1. INTRODUCCIÓN

La información de una empresa se ha considerado como un activo fundamental para la prestación de los servicios y la toma de decisiones eficientes, en virtud de ello se requiere contar con estrategias que permitan el control y administración efectiva de los datos.

Dicha información pueda ser sujeta a pérdida, robo, alteración, sustracción o revelación por parte de propios o extraños de manera imprudencial o intencionada, o bien, a sufrir un uso indebido y con ello acarrear daños a su propietario, pueda ser éste un individuo o una organización, se denomina información sensitiva. "La información es poder" y por ello, debemos asegurar que dicho poder resida en nuestras manos aprendiendo a protegerla.

Para resguardarla es fundamental analizarla, evaluarla y clasificarla con el objetivo de determinar el nivel de seguridad que merece, considerando los riesgos a los cuales pueda estar expuesta. Una vez clasificada es preciso llevar a cabo respaldos o soportes, conocidos como "backups" y resguardarla adecuadamente ya sea en archivos de seguridad físicos, cajas fuertes, discos duros cuyos accesos se encuentren debidamente restringidos con contraseñas robustas. Por otro lado, es importante tener cuentas usuario a fin de tener privacidad en nuestras sesiones y restringir el acceso a otros usuarios a nuestros documentos. Asimismo, para evitar robo de información al ausentarnos de nuestro lugar, se debe activar un doble "password" de seguridad: el de arranque al iniciar sesión y el que se activa al no utilizar un sistema.

Conscientes de las necesidades actuales, se hace necesario por parte de la Red de Salud del Norte ESE implementar Políticas de Seguridad de La Información donde los usuarios incorporen buenas prácticas para proteger las leyes de derechos de autor, protección de datos personales, la seguridad informática y el entorno de información, para ello se deben conocer los deberes, recomendaciones, buenas prácticas y demás peligros latentes a nivel de informática, y cómo detenerlos a través de mecanismos de prevención.

2. DEBERES DE LOS USUARIOS DE EQUIPOS DE CÓMPUTO SOBRE EL USO DEL SOFTWARE

Para dar cumplimiento a las leyes de derechos de autor y las normas de la Red de Salud Norte sobre el uso de equipos de cómputo y software se disponen los siguientes deberes y obligaciones del usuario:

1) Ningún usuario de equipos de cómputo debe instalar ningún tipo de software. El software no autorizado encontrado en el equipo será responsabilidad del usuario del equipo. Solamente se autoriza al personal de sistemas para realizar instalaciones de software siempre y cuando este se encuentre licenciado.
2) Todos los equipos se entregan únicamente con la licencia del sistema operativo y la licencia de acceso al aplicativo de operaciones diarias (sistema de facturación, sistema contable, etc.)
3) Las licencias de software ofimática tales como Microsoft office serán instaladas únicamente en los equipos autorizados por la gerencia.
4) El acceso a internet debe ser realizado de forma responsable y segura; siendo usado únicamente para actividades de índole laboral.
5) Los usuarios deben dar buen uso del correo corporativo. Evitar el envío de mensajes con archivos adjuntos tales como cadenas, videos, música, presentaciones, etc.
6) El usuario no tiene permitido instalar o copiar archivos de tipo mp3, Mp4, u otros archivos de música y videos que no cumplan con las leyes de derechos de autor.
7) No está permitido el uso de redes punto a punto o la instalación de software para tal fin.
8) El uso indiscriminado del correo electrónico conlleva a que riesgos como el spam y los programas espías infecten las máquinas utilizadas y se incrementen las ventanas de exposición al fraude, al robo de información, a la suplantación de identidad, entre otras amenazas que a diario comprometen la seguridad informática en las organizaciones.

3. RECOMENDACIÓN SOBRE EL USO DEL SOFTWARE

1) El personal del Proceso de Sistemas de Información, puede revisar, re-instalar o des-instalar software. Tiene autorización de eliminar software que no cuente con las licencias debidamente registradas y tiene la prohibición expresa de

instalar software que no sea proporcionado por la empresa y que se encuentre debidamente licenciado.

2) Está prohibido realizar copias en CD o USB de archivos que son propiedad de la empresa, para fines externos, solo el jefe podrá realizar copias con conocimiento del jefe de área de informática.

