POLÍTICAS DE SEGURIDAD INFORMÁTICA
ESE HOSPITAL NAZARETH DE QUINCHIA RISARALDA

ELABORADO POR:
ADMINISTRACION INFORMATICA

MARZO 2021

CONTENIDO:

1. INTRODUCCIÓN

Con la llegada a nuestros países de las tecnologías de la información y las comunicaciones, para la masificación de uso e integración con nuevos procesos y procedimientos complejos, simples, cotidianos, el mundo se ha convertido en una red de personas y entidades que interactúan entre sí, comparten información, generan y almacenan datos, se comunican en tiempo real, realizan transacciones utilizando medios electrónicos. Lo anterior es producto del avance notable del conocimiento y la evolución de la sociedad en sus diferentes instancias.

Con la llegada de estas herramientas tecnológicas a nuestros territorios es innegable la inherente llegada de nuevas amenazas tanto a la privacidad de las personas, como la seguridad de la información y los sistemas implementados, así como las posibilidades de que nuestras entidades puedan ser blanco de ataques que comprometan el correcto funcionamiento de sus procesos, su estabilidad jurídica o incluso la gobernabilidad.

En este sentido, las políticas de seguridad informática definidas en este documento, surgen como una herramienta organizacional para generar conciencia en los funcionarios de la entidad ESE Hospital Nazareth municipio de Quinchía, sobre la importancia y sensibilidad de la información, de servicios que permiten a la entidad mantener su integridad. Ante este hecho, el proponer nuestra política de seguridad requiere un alto compromiso con la empresa social del estado ESE requiera de técnicas para establecer fallas o debilidades en su aplicación, constancia para renovar y actualizar estas

políticas adaptándolas a los diferentes cambios que de manera vertiginosa afectan el mundo de la tecnología.

2. ALCANCE DE LAS POLÍTICAS

En este manual de políticas de seguridad informática, están consignados la gran mayoría de los aspectos a tener en cuenta en la entidad ESE Hospital Nazareth, para prevenir, gestionar y superar, las diferentes situaciones que se pueden presentar, teniendo en cuenta los puntos críticos y las prácticas que pueden ser objeto de aprovechamiento por parte de terceros para la vulneración de los sistemas o ambientes.

Este documento debe ser actualizado de manera periódica, teniendo presente que la capa tecnológica de la sociedad tiene particularidades extremadamente dinámicas y cambiantes. Se debe realizar además la respectiva socialización con todos los funcionarios para que se pueda llevar a cabo la aplicación de la misma.

2. OBJETIVOS

Establecer políticas organizacionales, tendientes a que los funcionarios se adhieran a directrices que permitan un ambiente seguro, en términos de implementación informática y que con cada paso se conviertan las buenas prácticas en seguridad informática en hábitos personales que no solo sirvan en la vida laboral de los funcionarios sino a nivel personal.

Los objetivos que se desean alcanzar luego de socializar el manual de seguridad son los siguientes:

- Funcionarios conscientes de las herramientas tecnológicas disponibles en la entidad y conozcan a cabalidad los riesgos que conlleva para una entidad su implementación.
- Lograr un compromiso desde la alta dirección para establecer mecanismos que permitan un seguimiento y cumplimiento de lo estipulado en este documento.
- Lograr el compromiso desde los funcionarios de la entidad, para que tengan presente que cada uno de ellos es un eslabón de una gran cadena que debe permanecer fuerte ante las amenazas derivadas de la implementación de tecnologías de la información y las comunicaciones
- Que los servicios virtuales y las herramientas generen confianza plena a usuarios internos y externos.

- Tener las herramientas necesarias para actuar en caso de contingencias o situaciones adversas.
- Fomentar el uso responsable de las herramientas que sean proyectadas a la entidad ESE.
- Aprender del día a día y ganar experiencia de cada una de las situaciones que se presenten: mejora continua.

