PLAN ESTRATEGICO DE TECNOLOGIA DE LA INFORMACION Y LAS COMUNICACIONES

SALUD NORTE

Red de Salud del Norte E.S.E.

COPIA

Vigencia 2022

PLAN ESTRATEGICO DE TECNOLOGIA DE LA INFORMACION Y LAS COMUNICACIONES

- PETIC-

COPIA CONTROLADA

GERENTE

ANGIE GUTIERREZ

2022

TABLA DE CONTENIDO

icontec ISO 9001
IQNet
Certificado SC-CER880701

TABLA DE CONTENIDO

1. INTRODUCCION
2. OBJETIVOS
2.1. OBJETIVO GENERAL
2.2. OBJETIVOS ESPECÍFICOS
3. ALCANCE
4. MARCO NORMATIVO
5. DEFINICIONES
6. RUPTURAS ESTRATÉGICAS
7. ANALISIS DE LA SITUACION ACTUAL
7.1. COMPONENTES DE TECNOLOGÍA
7.1.1. INFRAESTRUCTURA TECNOLÓGICA
7.1.2. TOPOLOGÍA DE RED
7.1.3. EQUIPOS DE COMUNICACIÓN
7.1.4. HERRAMIENTAS Y SOFTWARE
8. SERVICIOS DE TECNOLOGIA
8.1. SERVICIOS DE OPERACIÓN
8.2. SERVICIOS DE CORREOS
8.3. ADMINISTRACIÓN DE SERVIDORES
8.4. ANTIVIRUS
8.5. BACKUPS
8.6. TELEFONÍA (IP-CALLCENTER-MÓVILES)
8.7. MANTENIMIENTO, MONITOREO Y SOPORTE OFIMÁTICO
8.8. INTRANET
8.9. GESTIÓN DE USUARIOS, ROLES Y PERFILES.
8.10. ATENCIÓN, ANÁLISIS Y SOLUCIÓN DE SERVICIOS REQUERIDOS DE SOFTWARE Y HARDWARE
9. PLATAFORMA ESTRATÉGICA DE LA RED DE SALUD DEL NORTE
9.1. MODELO DE GESTIÓN
9.1.1. MISIÓN
9.1.2. VISIÓN
9.1.3. POLÍTICA DE CALIDAD
9.1.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
9.2. DEBERES DE LOS USUARIOS DE EQUIPOS DE CÓMPUTO SOBRE EL USO DEL SOFTWARE
9.3. RECOMENDACIÓN SOBRE EL USO DEL SOFTWARE
9.4. Deberes de los Usuarios de Equipos de Cómputo sobre el Uso del Hardware
9.5. Deberes de los Usuarios de Equipos de Cómputo sobre el Uso de la Información
9.6. Buenas Prácticas para la Protección de la Información
9.7. Protección en el correo electrónico
9.8. Spam
9.9. Suplantación de páginas (Phishing)
9.10. Seguridad en la Navegación
9.11. Seguridad en redes sociales

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

9.12. Seguridad en mensajería instantánea 24
9.13. Seguridad en dispositivos removibles 25
9.14. MANEJO DE CARPETAS COMPARTIDAS 25
9.15. Servicio de sistema de archivos en red 26
9.16. Tipos de carpetas 26
9.17. Control de acceso 26
9.18. Copias de seguridad 27
10. POLÍTICA DE USO 27
10.1. Carpetas compartidas en Red. 28
10.2. Uso de equipos de comunicación 28
10.3. Trabajo Remoto 29
10.4. Instalación de un Nuevo Usuario 29
10.5. Uso de E-mail y Chat 29
10.6. Gestión de Contraseñas 30
10.7. Uso de Utilitarios del Sistema 31
11. PLAN DE CONTINGENCIA 31
11.1. Recuperación de información. 31
12. ESTRATEGIA DE TI 32
12.1. Modelo de Operación por Procesos 33
12.2. Misión TI 33
12.3. Visión TI 33
12.4. Actividades 34
12.5. Uso y Apropiación de la Tecnología 34
12.6. Servicios Tecnológicos 35
12.7. Gobierno de TI 35
13. Riesgos 36
13.1. Política de Riesgos Red de Salud del Norte E.S.E 36
13.2. Plan de Tratamiento 36
13.3. Identificación de los Activos de Seguridad de la Información 37
13.4. Valoración del Riesgo 37
13.5. Tabla de Impacto 37
13.6. Responsables 38
13.7. Indicadores 39
14. ESTRUCTURA ORGANIZACIONAL DEL ÁREA DE SISTEMAS 40
15. EVALUACIÓN INTERNA TI 41
15.1. Debilidades 41
15.2. Fortalezas 42
15.3. Estrategia de TI 42
15.4. Plan de Proyectos de TI 43
16. PLAN DE COMUNICACIONES DEL PETI 44

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

1. INTRODUCCION

La RED DE SALUD DEL NORTE E.S.E, con el propósito de mejorar sus servicios de salud, está implementando la plataforma tecnológica para soportar su operación. Sin embargo, los avances en esta materia no se detienen y es fundamental realizar una planeación estratégica de TIC (Tecnología de Información y Comunicaciones) que se alinee a las necesidades de la institución.

El Plan Estratégico de Tecnología de Información y Comunicaciones (PETIC), es un documento muy importante para la organización, mediante el cual se establecen los lineamientos, planes, estrategias y objetivos del área TIC, que permitirá aportar al logro de los objetivos estratégicos institucionales, por lo cual traza un horizonte claro y a enfocar los recursos en el cumplimiento de los objetivos.

La metodología planteada, permite analizar lo que se tiene (Diagnostico), identificar las necesidades de la organización en cuanto a tecnologías de información (orientadas al plan de gestión institucional), priorizarlas y planear su ejecución durante la vigencia del 2021 al 2023.

De igual manera este documento se debe actualizar de forma periódica (anual) y siempre debe estar acorde a los objetivos estratégicos organizacionales.

2. OBJETIVOS

2.1. Objetivo General

El Plan Estratégico de Tecnología de Información y Comunicaciones (PETIC), tiene como objetivo orientar la toma de decisiones institucional para el desarrollo y fortalecimiento de la infraestructura informática, que permita una la interacción fácil, efectiva, oportuna y transparente con nuestros grupos de valor.

2.2. Objetivos Específicos

- Fortalecer los servicios y procesos tecnológicos de la Red De Salud del Norte E.S.E., mediante el uso efectivo de las tecnologías de la información.
- Desarrollar la Arquitectura Empresarial de la Red De Salud del Norte E.S.E bajo los criterios de Gobierno en Línea, transparencia y accesibilidad.
- Mejorar los componentes de seguridad y la protección de los activos de información de la Red De Salud del Norte E.S.E.
- Definir el mapa de ruta del PETI para la Red De Salud del Norte E.S.E.

COPIA CONTROLADA

- Aplicar los lineamientos impartidos para lograr el crecimiento, mantenimiento y fortalecimiento TI de la institución.

- Implementar un gobierno corporativo de las tecnologías de la información y las comunicaciones en la RED DE SALUD DEL NORTE E.S.E, a través del cual se dirige y controla el uso actual y futuro de dichas tecnologías.

- Fortalecer la gestión e interoperabilidad de la RED DE SALUD DEL NORTE E.S.E, en beneficio de sus dependencias y los intereses de la entidad a través de las tecnologías de información y la comunicación.

- Apoyar la toma de decisiones estratégicas y operativas de la RED DE SALUD DEL NORTE E.S.E, basadas siempre en datos e información oportuna, pertinente y de calidad.

3. ALCANCE

Este documento describe las estrategias y proyectos de Tecnologías de Información que propone ejecutar la Red de Salud del Norte E.S.E., a través del proceso de Sistemas e Información durante la vigencia 2021 a 2023, para apoyar el cumplimiento de los objetivos estratégicos y contar con el respaldo de una gestión tecnológica, orientada a la eficiencia, la efectividad y la seguridad, en un marco de aplicación sensible a las necesidades de los usuarios y los colaboradores.

