnologías de la Información y Comunicación deberá propiciar la adquisición y asesoramiento en cuanto a software de vanguardia.

5.2 DE LA INSTALACIÓN

Corresponde a la Dirección de Tecnologías de la Información y Comunicación establecer las normas y procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo.

En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento apropiado y acorde a la propiedad intelectual.

La Dirección de Tecnologías de la Información y Comunicación es la responsable de brindar asesoría y supervisión para la instalación de software informático y de telecomunicaciones.

La instalación de software que desde el punto de vista de la Dirección de Tecnologías de la Información y Comunicación pudiera poner en riesgo los recursos de la institución no está permitida.

Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso y otros que se apliquen).

A todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados.

El personal tiene prohibido borrar cualquiera de los programas instalados legalmente.

5.3 DE LA ACTUALIZACIÓN

La adquisición y actualización de software para equipo especializado de cómputo y de telecomunicaciones se llevará a cabo de acuerdo con la programación que anualmente sea propuesta por la Dirección de Tecnologías de la Información y Comunicación.

Corresponde la Dirección de Tecnologías de la Información y Comunicación autorizar cualquier adquisición y actualización de software.

Las actualizaciones del software de uso común o más generalizado se llevarán a cabo de acuerdo como lo establezca la Dirección de Tecnologías de la Información y Comunicación.

5.4 DE LA AUDITORIA DE SOFTWARE INSTALADO

El personal encargado del control interno de EMELNORTE es el responsable de realizar revisiones periódicas para asegurar que el software instalado en los computadores de la institución cuente con licencia.

5.5 DEL SOFTWARE PROPIEDAD DE LA INSTITUCIÓN

Todos los programas de la institución sean adquiridos mediante compra, donación o cesión son de su propiedad y mantendrán los derechos que la ley de propiedad intelectual le confiera.

La Dirección de Tecnologías de la Información y Comunicación en coordinación con el procedimiento de almacenamiento, aseguramiento e inventarios deberá tener un registro de todos los paquetes de programación.

Todos los sistemas programáticos (programas, bases de datos, sistemas operativos, interfaces) desarrollados con o a través de los recursos de EMELNORTE se mantendrán como propiedad de la institución respetando la propiedad intelectual de los mismos.
Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo de la institución que debe preservarse.

Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la institución deben estar resguardados.

La Dirección de Tecnologías de la Información y Comunicación propiciará la gestión de patentes y derechos de creación de software de propiedad de la institución.

La Dirección de Tecnologías de la Información y Comunicación administrará los diferentes tipos de licencias de software y vigilará su vigencia en concordancia con la política informática.

5.6 DE LA PROPIEDAD INTELECTUAL

Corresponde a la Dirección de Tecnologías de la Información y Comunicación procurar que todo el software instalado en EMELNORTE esté de acuerdo con la ley de propiedad intelectual a que dé lugar.

6 INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

La Dirección de Tecnologías de la Información y Comunicación busca asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.

Es conveniente establecer el reporte formal del evento y los procedimientos de escalada.

Todos los empleados, contratistas y usuarios de tercera parte deberían tener conciencia sobre los procedimientos para el reporte de los diferentes tipos de evento y las debilidades que puedan tener impacto en la seguridad de los activos de la organización.

Se les debería exigir que reporten todos los eventos de seguridad de la información y las debilidades tan pronto sea posible al punto de contacto designado.

6.1 REPORTE SOBRE LOS EVENTOS

Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados tan pronto como sea posible.

Se debería instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente que establezca la acción que se ha de tomar al recibir el reporte sobre un evento de seguridad de la información. Se debería establecer un punto de contacto para el reporte de los eventos de seguridad de la información. Es conveniente garantizar que este punto de contacto se conoce en toda la organización, siempre está disponible y puede suministrar respuesta oportuna y adecuada.

Todos los empleados, contratistas y usuarios de tercera parte deberían tener conciencia de su responsabilidad para reportar todos los eventos de seguridad de la información lo más pronto posible.

Deberían conocer el procedimiento para reportar los eventos de seguridad de la información y el punto de contacto. Los procedimientos de reporte deberían incluir los siguientes aspectos:

a) Procesos adecuados de retroalimentación para garantizar que aquellos que reportan los eventos de seguridad de la información reciben notificación de los resultados después de que se ha tratado y solucionado el problema;
b) Formatos para el reporte de los eventos de seguridad de la información para contener la acción de reporte y ayudar a que la persona que hace el reporte recuerde todas las acciones necesarias en caso de un evento de seguridad de la información;
c) El comportamiento correcto en caso de un evento de seguridad de la información.

6.2 REPORTE SOBRE LAS DEBILIDADES

Se debería exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.

Todos los empleados, contratistas y usuarios de terceras partes deberían informar sobre estos asuntos a su director o directamente a su proveedor de servicio, tan pronto sea posible para evitar los incidentes de seguridad de la información. Los mecanismos de reporte deberían ser fáciles, accesibles y disponibles. Se les debería informar a ellos que, en ninguna circunstancia, deberían intentar probar una debilidad sospechada.

6.3 GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN

La Dirección de Tecnologías de la Información y Comunicación tiene como objetivo asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.

Es conveniente establecer las responsabilidades y los procedimientos para manejar los eventos y debilidades de la seguridad de la información de manera eficaz una vez se han reportado. Se debería aplicar un proceso de mejora continua a la respuesta para monitorear, evaluar y gestionar en su totalidad los incidentes de seguridad de la información.

Cuando se requiere evidencia, ésta se debería recolectar para garantizar el cumplimiento de los requisitos legales.

7 SUPERVISIÓN Y CUMPLIMIENTO

7.1 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD

Debido al carácter confidencial de la información, el personal de la Dirección de Tecnologías de la Información y deberá de actuar de acuerdo con lo establecido en el Código de Ética, normas y procedimientos que rigen en la empresa.

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo a las sanciones disciplinarias y penales correspondientes.

Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del servicio dependiendo de la gravedad de la falta y de la malicia o perversidad que esta manifiesta.

7.2 VERIFICACIÓN DEL CUMPLIMIENTO TÉCNICO

Para efectos de que la institución disponga de una red con alto grado de confiabilidad, será necesario que se realice un monitoreo constante sobre todos y cada uno de los servicios que las tecnologías de la Internet e Intranet disponen.

7.3 CONSIDERACIONES DE LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN

Las auditorías de cada actividad donde se involucren aspectos de seguridad lógica y física deberán realizarse periódicamente y deberá sujetarse al calendario que establezca planeación y direccionamiento estratégico.