4. ANÁLISIS DE LAS RAZONES QUE IMPIDEN LA APLICACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

a. A pesar de que un gran número de organizaciones canalizan sus esfuerzos para definir directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, muy pocas alcanzan el éxito, ya que la primera barrera que se enfrenta es convencer a los altos directivos de la necesidad y beneficios de buenas políticas de seguridad informática.
b. Otra de las barreras son los tecnicismos informáticos y la falta de una estrategia de marketing por parte de los coordinadores de Informática o los especialistas en la materia, que llevan a los direccionadores a pensar que las inversiones no son necesarias o que podrían suplirse con más trabajo de las personas encargadas de los sistemas. Esta situación generalmente lleva a que las entidades con activos muy importantes, se encuentren expuestas a graves problemas de seguridad y riesgos

innecesarios, que en muchos casos comprometen información sensible y por ende su imagen corporativa e integridad. Ante esta situación, los encargados de la seguridad deben confirmar que las personas entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos

c. Las políticas de seguridad deben ser aceptadas e integradas a las estrategias de la organización, su misión y visión, con el propósito de que quienes toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la empresa.
d. Las políticas por sí solas no constituyen una garantía para la seguridad de la entidad, ellas deben responder a intereses y necesidades de las diferentes dependencias basadas en la visión de su rol social, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la entidad y por ende con la comunidad.

5. RESPONSABILIDADES

Es responsabilidad del coordinador de Seguridad Informática y su equipo de trabajo, desarrollar, someter a revisión y divulgar en adición a los demás medios de difusión (intranet, email, sitio web oficial, medios internos) de los Procedimientos de Seguridad. Así mismo, es responsabilidad del

direccionamiento facilitar el ambiente físico para capacitar a sus funcionarios en lo relacionado con los Procedimientos de Seguridad.

6. DEFINICIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

Las políticas de seguridad informática son un recurso que mitigar los riesgos y generar escudos que permitan reducir las vulnerabilidades que conllevan la implementación de los sistemas informáticos.

7. DISPOSICIONES GENERALES

El presente ordenamiento tiene por objeto estandarizar y contribuir al desarrollo informático de las diferentes áreas de la ESE Hospital Nazareth de Quinchía Risaralda del Municipio de Quinchía. En este sentido se deben crear los siguientes elementos y se describirán y entenderán a lo largo del documento como:

Comité: Es el equipo o grupo de personas integrado por Gerente de la entidad, los jefes de dependencia y el personal involucrado según se disponga en cada uno de las instancias de este organismo, este grupo se define como el direccionador de los siguientes aspectos:

- Adquisición de Hardware y software
- Generación de estándares y políticas nuevas o modificaciones de las existentes según la instancia o la situación actual de la entidad en términos de implementación de sistemas.
- Definición de la estructura tecnológica.

- Definición de directrices que conlleven a un buen desarrollo de todas las actividades
- Definición de las estrategias de seguimiento de los proceso para verificar las prácticas referentes a seguridad informática.
- Definición de los espacios de socialización de las políticas
- Definición de las sanciones o exaltaciones derivadas de la buena o mala adherencia de los funcionarios a la política de seguridad informática.
- Velar por el cumplimiento de las políticas y procedimientos establecidos.

Equipo técnico: Está integrada por los funcionarios encargados del área de sistemas, y se encargará de los siguientes temas:

- Velar por el funcionamiento en tecnologías informáticas que se utilice en las diferentes áreas.
- Elaborar y efectuar seguimiento a las tareas operativas derivadas de la implementación de los sistemas de información
- Definir estrategias y objetivos a corto, mediano y largo plazo
- Mantener la Arquitectura tecnológica
- Controlar la calidad del servicio brindado
- Mantener el Inventario actualizado de los recursos informáticos.

En el contexto de este documento, se entiende por Políticas en Informática, al conjunto de reglas obligatorias, que deben observar los Jefes de Sistemas responsables del hardware y software existente en la ESE Hospital Nazareth de

Quinchía, siendo responsabilidad de la Administración Informática, vigilar su estricta observancia en el ámbito de su competencia, tomando las medidas preventivas y correctivas para que se cumplan.

Las Políticas en Informática son el conjunto de normas locales y lineamientos enmarcados en el ámbito jurídico y administrativo de la ESE Hospital Nazareth. Estas normas inciden directamente en la adquisición, el uso de los bienes y servicios informáticos, las cuales se deberán de acatar invariablemente, por aquellos que intervengan directa y/o indirectamente en la operación o suministro.

La instancia de los sistemas de informática del ESE Hospital Nazareth Quinchía es el despacho del gerente, y el organismo competente para la aplicación de las directrices en el Comité.

Las políticas contenidas en este documento para la adquisición, uso de bienes y servicios informáticos en la entidad ESE Hospital Nazareth, en caso de incumplimiento de la normativa, la responsabilidad recae en el área administrativa.