3) Está prohibido visitar páginas con contenido obsceno, así como bajar programas de internet que no estén permitidos su instalación por parte del área de informática. Todas las páginas visitadas se van a monitorear desde el servidor web.

4. DEBERES DE LOS USUARIOS DE EQUIPOS DE COMPUTO SOBRE EL USO DEL HARDWARE

Se disponen los siguientes deberes del usuario con relación al uso de hardware:

1) Los equipos de cómputo se compone mínimo de los siguientes elementos: monitor, CPU, teclado, mouse, adicionalmente impresora si ha sido asignada. Ninguno de los componentes deberá ser manipulado por personal diferente al área de sistemas.

2) No se debe abrir ninguno de los equipos ni manipular los componentes electrónicos y/o mecánicos que los componen.

3) No se deben trasladar componentes entre equipos, ni realizar prestamos entre sedes sin previa autorización.

4) No debe consumir alimentos o bebidas en el sitio de trabajo, en el cual se encuentran instalados los equipos de cómputo.

5) Debe dar buen trato a los elementos de cómputo, evitando golpearlos o ensuciarlos.

5. DEBERES DE LOS USUARIOS DE EQUIPOS DE CÓMPUTO SOBRE EL USO DE LA INFORMACION

Se disponen los siguientes deberes del usuario con relación al uso de la información:

1) La información manejada en cada uno de los equipos de cómputo es de uso exclusivo de la organización, por tal motivo debe abstenerse de divulgar, modificar o extraer información almacenada en los medios suministrados por la institución para realizar las actividades o labores, por lo que se debe velar

por la confidencialidad de la información. El uso del correo electrónico debe realizarse de forma controlada, no debe enviar por medios electrónicos cadenas, u otros archivos de tipo personal.

2) No debe enviar correos personales masivos.

6. BUENAS PRÁCTICAS PARA LA PROTECCION DE LA INFORMACIÓN

Recomendaciones generales sobre el uso del Software

1) Abstenerse de abrir correos electrónicos de personas desconocidas, ya que normalmente estos contienen virus informáticos que se instalan con solo abrir el mensaje electrónico. Estos mensajes deben ser eliminados tan pronto aparecen en la bandeja de entrada.
2) Al navegar en internet, no navegar en sitios desconocidos ya que estos sitios normalmente instalan software no autorizado por el usuario.
3) Evite seleccionar los botones de “aceptar” en los botones de las ventanas emergentes al navegar en internet, normalmente al hacer esto está autorizando la instalación de software malicioso.
4) **Lea** las ventanas de mensajes que el computador informa antes de presionar cualquier botón de “Aceptar”.
5) No envié cadenas o mensajes ya que puede congestionar la red.
6) No abra carpetas desconocidas que provienen de memorias USB.
7) No ejecute aplicaciones sin saber qué función realizan en el computador. Si las ejecuta por error **Lea** las ventanas antes de continuar y seleccionar “Aceptar”.
8) Antes de abrir un dispositivo USB verifique que no tenga virus. Tenga en cuenta que el conectar una memoria USB esta se puede reproducir automáticamente, debe cerrar la ventana de reproducción automática y desde la opción Mi PC con clic derecho sobre la unidad de memoria USB debe seleccionar la opción de escanear con antivirus.
9) No generar o enviar correos electrónicos a nombre de otra persona o suplantándola.
10) Cambie constantemente la clave de acceso a internet y/o al correo electrónico.
11) Las aplicaciones tales como: protectores de pantalla, aceleradores de internet, programas para descargar música; normalmente contienen software oculto

(spyware, malware, etc.) Que se instala también en el equipo al momento de instalar la aplicación. Además de no cumplir con los deberes como usuario al instalar este tipo de aplicaciones pone en riesgo la información y la seguridad del equipo.

6.1 Protección en el correo electrónico

El correo electrónico constituye uno de los canales de propagación de virus más utilizados. A continuación, se presenta una serie de medidas preventivas orientadas a aumentar la seguridad durante el uso del correo electrónico.