Al desarrollar e implementar el PETI en la entidad, se logrará apropiar y usar eficientemente las tecnologías de información, generando ventajas relacionas con los siguientes aspectos:

- Darle sentido al trabajo que realiza cada uno de los colaboradores, identificando su valor agregado frente a los propósitos la RED DE SALUD DEL NORTE E.S.E

- Integrar los procesos y los procedimientos con los sistemas y tecnologías de la información, garantizando apoyo efectivo para el cumplimiento de los objetivos y desarrollo de actividades establecidas en la E.S.E.

4. MARCO NORMATIVO

- **Ley 527 de 1999:** por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

- **Directiva Presidencial 02 de 2002:** Respeto al derecho de autor y los derechos conexos, en lo referente a utilización de programas de ordenador (software).

- **Ley 872 de 2003:** Con esta Ley se ordena la creación del Sistema de Gestión de Calidad (SGC) en las instituciones del Estado, como una herramienta para la gestión sistemática y transparente, que permita dirigir y evaluar el desempeño institucional en términos de calidad y satisfacción social con la prestación de los servicios, enmarcada en los planes estratégicos y de desarrollo que el sector Estatal debe cumplir para ejercer su función social.

- **Decreto 1011 de 2006:** Por el cual se establece el Sistema Obligatorio de Garantía de Calidad de la Atención de Salud del Sistema General de Seguridad Social en Salud.

- **Resolución 1445 De 2006:** El cumplimiento del Sistema Único de Acreditación es voluntario para las IPS de naturaleza privada. Para las IPS de naturaleza pública, entre estos las Empresas Sociales del Estado (E.S.E.).

- **Decreto Nacional 1151 del 14 de abril de 2008 y Manual para la implementación de la Estrategia de Gobierno en Línea de la República de Colombia:** Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.

- **Resolución 185 del 6 de junio de 2007:** Políticas de Conectividad para las Entidades del estado.

- **Ley 1266 de 2007:** por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.

- **Ley 1273 de 2009:** "Delitos Informáticos" protección de la información y los datos.

- **Ley 1341 de 2009**: en el Parágrafo de su artículo 38 establece que: “Las autoridades territoriales implementarán los mecanismos a su alcance para gestionar recursos a nivel nacional e internacional, para apoyar la masificación de las TIC, en sus respectivas jurisdicciones”.

- **Ley 1474 de 2011:** Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública, hace referencia al uso obligatorio de los sitios web de las entidades públicas como mecanismo para la divulgación de información pública.

- **Artículo 232 de la Ley 1450 de 2011:** prevé, sobre la Racionalización de trámites y procedimientos al interior de las entidades públicas. Que: los organismos y entidades de la Rama Ejecutiva del Orden Nacional y Territorial procederán a identificar, racionalizar y simplificar los procesos, procedimientos, trámites y servicios internos, con el propósito de eliminar duplicidad de funciones y barreras que impidan la oportuna, eficiente y eficaz prestación del servicio en la gestión de las organizaciones.

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

- **Ley 1581 de 2012:** "Protección de Datos personales".
- **Decreto 2609 de 2012:** por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011
- **Decreto 1377 de 2013:** por la cual se reglamenta la ley 1581 de 2012
- **Ley 1712 de 2014:** "De transparencia y del derecho de acceso a la información pública nacional"
- **Ley 1753 de 2015:** Por la cual se expide el Plan Nacional de Desarrollo 2014- 2018 "Todos por un nuevo país" en el artículo 45 establece:" Estándares, modelos y lineamientos de tecnologías de la información y las comunicaciones para los servicios al ciudadano"
- **Decreto N°415 de 7 de marzo 2016**: en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones
- **Decreto 1008 Del 14 De junio De 2018:** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
- **CONPES - Política Nacional de Seguridad Digital:** se tiene como objetivo: "Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país".
- **Resolución N° 0002405 de 25 de noviembre de 2016:** por el cual se adopta el sello de la excelencia Gobierno en Línea y se conforma su comité.
- **Decreto 3816 de 2003**: "Por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública".
- **Resolución N° 0002710 del 3 de octubre de 2017:** "Por la cual se establecen lineamientos para la adopción del protocolo IPv6"
- **Decreto 1499 de 2017:** se modifica el decreto 1083 de 2015 y se definen los lineamientos del modelo integral de planeación y gestión para el desarrollo administrativo y la gestión de la calidad para la gestión pública.
- **NTC-ISO/IEC 27002:** Establece las mejores prácticas para la implementación del Sistema de Gestión de Seguridad de la Información.
- **NTC-ISO/IEC 27001:** Señala los requerimientos del Sistema de Gestión de Seguridad de la Información.

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

5. DEFINICIONES

- **Presupuesto:** conjunto de los gastos e ingresos previstos para un determinado período de tiempo. Cálculo anticipado del coste de una obra o un servicio.
- **PETIC:** Plan Estratégico de Tecnologías de la Información y las Comunicaciones.
- **TIC:** Tecnologías de la Información y las Comunicaciones.
- **Activos De Información:** cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la institución y, en consecuencia, debe ser protegido.
- **Autenticación:** Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
- **Confiabilidad**: Aseguramiento de que la información es accedida solo para quienes es tan autorizados.
- **Información:** conjunto de datos organizados y procesados que constituyen mensajes, instrucciones, operaciones, funciones y cualquier tipo de actividad que tenga lugar en relación con un ordenador.
- **Perfiles de usuario:** conjunto de usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.
- **Política:** Son instrucciones mandatarias que indican la intención de la alta gerencia respecto a la operación de la organización.
- **Responsable por el activo de información:** Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.
- **Virus:** Es un programa informático que al ser ejecutado puede llegar a alterar el normal funcionamiento de un equipo de cómputo, sin el permiso o el conocimiento del usuario
- **Kaspersky:** Antivirus, software de seguridad y protección.
- **Riesgo:** Es la probabilidad de que una amenaza se convierta en un desastre.
- **MINTIC**: Ministerio de Tecnología de Información y de las Comunicaciones

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

- **Recursos tecnológicos:** son componentes de hardware y software tales como: servidores, estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas y asistenciales necesarias para el buen funcionamiento y la optimización del trabajo al interior de la institución.
- **Gestión tecnológica:** Es un sistema de conocimientos y prácticas relacionados con los procesos de creación, desarrollo, transferencia y uso de la tecnología.
- **Sistema de información hospitalario:** Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. es todo componente de software adquirido por la E.S.E Hospital el salvador de Ubaté como un producto desarrollado para las necesidades de ésta.
- **Seguridad de la información:** es la preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Terceros:** Todas las personas jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la institución.
- **Usuarios del Sistema:** persona que se conecta al sistema para hacer uso de los servicios que este les proporciona.
- **Copia de seguridad o Backup:** Copia de los datos originales alojados en cualquier medio de almacenamiento que se realiza con el fin de disponer de una manera de recuperarlos en caso de su pérdida.
- **Centro de Cómputo:** Es el lugar dentro de la entidad que se encarga del procesamiento de datos e información de forma sistematizada, por medio de la utilización de ordenadores que están equipados con el hardware y el software necesarios para cumplir con dicha tarea.

COPIA CONTROLADA

6. RUPTURAS ESTRATÉGICAS

A continuación, identificamos los paradigmas que se deben de intervenir para lograr que el resultado de estas estrategias impacte en el logro de los objetivos estratégicos, la misión y visión de la Red de Salud del Norte E.S.E.:

- Fortalecer al personal de apoyo e incentivar al uso y apropiación de TIC.

icontec ISO 9001
IQNet
Certificado SC-CER880701

- Las inversiones en los proyectos de las TIC son vistas como de alto costo y no es claro el retorno de su inversión.