8. LINEAMIENTOS PARA LA ADQUISICIÓN DE BIENES INFORMÁTICOS

a. Toda adquisición de tecnología informática será verificada a través del Comité, en el cual se deben identificar, presentar las necesidades y definir las acciones respectivas para la adquisición del bien o servicio.

b. La adquisición de Bienes de Informática en la ESE, quedará sujeta a las directrices establecidas en este documento.

c. La Administración de Informática, al planear las operaciones relativas para la adquisición de Bienes informáticos, establecerá prioridades y en su selección deberá tomar en cuenta: estudio técnico, precio, calidad, experiencia, desarrollo tecnológico, estándares y capacidad. A continuación, la explicación más detallada:

Precio: Costo del producto, costo de mantenimiento y consumibles por el período estimado de uso de los equipos.

Calidad: Se refiere a los parámetros cualitativos que especificas las características técnicas de los recursos informáticos y su viabilidad.

Experiencia: Presencia del producto en el mercado nacional y/o internacional, estructura de servicio, la confiabilidad de los bienes y certificados de calidad, si se tienen.

Desarrollo Tecnológico: Se deberá analizar su grado de obsolescencia, su nivel tecnológico con respecto a la oferta existente y su permanencia en el mercado.

Estándares: Los estándares definen las hojas de ruta de las tecnologías y las líneas técnicas generalmente aceptadas a nivel mundial. Toda adquisición se basa en esos estándares; se debe hacer el análisis del cumplimiento de los mismos para garantizar aspectos como la interoperabilidad, compatibilidad, usabilidad, entre otros.

Capacidades: Se deberá analizar si satisface la demanda actual y futura, dependiendo de las características de crecimiento y desarrollo de los aspectos que maneje

d. Para la adquisición de Hardware se observará lo siguiente:

- El equipo o recurso que se desee adquirir, deberá estar dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores del mismo y deberá cumplir con los requerimientos de la alcaldía según la necesidad presentada.
- Los equipos adquiridos deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente disponible preferiblemente de manera local o regional.
- La marca, referencias de los equipos, componentes deberá contar con presencia y permanencia demostrada en el mercado nacional e internacional, así como con asistencia técnica y refaccionaria local. Tratándose de equipos de cómputo, a fin de mantener actualizada la arquitectura informática de la entidad, el Comité emitirá periódicamente las especificaciones técnicas mínimas para la adquisición de equipos conocidos.
- Los dispositivos de almacenamiento, como las interfaces de entrada / salida, deberán estar acordes con la tecnología de punta vigente, tanto en velocidad de transferencia de datos, como en procesamiento.

- Las impresoras deberán apegarse a los estándares de Hardware y Software vigentes en el mercado, corroborando que los suministros (tóner, papel, etc.) se consigan fácilmente en el mercado y no estén sujetas a un solo proveedor.
- En lo que se refiere a los computadores denominados personales, al vencer su garantía por adquisición, deben de contar por lo menos con un programa de servicio de mantenimiento preventivo que incluya el suministro de refacciones.

e. Para la adquisición de equipos de cómputo se deberá incluir el software vigente precargado con su licencia correspondiente, dependiendo del tipo de licenciamiento dispuesto por los fabricantes.

f. Para la adquisición de software base y utilitarios, el Comité dará a conocer periódicamente las tendencias con tecnología de punta vigente. En caos especiales, sólo se adquirirán las últimas versiones liberadas de los productos seleccionados, salvo situaciones específicas que se deberán justificar ante el Comité. Todos los productos de Software que se adquieran deberán contar con su licencia de uso y documentación respectivas

g. Todos los productos de software que se utilicen a partir de la fecha en que entre en vigencia el presente manual de políticas, deberán contar con su licencia de uso respectiva; por lo que se promoverá la regularización o eliminación de los productos ya instalados que no cuenten con el debido licenciamiento.

h. Para la operación del software en la nube o sistemas basados en la interacción por medio de redes, en caso de manejar los datos empresariales mediante sistemas de información, se deberá tener en consideración lo siguiente:

- Debe fomentarse el uso uniforme de la información institucional para proyectar organización y fortalecer la integridad de la información a la hora de realizar consultas o generar reportes que se proyecten a la comunidad o a otros entes.
- El acceso a sistemas de información, deberá contar con capas de privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información institucional. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser manipulado a través de la interfaz gráfica de la aplicación.
- Se deben delimitar las responsabilidades en cuanto al acceso de cada usuario a la información o a los procedimientos establecidos en cada herramienta.
- Los datos de los sistemas de información, deben ser respaldados de acuerdo a la frecuencia de actualización natural de cada herramienta, rotando los dispositivos de respaldo y guardando respaldos históricos. Es indispensable llevar una bitácora de los respaldos realizados, asimismo, los medios de respaldo deberán

guardarse en un lugar de acceso restringido con condiciones ambientales suficientes para garantizar su conservación. En cuanto a la información de los equipos de cómputo personales, se recomienda a los usuarios que realicen sus propios respaldos en la red o en medios de almacenamiento alternos.