6.2 Spam

1) El spam es el correo electrónico que promociona diferentes productos y servicios a través de publicidad no solicitada, enviada masivamente a las direcciones de correo de los usuarios.
2) No confiar en correos spam con archivos adjuntos y explorar el archivo antes de ejecutarlo. Estos aseguran que no se ejecutara un malware.
3) Evitar publicar las direcciones de correo en sitios web de dudosa reputación como sitios pornográficos, foros, chats entre otros. Estos minimizan la posibilidad de que la dirección se guarde en la base de datos de los spam.
4) Utilizar filtros anti-spam que permitan el filtrado del correo no deseado.
5) No responder jamás el correo spam. Es preferible ignorarlos y/o borrarlos, ya que si se responde se confirma que la dirección de correo se encuentra activa.
6) Evitar el re-envió de mensajes de cadena ya que suelen ser utilizados para recolectar direcciones de correo activas.
7) Si de todos modos se desea enviar mensajes en cadena, es recomendable hacerlo siempre con copia oculta (CCO) para que quien lo recibe lea solo la dirección del emisor.
8) Proteger la dirección de correo utilizando una cuenta alternativa durante algún proceso de registro en sitios web y similares. Estos previenen que la dirección de correo personal sea foco del spam.
9) Utilizar claves seguras y cambiar la contraseña con periodicidad. Esto favorece la seguridad de la cuenta, evitando que sea descubierta a través de un proceso sencillo.
10) Como medida de seguridad extra, bloquear las imágenes de los correos y descargarlas cuando se asegure de que el correo no es dañino.

11) También es preferible que se evite ingresar el nombre de usuario y su respectiva contraseña en sitios de los cuales no se tenga referencia. De esta manera se preserva la privacidad de la cuenta de correo y, por ende, la información que se intercambia a través de la misma.

6.3 Suplantación de páginas (Phishing)

El Phishing es una modalidad delictiva de estafa realizada a través de internet, y constituye otra de las amenazas de seguridad más propagadas a través del correo electrónico. Entre las buenas prácticas de seguridad recomendadas, están las siguientes:

1) Tener en cuenta que las entidades bancarias y financieras no solicitan datos confidenciales a través de este medio.

2) Desconfiar de los correos que dicen ser emitidos por entidades que brindan servicios y solicitan cambios de datos sensibles ya que suelen ser métodos de ingeniería social.

3) No hacer clic sobre enlaces que aparecen en el cuerpo de los correos electrónicos, ya que pueden re direccionar hacia sitios web clonadas o hacia la descarga de malware.

4) Asegurarse de que la dirección del sitio web la cual se accede comience con el protocolo https. La “s” final, significa que la página web es segura y que toda la información depositada en la misma viajara de manera cifrada.

5) Verificar la existencia de un certificado digital en el sitio web. El certificado digital se despliega en pantalla al hacer clic sobre la imagen del candado.

6) Revisar que el certificado digital no haya caducado, ya que el mismo podría haber sido manipulado intencionalmente con fines maliciosos.

7) Comuníquese telefónicamente con la compañía para descartar la posibilidad de ser víctimas de un engaño, si se tiene dudas sobre la legitimidad de un correo.

8) Jamás se debe enviar contraseñas, números de tarjetas de crédito u otro tipo de información sensible a través del correo electrónico, ya que la comunicación podría ser interceptada y robada.

6.4 Seguridad en la navegación

Es fundamental navegar con cautela y tener presente las siguientes recomendaciones:

1) Evitar el ingreso a sitios web con contenidos que, dependiendo el país, son ilegales, como aquellos que ofrecen cracks y programas gratis; ya que constituyen canales propensos a la propagación de malware.
2) Impedir la ejecución de archivos desde sitios web sin verificar previamente que es lo que dice ser.
3) Es importante no hacer clic sobre el botón ejecutar ya que esto provoca que el archivo se ejecute automáticamente luego de descargado, dejando al margen la posibilidad de verificar su integridad.
4) Descargar programas de seguridad solamente desde el sitio oficial del mismo, para evitar descarga de archivos que pudieran ser previamente manipulados con fines delictivos.
5) Si es posible, leer atentamente las políticas de privacidad de las aplicaciones descargadas desde sitios web no oficiales o de dudosa reputación, antes de instalarlas.
6) No realizar la instalación de complementos extras como barras de tareas o protectores de pantallas sin verificar previamente su autenticidad.
7) Configurar el navegador web para minimizar el riesgo de ataques a través del mismo.
8) El bloqueo de determinados sitios considerados maliciosos, ya sea porque descargan malware o porque contiene material de dudosa reputación, es también otras de las mejores prácticas que ayudan a la prevención y refuerzan la seguridad del equipo.