Todo proyecto relacionado con el uso de tecnología estará acompañado por parte del Grupo Funcional de Apoyo Tecnológico desde su conceptualización hasta su implementación, seguimiento y evaluación

7. ANALISIS DE LA SITUACION ACTUAL

El área de Sistemas de Información y comunicaciones es el área responsable de brindar las herramientas tecnológicas (Infraestructura – Sistemas de Información, comunicación y Soporte) a nivel transversal, para que la Entidad a través de sus dependencias, cumpla con las metas propuestas.

Actualmente se deben generar estrategias de mejoramiento a nivel tecnológico, se deben gestionar herramientas que coadyuven a mantener la integridad de la información, optimización de los recursos tecnológicos, proyección y búsqueda de las herramientas tecnológicas que faciliten procesos o actividades, mejoren el servicio de cara al ciudadano y aseguramiento y protección de la información a todo nivel.

7.1. Componentes de Tecnología

Los recursos tecnológicos de la Red de Salud de Norte nos permiten recopilar y administrar los activos intangibles de la empresa, como bases de datos e información. Los recursos tecnológicos además permiten tener efectividad en el manejo de esta.

7.1.1. Infraestructura Tecnológica

El parque tecnológico de la E.S.E. Norte está compuesta por:

- 7 servidores de archivos central
- 423 equipos de cómputo, 260 propios y 163 en alquiler
- 60 impresoras, 7 Propias y 53 en alquiler
- Sistemas de monitoreo compuesto por 100 cámaras

Equipos de usuario final: Computadores de Escritorio y Computadores Portátiles: Los dos modelos de computadores de escritorio que se utilizan en la institución, tanto físicamente en las tarjetas de red, como lógicamente en los sistemas operativos la funcionalidad de IPv6 es soportada y adquirir

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

direcciones IPv6 o IPv4 es transparente sin necesidad de requerir software y hardware adicional.

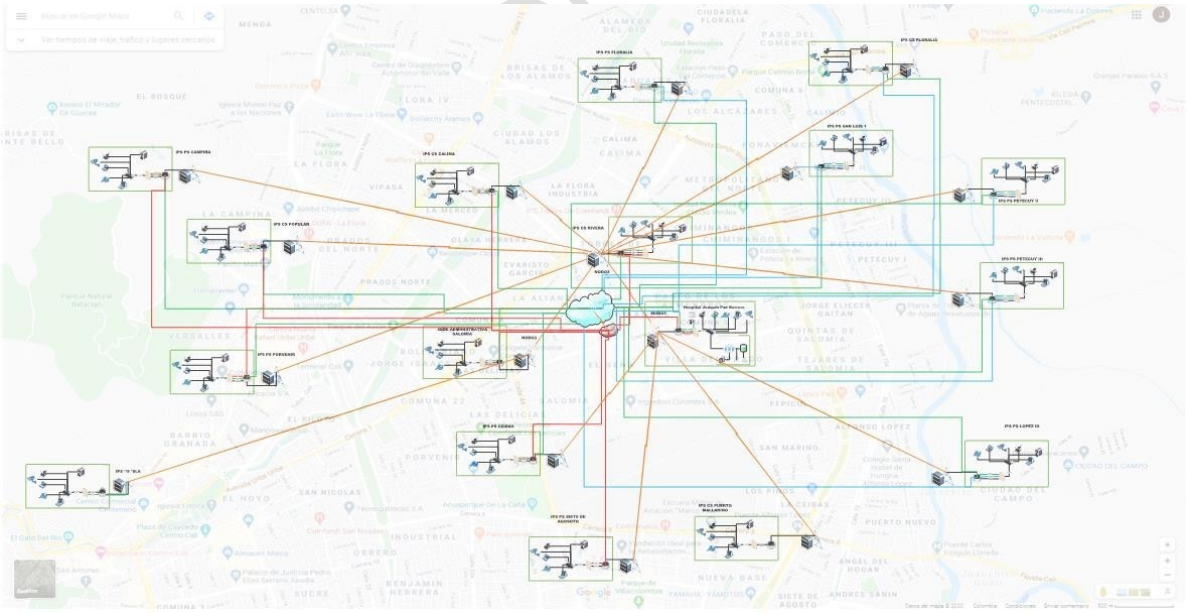
Impresoras: Los modelos de impresoras que actualmente se tienen en la institución soportan IPv6, algunas estas por conexión local o compartida.

7.1.2. Topología de Red

Por medio de protocolos de conexión MPLS, uso de banda ancha y antenas inalámbricas logramos intercomunicar las 17 IPS mediante red local, centralizando la información y controlando de forma remota desde cualquier lugar los componentes de cómputo y de red, permitiendo así asegurar la disponibilidad e integridad de la información.

7.1.3. Equipos de Comunicación

Switch: no requieren migrarse ni física ni lógicamente, los parámetros de enrutamiento se administrarán directamente desde el Router HP implementado, y este asumiendo el rol de las políticas de enrutamiento IPv4 e IPv6 y las características de tunneling si así se requirieran.



Actualmente se cuenta con una conexión de INTERNET así:

- Paquete Hosting 200 MB

CONTROLADA
icontec ISO 9001
IQNet
Certificado SC-CER880701

- Internet dedicado de 200 Mb y contingencias banda ancha de 500 y 50 Mb
- Canales MPLS de 40, 70, 150 Mb
- Contingencia con nodos de antenas inalámbricas.

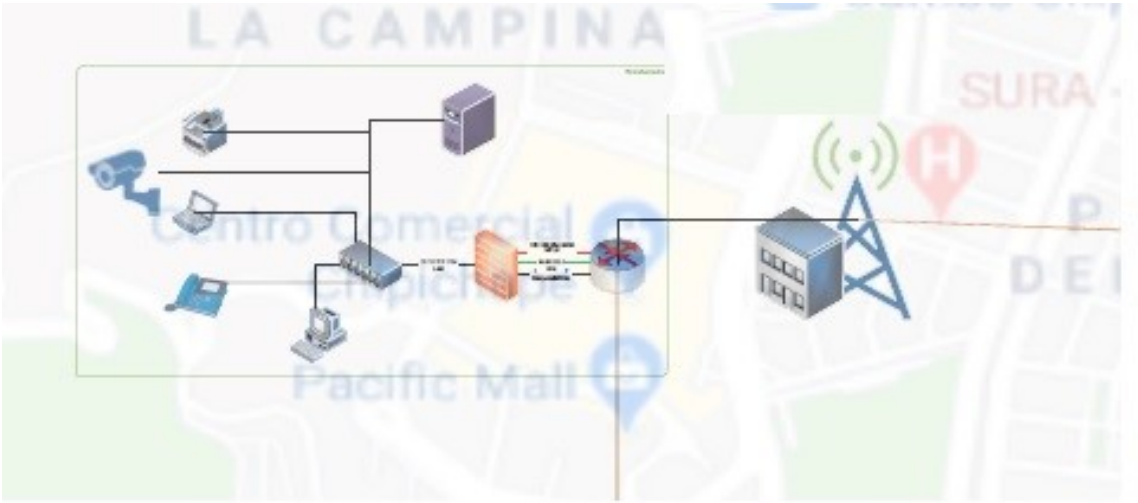


Diagrama de Red

7.1.4. Herramientas y Software

Para apoyar los procesos misionales y de apoyo en la organización, es importante contar con sistemas de información que se conviertan en fuente única de datos útiles para la toma de decisiones en todos los aspectos; que garanticen la calidad de la información, dispongan recursos de consulta a los públicos de interés, permitan la generación de transacciones desde los procesos que generan la información siendo fáciles de mantener.