- Los sistemas de información, deben contemplar el registro histórico de las transacciones sobre datos relevantes, así como la clave del usuario y fecha en que se realizó.
- Se deben implantar rutinas periódicas de auditoria a la integridad de los datos y de los programas de cómputo, para garantizar su confiabilidad.

i. Para la prestación del servicio de desarrollo o construcción de Software aplicativo se observará lo siguiente: Todo proyecto de contratación de desarrollo o construcción de software requiere de un estudio de factibilidad que permita establecer la rentabilidad del proyecto, así como los beneficios que se obtendrán del mismo.

9. INSTALACIONES DE LOS EQUIPOS DE CÓMPUTO

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 tráfico de personas.
- La coordinación informática, así como las áreas operativas

deberán contar con un croquis actualizado de las instalaciones eléctricas y de comunicaciones del equipo de cómputo en red.

- 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.

La supervisión y control de las instalaciones se llevará a cabo en los plazos y mediante los mecanismos que establezca el Comité.

10. LINEAMIENTOS EN INFORMÁTICA: INFORMACIÓN

a. La información almacenada en medios magnéticos externos se deberá inventariar, anexando la descripción y las especificaciones de la misma, clasificándola según su procedencia y destino. Esto solo cuando no se trata de información referente al programa de gestión documental de la empresa que ya dispone de un tratamiento específico para la misma.

b. Los jefes de área responsables de la información contenida en los equipos a su cargo, delimitarán las responsabilidades de sus subordinados y determinarán quien está autorizado a efectuar

operaciones emergentes con dicha información tomando las medidas de seguridad pertinentes.

c. Los sistemas de información en operación, como los que se desarrollen deberán contar con sus respectivos manuales. Un manual del usuario que describa los procedimientos de operación y el manual técnico que describa su estructura interna, programas, catálogos y archivos.

d. Ningún colaborador en proyectos de software y/o trabajos específicos, deberá poseer, para usos no propios de su responsabilidad, ningún material o información confidencial de la alcaldía.

11. FUNCIONAMIENTO DE LOS EQUIPOS DE CÓMPUTO

a. Es obligación de la Administración de Informática 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.

b. Los colaboradores 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.

c. Por seguridad de los recursos informáticos se deben establecer seguridades:

- Física
- Sistema Operativo
- Software
- Comunicaciones
- Base de Datos
- Proceso
- Aplicaciones

Por ello se establecen los siguientes lineamientos

- Mantener claves de acceso que permitan el uso solamente al personal autorizado para ello.
- Verificar la información que provenga de fuentes externas a fin de corroborar que esté libre de cualquier agente contaminante o perjudicial para el funcionamiento de los equipos.
- Hacer un diagnóstico previo cuando se utilicen medios magnéticos provenientes de entes externos y que puedan contener archivos contaminados por virus informáticos.

12. ACCESO FÍSICO

a. Sólo al personal autorizado le está permitido el acceso a las instalaciones donde se almacenan información sensible o confidencial de la ESE Hospital Nazareth de Quinchía.

b. Sólo bajo la vigilancia de personal autorizado, puede el personal externo entrar en las instalaciones donde se almacena la información confidencial, y durante un período de tiempo justificado.

c. El uso de la red de datos es exclusivo para los equipos de la ESE y debe evitarse la conexión de computadoras personales u otros dispositivos ubicados en los puestos de trabajo para acceso a la red.

d. Se deben reportar las incidencias referentes al punto anterior, es decir cuando se conecte un equipo extraño a las tomas de red.

e. Por ningún motivo se deben manipular los elementos de la red, como switches, routers, cableado, entre otro; esta actividad es exclusiva del equipo técnico.

13. IDENTIFICADORES DE USUARIO Y CONTRASEÑAS

a. 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.

b. 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 y reciba la capacitación adecuada para el manejo de las mismas.

c. 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.

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

14. RESPONSABILIDADES PERSONALES

- 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 o sistema informático afectado.

- 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, u otros elementos que puedan ser objeto de ingeniería social.
- 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.
- 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.
- 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 memorias, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos.