6.5 Seguridad en redes sociales

En la actualidad, las redes sociales son muy populares y los usuarios las utilizan masivamente; estas características las transforman en importantes focos de propagación de malware. Por tal motivo tener en cuenta y aplicar las siguientes medidas preventivas:

1) No publicar información sensible y confidencial, debido a que personas extrañas pueden aprovechar esta información con fines maliciosos.

2) Evitar la publicación de fotografías propias y de familiares. Las fotografías pueden ser utilizadas para complementar actos delictivos, incluso fuera del ámbito informático.

3) Mantener la privacidad del perfil; es decir, configurar el perfil para que no sea público.

4) No responder las solicitudes de desconocidos, ya que pueden contener códigos maliciosos o que pueden formar parte de actividades delictivas.

5) Ignorar los mensajes que ofrecen material pornográfico, pues usualmente a través de ellos suele canalizarse la propagación de malware, además de otras acciones ofensivas desde el punto de vista ético y moral.

6) No abrir contenidos con spam a través de este medio. De esta manera se evita formar parte del ciclo de vida del spam a través de este canal.

7) Cambiar periódicamente la contraseña para evitar que la misma sea descubierta fácilmente.

8) Antes de aceptar contactos espontáneos, es recomendable verificar su existencia y que realmente proviene de quien dice ser.

6.6 Seguridad en mensajería instantánea

Los clientes de mensajería instantánea constituyen uno de los vehículos más explotados por diferentes amenazas, dentro de las cuales una de las más activas es el malware.

1) Evitar aceptar como contacto de cuentas desconocidas son verificar a quien pertenece.

2) No descargar archivos sospechosos, sobre todo cuando vienen acompañados de mensajes genéricos o en otro idioma.

3) En caso de descargar archivos, explorarlos con un antivirus antes de ser ejecutados.

4) Configurar en el cliente de mensajería la exploración automática de archivos en el momento de su recepción. La mayoría de estos clientes contemplan la posibilidad de configurarlos con un antivirus.

5) Es recomendable, al igual que con el correo electrónico, no hacer clic sobre los enlaces incrustados en el cuerpo del mensaje, ya que pueden direccionar a páginas con contenido malicioso o hacia la descarga de malware.

6) Cuando se reciben mensajes de contenido un enlace no esperado, es recomendable preguntar si la otra persona realmente lo ha enviado; de esta manera se puede verificar la autenticidad del mismo.

7) No escribir los datos de autenticación en páginas que prometen ofrecer información de contactos bloqueados y similares. Estos sitios suelen comprometer la privacidad de la información que se aloja en los correos, además de utilizar la cuenta con otros fines delictivos.

8) No compartir la contraseña con nadie. El carácter de esta es privado.

9) Cuando se accede al mensajero desde lugares públicos, es recomendable deshabilitar la opción de inicio automático para que no puede la dirección (ni la contraseña) grabada. Esto evita que terceros inicie sesión de manera automática.

10) No compartir información confidencial a través de este medio ya que la misma puede ser interceptada y robada con fines delictivos.

6.7 Seguridad en dispositivos removibles

Los dispositivos de almacenamiento removibles que se conectan a través del puerto USB (memorias, cámara digitales, filmadoras, teléfonos celulares, etc.), constituyen otro de los mayores focos de propagación/infección de códigos maliciosos. Por lo tanto, es necesario tener presente explorar con el antivirus para controlar a tiempo una posible infección.

INCLUIR CONTROLES EN ACCESO FISICO

7. MANEJO DE CARPETAS COMPARTIDAS

Debido a la importancia que la información tiene para el desempeño de las actividades de la organización en conjunto con los limitantes de la tecnología actual en cuanto a la capacidad de almacenamiento de archivos, se debe poner en evidencia el tipo de información que la organización debe manejar y almacenar, para lo cual se desarrolla el siguiente reglamento que normaliza estos procedimientos.

7.1. Servicio de sistema de archivos en red

Los Servicios Informáticos proporcionan a la Red de Salud del Norte ESE, un sistema de almacenamiento centralizado de archivos en red, accesible desde cualquier dispositivo conectado a la red.