A continuación, se describe la situación actual de los sistemas de información:

NOMBRE DEL SISTEMA DE INFORMACION	BREVE DESCRIPCION DE LA ACCION QUE REALIZA
Rfast 8	Sistema de información administrativa, financiera y asistencial

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

NOMBRE DEL SISTEMA DE INFORMACION	BREVE DESCRIPCION DE LA ACCION QUE REALIZA
SQL Server 2012 Standard	Base de datos principal
Spark	Herramienta de Chat corporativo, usado para comunicar y medio de difusión institucional.
ISSABEL	Controlador de telefonía IP, configuración de PBX, troncales y canales.
INTRANET (Intranorte)	Red informática interna, con estándares, que permite a toda la red de equipos de la ESE estar conectada a uno o varios servidores, para acceder de forma estructurada a la información
Suite Tecnológica	Plataforma donde registramos Ticket o casos de mantenimiento, Gestión de PQRS, Registro de eventos Adversos, incidentes o atención insegura, Indicadores
REPORTING	Plataforma para la generación de informes personalizados por rangos de fecha
RIAS	Plataforma misional que permite la recopilación de los datos resolución RIAS 3280
Página Web	Portal https://esenorte.gov.co/ Información Institucional, Portafolio de Servicios, Transparencia e información Pública, Atención al ciudadano, Agendamiento de Citas y Noticias de interés
Correos Electrónicos	Contamos con Hosting, alojamiento Web y administrador de correos corporativos
Hospitium	Reportadores para servicios hospitalarios de Triage, Laboratorio y Vacunas.
Kaspersky Security Center	Consola de administración corporativa de antivirus. Nos permite hacer inventario de equipos, directivas,

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

NOMBRE DEL SISTEMA DE INFORMACION	BREVE DESCRIPCION DE LA ACCION QUE REALIZA
	tareas, informes, creación de grupos, bloques, permisos y excepciones
Agendamiento de citas WEB	Solicitud de citas para usuarios, a través de la página WEB de acuerdo a disponibilidad de agendas.

8. SERVICIOS DE TECNOLOGIA

8.1. Servicios de Operación

Actualmente el área de Sistemas de Información y Comunicación de la entidad se encuentra en un estado maduro, con procedimientos sólidos y con contrataciones definidas, tanto de productos y servicios, como en general de la gestión de la infraestructura tecnológica.

Actualmente el soporte y mantenimiento preventivo y correctivo se realiza de manera directa por el área.

8.2. Servicios de Correos

Este servicio se presta a todos los usuarios de la Empresa tanto Asistenciales como administrativos, es un servicio que optimiza la operación diaria y comunicación externa e interna de los usuarios.

8.3. Administración de Servidores

La administración de Servidores se encarga de asegurar y garantizar el tiempo de actividad, rendimiento, uso de recursos y la seguridad de los servicios instalados en cada uno de ellos, administrando de forma dinámica y con oportunos tiempos de respuesta con el fin de dar continuidad ininterrumpida al negocio y la prestación de los servicios de salud.

8.4. Antivirus

La plataforma de antivirus ofrece protección a los equipos de la RED DE SALUD DEL NORTE E.S.E., brindando seguridad y pocos recursos del sistema. Esta plataforma ofrece los siguientes beneficios:

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

- Protección exhaustiva para todos los dispositivos frente al malware
- Soporte para nuevas tecnologías
- Suministro de protección ante criminales informáticos.
- Control para limitar el acceso a los sitios Web maliciosos.
- Protección frente robos de identidad y suplantaciones
- Ayuda a mantener el rendimiento de tu PC y minimizar las vulnerabilidades

8.5. Backups

El procedimiento de backups ofrece protección de datos completa a las carpetas protegidas de forma periódica para lavase de datos, garantizando las copias de seguridad y la recuperación simple y fiable. Brindando alta disponibilidad de la información almacenada en las carpetas compartidas del Servidor de Archivos cuando sea requerida con periodos reescribibles.

8.6. Telefonía (Ip-Callcenter-Móviles)

La administración de la plataforma de telefónica, se encarga de dar soluciones integrales a los usuarios de la RED DE SALUD DEL NORTE E.S.E, donde se gestionan y administran servicios como Telefonía IP, extensiones, Call Center gestionable, Móviles y mensajes autorespuesta.

8.7. Mantenimiento, Monitoreo y Soporte Ofimático

El servicio de mantenimiento preventivos prevenimos la generación de incidencias con respecto a los soportes de atención, minimizando el número de casos o tickets de atención software/hardware. Estas actividades de prevención y diagnóstico de fallas son programadas y se realizan de forma periódica. Gestionando el soporte y mantenimiento del Software y Hardware autorizado, así como el suministro, instalación, configuración y puesta en marcha de herramientas de monitoreo que determinen en línea el estado de disponibilidad de los algunos procesos y servicios.

8.8. Intranet

Grupo de herramientas de software y aplicaciones que permiten la comunicación y transferencia de la información de forma digital entre todos los procesos de la Red de Salud del Norte, dentro de ellas tenemos, Archiweb de repositorios, Suite, Suite Learnig, Reporting y Rias.

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

8.9. Gestión de Usuarios, Roles y Perfiles.

Este procedimiento es realizado conjuntamente con el área de gestión humana y los lideres de cada proceso de la RED DE SALUDL DEL NORTE E.S.E., toda la administración de cuentas de usuarios de las aplicaciones internas y sistemas de información, así como la asignación de recursos (roles y perfiles) y seguridad en los accesos a la red son definidos y restringidos de acuerdo a las políticas de seguridad y a los niveles de responsabilidad de cada colaborador.

8.10. Atención, Análisis y Solución de Servicios Requeridos de Software y Hardware

Por medio de la Suite Tecnológica atendemos a los tickets de soporte, en donde el principal objetivo es recibir y dar solución a los requerimientos y/o incidencias aplicables a la infraestructura de TICS, Sistemas de Información y/o Aplicaciones corporativas, resolviéndolas de manera oportuna y eficientes, y en los tiempos establecidos con el fin de garantizar condiciones óptimas para la prestación de servicios ofrecidos por la RED DE SALUD DEL NORTE E.S.E.

9. PLATAFORMA ESTRATÉGICA DE LA RED DE SALUD DEL NORTE

La RED DE SALUD DEL NORTE E.S.E está ubicada en el norte y nororiente de Santiago de Cali. Esta se constituyó como resultado del proceso de descentralización de servicios de la Secretaría de Salud Pública Municipal bajo el Acuerdo 106 del 29 diciembre 2003.

Las Empresas Sociales del Estado, E.S.E. de Santiago de Cali, son entidades públicas, descentralizadas, del orden municipal, con personería jurídica, autonomía administrativa y patrimonio independiente, adscritas a la Secretaría de Salud Pública Municipal y sometidas al régimen jurídico previsto en la Ley.

El objeto de las Empresas Sociales del Estado, es la prestación de servicios de salud, como un servicio público de seguridad social, que contribuya al mejoramiento del estado de salud de la población en sus áreas de influencia; con capacidad para ofrecer servicios de promoción, prevención, diagnóstico, tratamiento y rehabilitación acorde con las necesidades determinadas en el perfil epidemiológico y con sujeción al Plan Sectorial de Salud, al Plan de Desarrollo Municipal y a los criterios operacionales señalados para el funcionamiento de la red de servicios del Departamento del Valle del Cauca, sin perjuicio de que pueda prestar otros servicios de salud que no afecten su objeto social y que contribuyan a su desarrollo y financiación.

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

Se cuenta con una red de 17 IPS de baja complejidad habilitadas para prestar los servicios de:

Hospital Joaquín Paz Borrero, prestación de servicios de salud de mediana y baja complejidad en: Consulta Médica General, Consulta de Enfermería, Promoción y Prevención, Odontología, Urgencias, Hospitalización, Obstetricia (partos), Terapia Física y Respiratoria, Optometría, Psicología, Laboratorio Clínico, Imágenes Diagnósticas, Esterilización, Consulta Médica Especializada en Ginecoobstetricia, Ortopedia y/o Traumatología, Oftalmología, Otorrinolaringología, Dermatología, Ortodoncia, Rehabilitación Oral, Salud Ocupacional y Medicina Alternativa; Cirugía en: Ginecología, Ortopedia, Oftalmología y Otorrinolaringología.