15. SALIDA DE INFORMACIÓN

- 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.
- Además, en la salida de datos especialmente protegidos (como son los datos de carácter personal para los que el Reglamento requiere medidas de seguridad de nivel alto), se deberán cifrar los mismos o utilizar cualquier otro mecanismo que garantice que la información no sea legible ni manipulada durante su transporte.

16. USO APROPIADO DE LOS RECURSOS

Los Recursos Informáticos, Datos, Software, Red Corporativa y Sistemas de Comunicación Electrónica están disponibles exclusivamente para cumplimentar las obligaciones y propósito de la operativa para la que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso.

- El uso de estos recursos para actividades no relacionadas con la misión de la entidad, o bien con la extralimitación en su uso.
- Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Software o de los Estándares de los Recursos Informáticos propios de la ESE Hospital Nazareth.
- Introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.
- Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos.
- El personal de la ESE Hospital Nazareth tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los Sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.

- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.
- Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.
- Borrar cualquiera de los programas instalados legalmente.

17. RECURSOS DE RED

- De forma rigurosa, ninguna persona debe:
  - Conectar a ninguno de los Recursos, ningún tipo de equipo de comunicaciones que posibilite la conexión a la Red Corporativa de la ESE Hospital Nazareth.
  - Conectarse a la Red Corporativa a través de otros medios que no sean los definidos.
  - Intentar obtener otros derechos o accesos distintos a aquellos que les hayan sido asignados.
  - Intentar acceder a áreas restringidas de los Sistemas de Información o de la Red.
  - Intentar distorsionar o falsear los registros “log” de los Sistemas de Información.
  - Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos.

- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros Usuarios, ni dañar o alterar los Recursos Informáticos.

18. CONECTIVIDAD A INTERNET

- La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los colaboradores de ESE Hospital Nazareth de Quinchía tienen las mismas responsabilidades en cuanto al uso de Internet.
- El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad a través del servidor proxy incorporado en la misma. No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso o utilizando un proxy diferente al establecido, o con otras herramientas de Internet
- Internet es una herramienta de trabajo. Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.
- Sólo puede haber transferencia de datos de o a Internet en conexión con actividades propias del trabajo desempeñado.

19.. MANEJO DE CORREOS ELECTRÓNICOS

Los correos electrónicos son actualmente el medio de comunicación por excelencia, habiendo reemplazado en gran medida a otros medios de comunicación de datos como el físico. Pero este uso masivo lo ha convertido también en la herramienta preferida por los atacantes para esparcir códigos dañinos o maliciosos, para el uso del correo se deben tomar en cuenta las siguientes recomendaciones:

- No guardar las credenciales de acceso en el navegador
- Cerrar sesión de forma segura al terminar la jornada o cuando el funcionario se disponga a ausentarse de su puesto de trabajo por lapsos considerables de tiempo.
- Utilizar contraseñas seguras tal y como se estableció anteriormente en este documento.
- Antes de abrir un archivo adjunto, verificar que el correo electrónico provenga de un remitente oficial; esto se puede verificar a través del dominio del remitente, por ejemplo: hospital.quinchia@risaralda.com es diferente a hospital.quinchia@risaralda.gov.co, un ente del estado como la el hospital raramente tendrá un dominio con sufijo .com, en estos casos se debe acudir al departamento de sistemas para verificar técnicamente la procedencia.
- No acceder a enlaces o vínculos contenidos en los mensajes de correo electrónico a menos que se haya comprobado su procedencia.

- No acceder registrarse o darse de alta en sitios que generen mensajes promocionales o correos basura que puedan entorpecer la labor diaria del funcionario.
- Al descargar un archivo al disco local, verificar que su extensión corresponda al formato indicado, por ejemplo; un archivo foto.exe definitivamente es sospechoso y peligroso ya que una foto puede tener extensiones como jpg, png, bmp, pero jamás .exe (archivos ejecutables de Windows)
-

20. ACTUALIZACIONES DE LA POLÍTICA DE SEGURIDAD

Debido a la propia evolución de la tecnología y las amenazas de seguridad, y a las nuevas aportaciones legales en la materia, la alcaldía municipal se reserva el derecho a modificar esta Política cuando sea necesario. Los cambios realizados en esta Política serán divulgados a todos los colaboradores.Es responsabilidad de cada uno de los colaboradores de la ESE Hospital Nazareth de Quinchía, la lectura y conocimiento de la Política de Seguridad más reciente.

El presente documento es una versión preliminar de la política de seguridad informática de la ESE Hospital Nazareth de Quinchía, y está en proceso de revisión para su posterior aprobación e implementación.

Elaborado por:

Administración informática

ESE Hospital Nazareth Quinchía