7.1.1 Tipos de carpetas

7.1.1.1 Carpetas compartidas

Proporcionan un lugar de almacenamiento centralizado de archivos de trabajo que pueden ser accedidos por múltiples usuarios de forma segura. El administrador de la carpeta puede asignar permisos de lectura o lectura/escritura a cada uno de los usuarios del grupo.

7.1.1.2. Carpetas personales

Proporcionan un lugar seguro y accesible para archivos con valor para el usuario, sin el riesgo de pérdida o deterioro por averías en los dispositivos de almacenamiento locales (discos duros).

7.2. Cuotas

Para administrar el espacio de disco disponible y garantizar un acceso equitativo de los recursos informáticos hay establecidos unos límites predeterminados de cuota de almacenamiento por carpeta compartida. Estos límites que pueden ser ampliados bajo petición justificada. 4Gb para carpetas compartidas.

7.3 Control de acceso

El control de acceso se realiza a través de la identidad del usuario en el dominio, usando su cuenta de usuario y su contraseña.

De manera periódica, los usuarios que sean retirados, trasladados o reubicados dentro de la organización, se debe proceder a la cancelación, modificación o ajustes de los permisos o derechos de acceso a la red y a los servicios asignados en el sistema de información, tomando como base los factores de riesgos en la seguridad informática.

El acceso físico a las instalaciones donde se encuentra ubicado el rack principal, solo podrá darse por parte del personal autorizado del área de Sistemas. Si se realiza algún tipo de visita por parte de un externo, se debe contar con

autorización previa del responsable del área y supervisado por un funcionario del área de Sistemas.

El control de acceso a la información a través de una aplicación, se realizará a través de roles que administren los privilegios de los usuarios dentro del sistema de información. El control de acceso a información física o digital, se realizará teniendo en cuenta los niveles de clasificación y el manejo de intercambio de información.

El proceso de Sistemas de Información, identificará según los niveles de clasificación de información cuales sistemas considera sensibles y que deberían gestionarse desde ambientes tecnológicos aislados e independientes. Al aislar estos sistemas se debe prever el intercambio seguro de información, con otras fuentes de datos, ya que no se permite duplicar información en otros sistemas, siguiendo las directrices de fuentes únicas de datos.

7.3.1. Copias de seguridad

La disponibilidad de los datos se garantiza mediante la realización de copias de seguridad periódicas:

- Backup diario de lunes a viernes cada 12 horas.

7.3.2. Política de uso

El almacenamiento centralizado es compartido por todos los usuarios y debe realizarse un uso adecuado y eficiente del mismo.

Los contenidos alojados deberán estar relacionados con las actividades de cada puesto, área o servicio. En particular, no está autorizado el alojamiento de cualquier otro contenido (p.e. música, fotos, películas, etc.) no relacionado con las actividades legítimas de la Red Norte. No está autorizado el almacenamiento de contenidos que puedan violar la Ley de Protección de Datos y/o que vulnere los derechos de Propiedad Intelectual.

Se prohíbe la restricción de permisos sobre el recurso a los administradores de red para garantizar la funcionalidad del servicio. Cualquier modificación de esos permisos, en tanto se detecta, puede resultar en la no realización de copias de seguridad hasta la restauración de los mismos. Por tanto, no se garantiza la

eventual recuperación de la información en caso de modificación de los permisos hasta que no se restauren los mismos y se realice la siguiente copia.

7.4 Carpetas compartidas en Red.

El Proceso de Gestión de Sistemas de información, proporciona distintas carpetas compartidas con distintos niveles de privilegios, según el área o cargo, para colaborar con las diferentes áreas de la Red Norte: carpetas compartidas para un proceso, área o para un servicio. Es importante que el usuario de dicha información se responsabilice de su uso, toda vez que:

- Al compartir una carpeta de un equipo se conseguirá que otros equipos de la red puedan acceder a los archivos presentes en ella.
- Los equipos de la red podrán abrir y guardar en ella archivos y carpetas, como si se tratase de una carpeta del propio disco duro.
- Si varios miembros de la red trabajan con los mismos archivos, se observa que el trabajo en red aporta un aumento de productividad inmediato.
- La carpetas mis documentos y pública, localizadas en cada uno de los equipos de la Red Norte, deben contener archivos relevantes al servicio de la Entidad, es decir archivos Word, Excel, PowerPoint, Outlook, Adobe Acrobat y Winzip de uso oficial para la Organización.
- De existir necesidad de almacenar archivos multimedia, tales como fotografías, archivos de audio o video con información de la Red Norte, deberán ser entregados al Administrador de la red para colocarlos en una carpeta compartida destinada exclusivamente para el almacenamiento de archivos Multimedia.
- Estas carpetas de ninguna manera deben contener archivos de música, fotografías o demás documentos de carácter personal.
- En caso de encontrar en las Carpetas de Mis documentos o las compartidas en el Servidor archivos de esta índole, el administrador de la red puede proceder a su eliminación sin notificación previa si los mismos están poniendo en riesgo la capacidad de almacenamiento de las mismas.