IPS´s Puerto Mallarino, La Rivera, Popular, Floralia y San Luis II prestación de servicios de salud de baja complejidad en: Consulta Médica General, Consulta por Enfermería, Promoción y Prevención, Odontología, Terapia Física, Optometría, Psicología, Toma de muestras de Laboratorio Clínico, Imágenes Diagnósticas.

IPS´s La Campiña, Porvenir, Alfonso López, Siete de Agosto, Las Ceibas, Petecuy II, Petecuy III, Floralia, Isla, San Luis I, Calima prestación de servicios de salud de baja complejidad en: Consulta Médica General, Consulta por Enfermería, Promoción y Prevención, Odontología, Optometría, Psicología, Toma de muestras de Laboratorio Clínico, Imágenes Diagnosticas.

9.1. Modelo De Gestión

9.1.1. Misión

Preservar y recuperar la salud de nuestros usuarios, mediante un modelo de salud integral, centrada en las personas, con atención humanizada, que integra la práctica formativa, la relación docencia servicio y la investigación en salud para lograr altos estándares de calidad.

9.1.2. Visión

Ser una institución prestadora de Servicios de Salud, líder en la detección temprana y tratamiento de Cáncer de mama, y reconocida como una institución confiable, con servicios humanizados y acreditada en salud.

9.1.3. Política de Calidad

En la Red de Salud del Norte E.S.E. Nos comprometemos a prestar servicios de salud de baja complejidad y complementarios con altos estándares de calidad, que garanticen la accesibilidad, la continuidad, la seguridad, la oportunidad y la pertinencia en la prestación de los servicios, sobre la base de un trato humanizado.

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

9.1.4. Política de Seguridad de la Información

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.

9.2. 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:

- 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.

- Todos los equipos se entregan únicamente con la licencia del sistema operativo y la licencia de acceso al aplicativo de operaciones diarias (sistema

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

de facturación, sistema contable, etc.)

- Las licencias de software ofimática tales como Microsoft office serán instaladas únicamente en los equipos autorizados por la gerencia.
- El acceso a internet debe ser realizado de forma responsable y segura; siendo usado únicamente para actividades de índole laboral.
- Los usuarios deben dar buen uso del correo corporativo. Evitar el envío de mensajes con archivos adjuntos tales como cadenas, videos, música, presentaciones, etc.
- 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.
- No está permitido el uso de redes punto a punto o la instalación de software para tal fin.
- 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.

9.3. Recomendación Sobre el Uso del Software

- El personal del Proceso de Sistemas de Información puede revisar, reinstalar o desinstalar 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.
- 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.
- 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.

9.4. Deberes de los Usuarios de Equipos de Cómputo sobre el Uso del Hardware

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

- 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.
- No se debe abrir ninguno de los equipos ni manipular los componentes electrónicos y/o mecánicos que los componen.
- No se deben trasladar componentes entre equipos, ni realizar prestamos entre sedes sin previa autorización.
- No debe consumir alimentos o bebidas en el sitio de trabajo, en el cual se

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

encuentran instalados los equipos de cómputo.
- Debe dar buen trato a los elementos de cómputo, evitando golpearlos o ensuciarlos.

9.5. Deberes de los Usuarios de Equipos de Cómputo sobre el Uso de la Información

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

- 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.
- No debe enviar correos personales masivos.

9.6. Buenas Prácticas para la Protección de la Información

Recomendaciones generales sobre el uso del Software:

- 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.
- Al navegar en internet, no navegar en sitios desconocidos ya que estos sitios normalmente instalan software no autorizado por el usuario.
- 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.
- Lea las ventanas de mensajes que el computador informa antes de presionar cualquier botón de “Aceptar”.
- No envié cadenas o mensajes ya que puede congestionar la red.
- No abra carpetas desconocidas que provienen de memorias USB.
- 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”.
- 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.
- No generar o enviar correos electrónicos a nombre de otra persona o suplantándola.

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

- Cambie constantemente la clave de acceso a internet y/o al correo electrónico.
- 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.

9.7. 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.

9.8. Spam

- 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.
- No confiar en correos spam con archivos adjuntos y explorar el archivo antes de ejecutarlo. Estos aseguran que no se ejecutara un malware.
- 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 spams.
- Utilizar filtros antispam que permitan el filtrado del correo no deseado.
- 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.
- Evitar el reenvió de mensajes de cadena ya que suelen ser utilizados para recolectar direcciones de correo activas.
- 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.
- 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.
- 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.
- Como medida de seguridad extra, bloquear las imágenes de los correos y descargarlas cuando se asegure de que el correo no es dañino.
- 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 esta.

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

9.9. 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:

- Tener en cuenta que las entidades bancarias y financieras no solicitan datos confidenciales a través de este medio.
- 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.
- 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.
- 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.
- 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.
- Revisar que el certificado digital no haya caducado, ya que el mismo podría haber sido manipulado intencionalmente con fines maliciosos.
- 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.
- 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.

9.10. Seguridad en la Navegación

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

- 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.
- Impedir la ejecución de archivos desde sitios web sin verificar previamente que es lo que dice ser.
- 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.
- Descargar programas de seguridad solamente desde el sitio oficial del mismo, para evitar descarga de archivos que pudieran ser previamente

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

manipulados con fines delictivos.

- 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.
- No realizar la instalación de complementos extras como barras de tareas o protectores de pantallas sin verificar previamente su autenticidad.
- Configurar el navegador web para minimizar el riesgo de ataques a través del mismo.
- 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.

9.11. 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:

- No publicar información sensible y confidencial, debido a que personas extrañas pueden aprovechar esta información con fines maliciosos.
- Evitar la publicación de fotografías propias y de familiares. Las fotografías pueden ser utilizadas para complementar actos delictivos, incluso fuera del ámbito informático.
- Mantener la privacidad del perfil; es decir, configurar el perfil para que no sea público.
- No responder las solicitudes de desconocidos, ya que pueden contener códigos maliciosos o que pueden formar parte de actividades delictivas.
- 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.
- 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.
- Cambiar periódicamente la contraseña para evitar que la misma sea descubierta fácilmente.
- Antes de aceptar contactos espontáneos, es recomendable verificar su existencia y que realmente proviene de quien dice ser.

9.12. 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.
- Evitar aceptar como contacto de cuentas desconocidas son verificar a quien

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

pertenece.

- No descargar archivos sospechosos, sobre todo cuando vienen acompañados de mensajes genéricos o en otro idioma.
- En caso de descargar archivos, explorarlos con un antivirus antes de ser ejecutados.
- Configurar en el cliente de mensajería la exploración automática de archivos en el momento de su recepción n. La mayoría de estos clientes contemplan la posibilidad de configurarlos con un antivirus.
- 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.
- 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.
- 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.
- No compartir la contraseña con nadie. El carácter de esta es privado.
- Cuando se accede al mensajero desde lugares públicos, es recomendable deshabilitar la opción de inicio automático para que no pueda la dirección (ni la contraseña) grabada. Esto evita que terceros inicie sesión de manera automática.
- No compartir información confidencial a través de este medio ya que la misma puede ser interceptada y robada con fines delictivos.

9.13. Seguridad en dispositivos removibles

Los dispositivos de almacenamiento removibles que se conectan a través del puerto USB (memorias, cámaras 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.

COPIA CONTROLADA

9.14. 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

icontec ISO 9001
IQNet
Certificado SC-CER880701

almacenar, para lo cual se desarrolla el siguiente reglamento que normaliza estos procedimientos.

9.15. 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.

9.16. Tipos de carpetas

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.

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).

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.

9.17. 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 deben 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

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

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.

9.18. 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.

10. 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.

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

10.1. 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.
- Las 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.

10.2. 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.

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

- 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.

10.3. 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.

10.4. 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.

10.5. 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.

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

- 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.

10.6. 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:

- No escribirlas en papeles de fácil acceso, ni en archivos sin cifrar.
- No habilitar la opción “recordar clave en este equipo “, que ofrecen los programas.
- No enviarla por correo electrónico
- Nunca guarde sus contraseñas, en ningún tipo de papel, agenda, etc.
- Las contraseñas se deben mantener confidenciales en todo momento.
- No compartir las contraseñas, con otros usuarios.
- Cambia tu contraseña si piensas que alguien más la conoce y si ha tratado de dar mal uso de ella.

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

- Selecciona contraseñas que no sean fáciles de adivinar.
- Nunca grabes tu contraseña en una tecla de función o en un comando de caracteres predefinido.
- Cambia tus contraseñas regularmente.
- No utilizar la opción de almacenar contraseñas en Internet.
- No utilizar contraseña con números telefónicos, nombre de familia etc.
- No utilizar contraseña con variables (soporte1, soporte2, soporte3 etc.)

10.7. 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

11. 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.

11.1. 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

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

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.

COPIA CONTROLADA

12. ESTRATEGIA DE TI

El plan estratégico propone los objetivos y las estrategias que se trabajan en la RED DE SALUD DEL NORTE E.S.E, y su área de influencia durante 4 años, los cuales se desagregan en planes de desarrollo. Cada uno tiene evaluaciones anuales por medio de planes de acción, los cuales permiten controlar y evaluar los logros para todo el periodo.

El plan compromete a todas las partes interesadas (funcionarios, entes de control, usuarios, comunidad, entre otros) en su ejecución, seguimiento y control, mediante la aplicación de la misión hasta la consecución de la visión, desarrollando las acciones y proyectos para el logro de los objetivos corporativos.

icontec ISO 9001
IQNet
Certificado SC-CER880701

El mapa de procesos describe y categoriza las actividades de la RED DE SALUD DEL NORTE E.S.E, para llegar a la satisfacción del usuario, partiendo de sus requisitos y expectativas.

Se muestran todos los procesos de la RED DE SALUD DEL NORTE E.S.E, los cuales están categorizados en procesos estratégicos, misionales, de apoyo, y de evaluación y control; cada uno con sus diferentes niveles, establecidos en macroprocesos y procesos.

12.1. Modelo de Operación por Procesos



Para el proceso de Sistemas e Información, desarrollamos los siguientes conceptos estratégicos:

12.2. Misión TI

El Área responsable del proceso de Sistemas e Información tiene como misión diseñar, implementar y administrar los elementos que constituyen la arquitectura tecnológica de la RED DE SALUD DEL NORTE E.S.E, entendiendo por tal los elementos físicos, lógicos, configuraciones y procedimientos necesarios para proporcionar a todos los clientes internos los servicios informáticos que le permitan desarrollar sus actividades y que conlleven a un crecimiento de la empresa.

12.3. Visión TI

En el 2025, seremos un grupo funcional reconocido con suficiente experiencia y buen desempeño dentro de la institución, gracias a su gran compromiso en la organización, ofreciéndole tecnología que ayude a optimizar los procesos que

icontec ISO 9001
IQNet
Certificado SC-CER880701

se lleven a cabo en la empresa, permitiéndole así ir a la búsqueda de sus objetivos, no solo en los procesos de atención sino también en los administrativos.

12.4. Actividades

- Garantizamos la continuidad del funcionamiento de las máquinas, redes y del "software" al máximo rendimiento, y facilitar su utilización a todos los clientes de la empresa.
- Realizamos mantenimientos preventivos y correctivos a la plataforma tecnológica con que cuenta la institución.
- Realizamos el diagnostico, planeación, implementación, evaluación y mejoramiento continuo al modelo de seguridad y privacidad de la información.
- Realizar la identificación, análisis, valoración, tratamiento y seguimiento de los riesgos asociados a la seguridad y privacidad de la información expedido por Mintic.
- Servir de apoyo, a todos los procesos y procedimientos de la institución.

12.5. Uso y Apropiación de la Tecnología

La institución ha tomado la decisión de Vincular a personas que facilitaran el desarrollo y promoción de una cultura o comportamientos culturales que faciliten la adopción de tecnología, siendo esencial para que las inversiones en TI sean productivas; para ello se requiere realizar actividades de fomento que logren un mayor nivel de uso y apropiación, generar canales y herramientas de comunicación directas y eficientes para inculcar el valor de las TIC como medio para optimizar la productividad laboral y optimizar la prestación de los servicios a todo ámbito (clientes internos, externos, ciudadanía), reconociendo las TIC como método de prestación de mejores servicios y generando un ambiente que genere apropiación en doble vía, cliente-usuario, usuario-cliente. Para fomentar el uso y apropiación de la tecnología es necesario tener en cuenta:

- Garantizar el acceso a todos los públicos.
- Crear productos o servicios usables.
- Brindar independencia del dispositivo y de la ubicación.
- Tener acceso a la red.

Para cada público se debe ofrecer y garantizar actividades de:

- Capacitación.
- Dotación de tecnología o de fomento al acceso.
- Desarrollar proyectos de evaluación y adopción de tecnología.

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

- Es preciso contar con herramientas en diferentes niveles: básico, analítico y gerencial. También se deben definir y aplicar procesos para comunicar, divulgar, retroalimentar y gobernar el uso y apropiación de TI.
- La alta dirección está comprometida con lo referente a las tecnologías aplicando Gobierno en Línea para facilitar y permitir el acceso de forma eficiente y segura manteniendo la triada (confidencialidad, integridad y disponibilidad) de los activos de la institución.

12.6. Servicios Tecnológicos

La adopción de las tecnologías de la información y comunicaciones está orientada por la política de gestión de la tecnología y la innovación en la cual la RED DE SALUD DEL NORTE E.S.E, se compromete a asignar los recursos disponibles para garantizar que los procesos institucionales, cuenten con el respaldo de una gestión tecnológica, orientada a la eficiencia, la efectividad y la seguridad, para los usuarios y sus familias, los colaboradores y el medio ambiente y a la promoción de una cultura organizacional para el buen uso de la tecnología con enfoque de riesgo.

12.7. Gobierno de TI

Al alinear las estrategias y los objetivos del negocio con las tecnologías de información se deben identificar las estrategias actuales y las proyectadas por la RED DE SALUD DEL NORTE E.S.E, de cara a al plan de gestión. Teniendo en cuenta el nivel de responsabilidad que tiene y basado en las operaciones de TI y de la gestión de TI, su principal objetivo es evaluar, dirigir y monitorizar las TI para que estas proporcionen el máximo valor posible a la organización para alcanzar lo establecido en los planes de la misma.

Por ello debe concentrarse en las decisiones que debe tomar para asegurar la gestión y el uso efectivo de las TI y que mecanismos le permitan medir para poder valorar las TI en su conjunto y poder tomar estas decisiones respecto a su gobierno.

El proceso de Gestión de la información de la Red de Salud del Norte, tiene como objetivo mantener y gestionar la infraestructura tecnológica necesaria para el aseguramiento en la disponibilidad, integridad y confiabilidad de la información; y garantizar la adecuada prestación del soporte técnico a las operaciones de los sistemas de información y los elementos de comunicación para contribuir al adecuado funcionamiento de los diferentes procesos de la organización. Alineado con el objetivo estratégico de Desarrollar y fortalecer una infraestructura informática que permita y facilite la interacción fácil y efectiva con nuestros grupos de valor (servicios digitales, acceso a la información, sistemas de información integrado y fidedigno).

Gestión de la información responsabilidad del Profesional en ingeniería de sistemas, y bajo de la Subgerencia Administrativa y Financiera. Sus responsabilidades dentro de la institución, están totalmente ligados al soporte

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

técnico (Software, Hardware, aplicativos, red de datos y telefónico), Administración de los recursos tecnológicos, alinear la institución y el proceso de gestión de la información con las estrategias de Arquitectura Empresarial o TI y Gobierno en Línea.