7.5. Uso de equipos de comunicación

Se entiende como equipos de comunicación los dispositivos de cómputo y comunicación móviles y todos aquellos que permitan tener acceso y almacenar información institucional, desde lugares diferentes a las instalaciones. El uso de equipos de cómputo y dispositivos de almacenamiento móviles, está restringido únicamente a los provistos por la institución y deberán contemplar las siguientes directrices:

- Uso de usuario y contraseña para acceso al mismo.
- Cifrado de la información.
- Uso de software antivirus provisto por el Proceso de Gestión de Sistemas de Información.
- Restricción de privilegios administrativos para los usuarios.
- Uso de software licenciado y provisto por el Proceso de Sistemas de Información.
- Realización de copias de seguridad periódicas.
- Uso de mecanismos de seguridad que protejan la información en caso de pérdida o hurto de los dispositivos.
- Permanecer siempre cerca del dispositivo
- No dejar desatendidos los equipos
- No llamar la atención, acerca de portar equipos móviles
- No identificar el dispositivo con distintivos del Proceso de Sistemas de Información
- No colocar datos de contacto técnico en el dispositivo
- Mantener cifrada la información clasificada
- No conectarse a redes WiFi publicas
- Mantener apagado el Bluetooth o cualquier otra tecnología inalámbrica que exista o llegara a existir.

7.6. Trabajo Remoto

El trabajo remoto solo será ejecutado por el proceso de Gestión de Sistemas de Información previa autorización del líder del proceso quien deberá solicitar la actividad e informar el porqué de la solicitud.

7.7 Instalación de un Nuevo Usuario

- Una vez recibida la solicitud para la Creación o modificación de usuarios, se procederá a realizar la actividad con la siguiente Información: Nombre de Usuario, Cuenta, cargo, IPS.
- Se entregará al responsable de la solicitud, las contraseñas de arranque, Nombre de Usuario, contraseña de red, dirección de correo y contraseña de correo de estar disponible al momento de su llegada.
- Se entregará al nuevo usuario las instrucciones que le permitirán acceso a la Intranet.
- Se entregará al nuevo usuario el reglamento de seguridad informática, que incluye las políticas de manejo de documentos y correo electrónico.

7.8. Uso de E-mail y Chat

- Para comprender el manejo de la política de uso de correo y Chat, debe comprenderse que los equipos de cómputo en la ESE Norte son de exclusivo uso institucional.
- Mensajes enviados a grupos usuarios no deben exceder de 2 MB
- El proceso de Gestión de Sistemas de información se responsabiliza de llevar actualizada la lista de usuarios activos, para lo cual cualquier cambio de personal debe comunicarse al encargado de soporte por medio de un mensaje electrónico para revisiones del sistema.
- ***La correspondencia por Email y las conversaciones vía Chat deben considerase un medio oficial de comunicación.*** El lenguaje utilizado en el email o el Chat puede no ser formal, sin embargo debe respetar ciertas reglas de buena conducta interpersonal y ajustarse a las normas generalmente aceptadas.
- Es prohibido utilizar el correo electrónico para enviar contenidos no éticos, ya sea en formato textual o gráfico, implícito o explícito. Está prohibido enviar contenidos de carácter político, contenidos para beneficio personal, para propósitos comerciales o de negocios que no sean del interés de la organización, para trasmitir cadenas y demás comunicaciones de este tipo.

- De acuerdo a lo anteriormente expuesto, la discreción es de gran importancia en el uso de estas o de otras tecnologías para enviar, grabar o intercambiar comunicación.
- El uso aceptable implica que sea legalmente y éticamente permitido, refleje la honestidad y no demuestre despilfarro de recursos compartidos.
- El usuario no debería violar derechos de propiedad intelectual, derechos sobre propiedad de información, mecanismos de seguridad ni tampoco usar correo electrónico para intimidar, cometer abuso, molestar, etc.
- Debe tomarse en cuenta que el correo electrónico y los mensajes escritos en los sistemas de Chat viaja por una cantidad de redes, por lo cual la información que por este transita ***no puede considerarse privada***.
- El email y los programas de Chat pueden ser usados para transmitir mensajes directos o archivos adjuntos, no se puede transmitir ningún archivo tipo: .exe, .pif, .bbs. Documentos Word, Excel, Power Point, PDF, .Zip o documentos audiovisuales son permitidos.
- Está permitido enviar mensajes a todos los destinos de Internet o Grupos, salvo cuando existe una prohibición administrativa explícita hacia ciertas direcciones.
- Se puede recibir mensajes de cualquier origen excepto de Spam, junk mail y mensajes con virus.
- Las políticas de uso de email y chat serán revisadas regularmente con el afán de adaptar los cambios tecnológicos relevantes.

7.9. Gestión de contraseñas

La asignación de contraseñas se deberá controlar a través de un proceso formal de gestión a cargo del Área de soporte. Las recomendaciones son:

a. No escribirlas en papeles de fácil acceso, ni en archivos sin cifrar.
b. No habilitar la opción —recordar clave en este equipo“, que ofrecen los programas
c. No enviarla por correo electrónico
d. Nunca guarde sus contraseñas, en ningún tipo de papel, agenda, etc.

Las contraseñas se deben mantener confidenciales en todo momento.

e. No compartir las contraseñas, con otros usuarios.
f. Cambia tu contraseña si piensas que alguien más la conoce y si ha tratado de dar mal uso de ella.
g. Selecciona contraseñas que no sean fáciles de adivinar.
h. Nunca grabes tu contraseña en una tecla de función o en un comando de caracteres predefinido.
i. Cambia tus contraseñas regularmente.
j. No utilizar la opción de almacenar contraseñas en Internet.
k. No utilizar contraseña con números telefónicos, nombre de familia etc.
l. No utilizar contraseña con variables (soporte1, soporte2, soporte3 etc.)

7.10. Uso de utilitarios del sistema

El uso de utilitarios licenciados del sistema, estará restringido a usuarios administradores. Se establecerá una política a nivel del controlador de dominio, que no permita la instalación de software y cambios de configuración del sistema. Ningún usuario final, deberá tener privilegios de usuario administrador

8. PLAN DE CONTINGENCIA

La seguridad de la infraestructura de Tecnología informática debe además estar respaldada por un plan de contingencia en caso de provocar colapsos extremos en la red de información y que pueden ser anticipados para que nos permitan una recuperación planificada de las operaciones de la Entidad.

- Mantener actualizado las fichas de los equipos, así como su inventario para que permita identificar de manera eficiente el período de garantía del mismo.
- Mantener actualizado el software antivirus y programar revisiones periódicas en el servidor y las estaciones de trabajo.
- Reportar al encargado de sistemas cualquier tipo de irregularidad detectada en el funcionamiento del equipo
- Cumplir con todas las normas estipuladas en este documento.

8.1 Recuperación de información.

- Identificar el problema existente

- Si el problema representa un daño de Hardware, acudir a las fichas de equipo para revisar el estado de su garantía, en caso de encontrarse dentro del período de garantía, acudir al proveedor para hacer válida la misma.
- En caso de que el proceso de garantía tome más de 48 horas y de que el proveedor no cuente con políticas de préstamo o arrendamiento de equipos de similares características y dependiendo de la importancia del hardware dañado, revisar la posibilidad de adquirir un equipo de backup mientras el original regresa de su garantía.
- En caso de que el equipo no se encontrase dentro del período de garantía, proceder a informar a la Subgerencia Administrativa Financiera, para que a la brevedad posible procedan a cumplir el proceso de adquisición del nuevo bien.
- En caso de que se produjere una catástrofe de índole natural o de destrucción masiva de los equipos, se procederá a instalar en una oficina alterna, equipos arrendados y aplicando las políticas de recuperación de archivos y backup se restaurará la información más actual, mientras la oficina y los equipos son devueltos mediante el reclamo a la compañía de seguros respectiva.
- En caso de que el colapso sea de Software, se procederá según las políticas de backup.
- En el proceso de restauración luego de un colapso, se dará importancia al esquema del organigrama de la Red Norte para atender las necesidades de las usuarias.