13. Riesgos

13.1. Política de Riesgos Red de Salud del Norte E.S.E

Declaración del Riesgo: En el desarrollo de las actividades de la ESE ocurren riesgos, por lo cual se compromete a adoptar mecanismos y acciones necesarias para que, a través de la gestión integral de los mismos, se prevenga o minimice su impacto.

Para ello se han adoptado mecanismos que permitan identificar, valorar, revelar y administrar los riesgos propios de su actividad, acogiendo una autorregulación prudencial. La entidad determinará su nivel de exposición concreta a los impactos de cada uno de los riesgos para priorizar su tratamiento, y estructurará criterios orientadores en la toma de decisiones respecto de los efectos de los mismos.

COPIA CONTROLADA

13.2. Plan de Tratamiento

Inicialmente se hace una breve descripción de los activos informáticos con que cuenta la Red de Salud del Norte, con el fin de reconocer el tipo de información y su clasificación. Para cada una de las amenazas se analiza las vulnerabilidades (debilidades) que se podrían presentar en el proceso, se identificarán las consecuencias, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de la información. Finalmente se describen acciones que se deben llevar a cabo para solventar las problemáticas presentadas.

Para la elaboración de este componente, se toma como punto de partida la matriz de riesgos de seguridad digital institucional.

- Riesgos de seguridad digital: Los riesgos priorizados para esta vigencia, son:
- Perdida de la confidencialidad (Bases de Datos)
- Perdida de la Integridad, disponibilidad y confidencialidad de la información (correos electrónicos)

icontec ISO 9001
IQNet
Certificado SC-CER880701

- Perdida de Información (Información Operativa de los procesos)
- Perdida de Conectividad (Sistemas de información y Software)
- Daños Físicos en los equipos tecnológicos (Hardware)

13.3. Identificación de los Activos de Seguridad de la Información

La Red de Salud del norte definió los siguientes activos como su seguimiento y control:

- Información
- Hardware
- Software
- Redes
- Personal

13.4. Valoración del Riesgo

En esta etapa se asocian las tablas de probabilidad y las de impacto, se define el nivel de severidad para el riesgo de seguridad de la información identificado a través de la matriz de calor

Bajo el criterio de probabilidad el riesgo se debe medir a partir de las siguientes especificaciones:

TABLA DE PROBABILIDAD			
NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir en algún momento	Al menos de una vez en los últimos 5 años.
3	Posible	El evento podría ocurrir en algún momento	Al menos de una vez en los últimos 2 años.
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos de una vez en el último año.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año.

13.5. Tabla de Impacto

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

Dependiendo de la afectación económica asociada a la perdida reputacional, definimos los niveles de impacto, así:

Tabla Criterios para definir el nivel de impacto

	Afectación Económica (o presupuestal)	Pérdida Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de alguna área de la organización
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta dircetiva y accionistas y/o
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país

COPIA CONTROL

13.6. Responsables

Son las personas encargadas y responsables de tomar medidas para dar solución a las circunstancias presentadas ya sea en mediano, corto o largo plazo, con el fin de remitir respuesta y dar solución a los eventos presentados.

La Red de Salud del Norte define sus responsabilidades de esta manera:

Gerencia: Formular en la política de gestión de los riesgos de la entidad, así como los lineamientos para tratamiento, manejo y seguimiento de los riesgos.

Jefe de Oficina de Planeación y Calidad: Corresponde liderar su elaboración y consolidación, servirá de facilitador en el proceso de Gestión de Riesgos.

Líderes de Procesos. En conjunto con sus equipos deben monitorear y revisar periódicamente el documento del Mapa de Riesgos y si es del caso ajustarlo.

Su importancia radica en la necesidad de monitorear permanentemente la gestión del riesgo y la efectividad de los controles establecidos.

En esta fase se debe:

Garantizar que los controles son eficaces y eficientes.

Obtener información adicional que permita mejorar la valoración del riesgo.

Analizar y aprender lecciones a partir de los eventos, los cambios, las tendencias, los éxitos y los fracasos.

icontec ISO 9001
IQNet
Certificado SC-CER880701

Detectar cambios en el contexto interno y externo.

Identificar riesgos emergentes.

Jefe de Oficina de Control Interno: Realizar seguimiento y evaluación de los riesgos. Su finalidad principal será asegurar la aplicación y sugerir los correctivos y ajustes necesarios para asegurar un efectivo manejo del riesgo.

CONTROLADA

13.7. Indicadores

Para el proceso se han definido los siguientes indicadores:

NOMBRE DEL PROCESO:	Sistemas e informacion			NOMBRE DEL SUBPROCESO:	N.A.
I. DATOS DEL INDICADOR					
NOMBRE INDICADOR:	Porcentaje de IPS con conectividad permanente				
OBJETIVO DEL INDICADOR:	Conocer el porcentaje de IPS de la ESE que cuentan con conectividad permanente				
TIPO DE INDICADOR:	Eficacia				
II. DEFINICION OPERACIONAL Y SEGUIMIENTO					
NUMERADOR:	Número de IPS con conectividad permanente en la ESE				
DENOMINADOR:	Total de IPS existentes en la ESE X 100				
FORMULA:	Se divide numerador entre denominador X 100				
UNIDAD DE MEDIDA:	Porcentual	FRECUENCIA DE MEDICION:	Anual	META:	>=90%
RESPONSABLE DE LA CAPTURA DEL DATO:	Oficina de Sistemas de información	RESPONSABLE DE LA VERIFICACION DEL DATO:	Oficina de Sistemas de información	RESPONSABLE DEL REPORTE AL CLIENTE INTERNO:	Oficina de Sistemas de información
FUENTE DEL DATO:	SD				

I. DATOS DEL INDICADOR					
NOMBRE INDICADOR:	Oportunidad en la respuesta de mantenimiento correctivo de hardware				
OBJETIVO DEL INDICADOR:	Calcular el promedio de tiempo en días transcurridos desde la solicitud del servicio hasta la solución del requerimiento.				
TIPO DE INDICADOR:	Eficacia				
II. DEFINICION OPERACIONAL Y SEGUIMIENTO					
NUMERADOR:	Sumatoria Total de Dias transcurridos desde la solicitud del servicio hasta la solución del requerimiento.				
DENOMINADOR:	Número Total de requerimientos recepcionados durante el período.				
FORMULA:	Se divide el numerador entre el denominador				
UNIDAD DE MEDIDA:	Dias	FRECUENCIA DE MEDICION:	Mensual	META:	<= 4 Dias
RESPONSABLE DE LA CAPTURA DEL DATO:	Responsable de Gestión de Información	RESPONSABLE DE LA VERIFICACION DEL DATO:	Responsable de Gestión de Información	RESPONSABLE DEL REPORTE AL CLIENTE INTERNO:	Responsable de Gestión de Información
FUENTE DEL DATO:	GESINFO				

icontec ISO 9001
IQNet
Certificado SC-CER880701

14. ESTRUCTURA ORGANIZACIONAL DEL ÁREA DE SISTEMAS

El área de Sistemas de Información y Comunicación se encuentra integrada actualmente por:

Profesional Universitario (2)

I. DATOS DEL INDICADOR					
NOMBRE INDICADOR:	Oportunidad en la respuesta de mantenimiento de Software				
OBJETIVO DEL INDICADOR:	Calcular el promedio de tiempo en días transcurridos desde la solicitud del servicio hasta la solución del requerimiento.				
NOMBRE DEL PROCESO:	Sistemas e informacion		NOMBRE DEL SUBPROCESO:	N.A.	

I. DATOS DEL INDICADOR					
NOMBRE INDICADOR:	Porcentaje de renovación tecnológica en equipos de computo				
OBJETIVO DEL INDICADOR:	Conocer el porcentaje de renovación tecnologica de los equipos de computo de la ESE				
TIPO DE INDICADOR:	Eficacia				
II. DEFINICION OPERACIONAL Y SEGUIMIENTO					
NUMERADOR:	Número de equipos de computo con fecha de adquisición menor a 5 años				
DENOMINADOR:	Total equipos de computo en funcionamiento X 100				
FORMULA:	Se divide numerador entre denominador X 100				
UNIDAD DE MEDIDA:	Porcentual	FRECUENCIA DE MEDICION:	semestral	META:	>=25%
RESPONSABLE DE LA CAPTURA DEL DATO:	Oficina de Sistemas de información	RESPONSABLE DE LA VERIFICACION DEL DATO:	Oficina de Sistemas de información	RESPONSABLE DEL REPORTE AL CLIENTE INTERNO:	Oficina de Sistemas de información

Tecnólogo (1)

Técnico (3)

Actividades que se realizan:

- Diseño e implementación de planes, proyectos que sean necesarios para garantizar el funcionamiento adecuado del área.
- Administración de las bases de datos de los diferentes sistemas con que cuenta la ESE.
- Mantenimiento y operación de los sistemas de información, así como todos los elementos que son parte de estos.
- Responder oportunamente ante las fallas que presente el ordenador reaccionando ante posibles amenazas de daño para no comprometer la información que en los equipos de almacenan.
- Controlar la estructura de la seguridad en la red, ordenadores y servidores para aplicar las medidas de seguridad que se crea conveniente para asegurar una buena protección contra ataques y posibles fallas de los equipos.
- Realización y actualización del inventario de la plataforma informática de la ESE.

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

- Estudio de la actual situación de la red de datos, e indicando las sugerencias que sean necesarios para su funcionamiento.
- Planificación de todas las programaciones y actividades asociadas al área de apoyo tecnológico.
- Efectuar el mantenimiento preventivo, correctivo (sin suministro de partes) para la tecnología informática de la ESE.
- Realización del mantenimiento general preventivo y correctivo (Inspecciones, tanto de funcionamiento como de seguridad, ajustes, reparaciones, análisis, limpieza y lubricación) a los equipos de la ESE.
- Soporte a los usuarios finales, en cuanto a Tecnologías de Información se refiere. Atenderlos identificando soluciones informáticas y aplicarlas según necesite, dar entrenamiento a usuarios y a otros miembros del grupo de soporte.
- Monitorear la conexión de Internet y conexión MPLS entre nodo principal y las demás IPS.
- Realizar backups de unidades de red, servidores y base de datos seleccionadas.
- Configurar las cuentas de los usuarios (afiliados participantes), además de apoyar con las diferentes situaciones de bloqueo y desbloqueo de las mismas.
- Administrar y controlar la operatividad de los servidores y otros sistemas informáticos.
- Actualizar la información de la página web de la Red.
- Instalar, administrar y actualizar los diferentes gestores de contenidos web que existen actualmente.
- El grupo funcional de apoyo tecnológico hace parte de la subgerencia administrativa y financiera.

COPIA CONTROLADA

15. EVALUACIÓN INTERNA TI

El estado actual del área se evaluará con la identificación de debilidades y fortalezas

15.1. Debilidades

- Presupuesto reducido para inversión en TIC’s
- Infraestructura tecnológica deficiente

icontec ISO 9001
IQNet
Certificado SC-CER880701

- Infraestructura eléctrica deficiente
- Los tiempos en la contratación de la entidad dificulta la gestión de los Proyectos que son requeridos actualmente en TIC
- El proceso de compras de la red no permite una reacción oportuna para las respuestas a los requerimientos tecnológicos sean estos de índole correctivos o preventivos.
- Existe un porcentaje aproximado del 25% de los Equipos de Cómputo que están cumpliendo su vida útil y es necesaria su renovación, así como la mejora de partes en equipos en un 30%

15.2. Fortalezas

- Compromiso del Personal Directivo y de Sistemas
- Implementación de los estándares de acreditación
- Personal capacitado y comprometido con la E.S.E.
- Adecuaciones de red para la interconexión entre sedes con el fin de reorganizar los servicios
- Adecuaciones parciales del cableado estructurado de algunas IPS.

15.3. Estrategia de TI

ESTRATEGIA 1

Proyectos de Inversión de la institución para fortalecer la Infraestructura Tecnológica, y proyectar mejores servicios tecnológicos a los usuarios, especialmente los alineados con la misión y visión de la entidad.

ESTRATEGIA 2

Mantener actualizado el inventario de equipos de cómputo de la E.S.E. con el fin de identificar rápidamente el estado del parque tecnológico en cuanto a disponibilidad, obsolescencia, garantías y mantenimiento.

ESTRATEGIA 3

Mantener actualizado el inventario de licencias de software identificando la propiedad intelectual de las mismas con el fin de garantizar el cumplimiento de la normatividad con respecto al tema.

ESTRATEGIA 4

Gestión de Seguridad y privacidad de la Información. Planear la implementación del modelo de Seguridad y privacidad de la información, buen uso de tecnologías en la Red y de la aplicación de buenas prácticas de seguridad. Involucrando en el plan de capacitación temas que permitan la apropiación de los usuarios de sus procesos.

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

ESTRATEGIA 5

Gestión de Riesgos en Seguridad y privacidad de la información. Realizar el levantamiento de los riesgos asociados a la privacidad de la información, su gestión y su tratamiento, según plan de riesgos de la seguridad y privacidad de la información.

15.4. Plan de Proyectos de TI

Implementación y continuidad del servicio

Todas las actividades de tecnología que de ella se deriven, mantenimiento y adecuación de infraestructura y redes, mantenimiento de equipos, Soporte a usuarios.

Mejoramiento de la Infraestructura Tecnológica

Instalación de MPLS para IPS faltantes, mantenimiento cableado y cuarto de máquinas de IPS.

Actualización parque tecnológico

Renovación de equipos de cómputo acorde a los requerimientos de tecnología que optimicen la prestación de los servicios de salud.

Mantenimiento Sistema de cámaras

Realizar mantenimientos preventivos y correctivos a circuito cerrado de cámaras de seguridad de la Red de Salud del Norte, para el monitoreo de las instalaciones de las 17 IPS y sede administrativa.

Fortalecimiento Sistema VOZ IP

Adquisición de servicio Call Center incluyendo adecuación de espacio, hardware, conectividad y capacitación del personal.

Adquisición Sistema de Información para Copias de Seguridad

Adquisición Software y Hardware (Sistema NAS) adecuado para garantizar los backup de base datos, aplicaciones y datos de la entidad.

Renovación y ampliación licencias antivirus

Compra y renovación licencias para protección antivirus así misma ampliación de número de licencias a adquirir.

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701

16. PLAN DE COMUNICACIONES DEL PETI

Como estrategia de comunicación y divulgación del Plan estratégico de tecnologías de la Información y comunicaciones se realiza la divulgación por medio de la página institucional y medios de comunicación internos para ser conocido a los colaboradores y usuarios.

De igual manera se identifican los medios para socializar con los grupos de interés primarios a quienes debe darse a conocer este plan:

- Alta dirección, a través del comité.
- Todos los funcionarios, a través de intranet, píldoras, Pagina Web, wallpaper, reinducción, mailing.
- Funcionarios nuevos, jornadas de capacitación e inducción.

Elaboró:	Revisó:	Aprobó:
ORIGINAL FIRMADO	ORIGINAL FIRMADO	ORIGINAL FIRMADO
JEAN CARLOS TEGUE GRANJA **Auxiliar Administrativo afiliado participe Agesoc**	**OMAR FERNADO ARREGOCES** **Profesional Administrativo Afiliado Participe Agesoc**	**XAVIER MONTOYA GOMEZ** **Subgerente Administrativo y Financiero**
Fecha: diciembre 2021	**Fecha:** diciembre 2021	**Fecha:** diciembre 2021

VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA DE VIGENCIA
01	Actualización del procedimiento frente a la nueva definición de procesos, niveles de la documentación, se establece consecutivo y control de cambio de los documentos.	Diciembre 2021

COPIA CONTROLADA

icontec ISO 9001
IQNet
Certificado SC-CER880701