9. TERMINOLOGÍA

- **Virus informático:** Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

- **Malware**: Es un software que tiene como objetivo infiltrarse en el sistema y dañar la computadora sin el conocimiento de su dueño.

- **Freeware**: Define un tipo de software de computadora que de distribuye sin costo y por tiempo ilimitado, siendo una variante gratuita del shareware, en el que la meta es lograr que un usuario pague, usualmente después de un tiempo de prueba (“trial”) limitado y con la finalidad de habilitar toda la funcionalidad. (Normalmente se consiguen en Internet)

- **Shareware**: Se denomina a shareware a una modalidad de distribución de software, tanto juegos como programas utilitarios, en la que el usuario puede evaluar en forma gratuita el producto, pero con limitaciones en el tiempo de uso o en algunas de la formas de uso o con restricciones en las capacidades finales.(normalmente se consiguen en Internet)

- **Gusano** Informático: Es un malware que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

- **Programa espía**: Spyware, es malware, que se instala en una computadora para recopilar información sobre las actividades realizadas en ella. La función más común que tiene estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas,

- **Keylogger**: Es una herramienta que se encargada de registrar las pulsaciones que se realizan sobre el teclado, para memorizarlas en un fichero y/o enviarlas a través de Internet:
  Suele usarse como malware, permitiendo que otros usuarios tengan acceso a los números de una tarjeta de crédito o a la contraseña de cuentas on line al infiltrarse en un ordenador.

- **Spam**: Se llama Spam, correo basura o SMS basura a los mensajes no son licitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor

- **Focos de propagación**: Los principales focos de propagación de virus son: Internet, correos electrónicos con mensajes adjuntos de cadenas, juegos, videos links a otras páginas, Mensajería instantánea externa, ICQ, Chat externo, redes compartidas Punto a punto (Ares, Kazaa, etc.), Memorias USB infectadas

- **Cookies**: Son archivos en los que almacena información sobre un usuario de internet en su propio ordenador, y se suelen emplear para asignar a los visitantes de un sitio de Internet un número de identificación individual para su reconocimiento subsiguiente.

- **Copyright**: Termino que proviene de la legislación anglosajona y que se refiere a la protección de los derechos económicos que un autor tienes sobre su obra o recreación.

- **Derecho de autor**: Figura legal que reconoce los derechos morales (de divulgación, autoría y modificación) de una obra, además de los derechos económicos de un autor sobre la misma.

- **Derecho de explotación**: Término legal que fija los derechos de reproducción, traducción y distribución de una obra determinada.

- **Entidad de gestión**: Asociación de autores cuya finalidad es la administración de los derechos de autor y otros derechos de propiedad intelectual.

- **Licencia**: Acuerdo mediante el que se otorga al usuario derecho legal para usar un producto y específica cómo puede utilizarlo.

- **Patente**: Título que reconoce el derecho de explotar en exclusiva una invención, impidiendo a otros su fabricación, venta o utilización sin consentimiento del titular.

- **Propiedad Intelectual**: Reconocimiento de los derechos de autoría, propiedad y de explotación de obras artísticas, científicas y software.

10. CONCLUSIÓN

Es importante comprender que los derechos de autor deben ser respetados y para ello se informan los principales deberes para dar cumplimiento a las leyes que los protegen.

Adicionalmente todos los usuarios (sin importar el nivel de conocimiento) tienden a ser dependientes de las tecnologías de información, lo que los expone a las diferentes vulnerabilidades y amenazas informáticas. En consecuencia es sumamente importante incorporar, como habito cotidiano, los deberes y las medidas de seguridad expuestas en este documento.

Elaboró:	Revisó:	Aprobó:
ORIGINAL FIRMADO **MARISOL GOMEZ HURTADO**	ORIGINAL FIRMADO **VIVIANA SOTO OSPINA**	ORIGINAL FIRMADO **MARIA PIEDAD ECHEVERRI CALDERON**
Cargo: Actividad Colectiva Proceso de Gestión de la Información.	**Cargo: Subgerente Administrativa y Financiera**	**Cargo: Gerente**
Fecha: 22-mayo-2019	**Fecha: 22-mayo-2019**	**Fecha: 28-mayo-2019**