

RESOLUCIÓN No. 015 (Enero 13 de 2021)

“POR MEDIO DE LA CUAL SE IMPLEMENTA EL PLAN DE GERENCIA DE LA INFORMACIÓN EN LA ESE HOSPITAL LOCAL DE PIEDECUESTA”

EL GERENTE GENERAL DE LA ESE HOSPITAL LOCAL DE PIEDECUESTA

En uso de sus facultades Constitucionales, legales y en especial las conferidas en el Decreto 018 expedido por la Gobernación de Santander, de fecha 25 de Enero de 2006 y

CONSIDERANDO:

1. Que el Decreto 1011 de 2016 establece el sistema obligatorio de la garantía de la calidad de la atención en salud, para las instituciones que conforman el sistema general de seguridad social en salud.
2. Que dentro de las actividades de mantenimiento del sistema de gestión de calidad se definió la importancia de implementar el modelo de operación por procesos.
3. Que el decreto 2573 de 2014, por medio del cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, y se reglamenta parcialmente la Ley 1341 de 2009, donde se definieron los principios y conceptos en materia de las TIC (tecnología de la información y las telecomunicaciones).
4. Que el estado colombiano ha promovido la estrategia de gobierno electrónico la cual busca construir un estado más eficiente, transparente y participativo gracias a las TIC.
5. Que el decreto 1068 de 2015, decreto único reglamentario del sector de las tecnologías de la información y las telecomunicaciones.



6. Que en mérito de lo expuesto y garantizando el ciclo de mejoramiento continuo es fundamental Promover el despliegue de los planes relacionados con el sistema de gestión de calidad.

RESUELVE

ARTICULO PRIMERO. IMPLEMENTAR: El plan de gerencia de la información para la vigencia 2021 a 2022 de la ESE Hospital Local de Piedecuesta, el cual tendrá la siguiente estructura.

1 GENERALIDADES

1.1 Objetivos

Gestionar la información Administrativa y Asistencial generada en la prestación de los servicios de Salud de forma oportuna y confiable para la toma de Decisiones en todos los niveles de la organización con el apoyo de los sistemas tecnológicos y de Información Disponible.

1.2 Alcance

El alcance del presente plan comprende la ejecución de acciones para garantizar la eficiente toma de decisiones.

2 Responsables

Ingeniero de sistemas

3 Definiciones

SISTEMA DE INFORMACIÓN: Conjunto de elementos que interactúan entre sí y que tienen como fin la administración de datos e información.



AMENAZA: probabilidad de ocurrencia, durante un período específico y dentro de un área determinada, de un fenómeno que puede potencialmente causar daños en los elementos en riesgo.

VULNERABILIDAD: La vulnerabilidad se refiere al grado de pérdidas relacionadas con un elemento en riesgo (o un conjunto de elementos en riesgo), que resulta como consecuencia de un fenómeno natural o artificial con una determinada magnitud. Se expresa de una escala de "0" (no hay daños) a "1" (daño total).

RIESGO: Se refiere a la cuantificación de los posibles daños ocasionados a los elementos en riesgo como consecuencia de un fenómeno natural o artificial en términos de vidas perdidas, personas heridas, daños materiales y ambientales e interrupciones de la actividad económica.

SEGURIDAD: Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que, en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

RIESGO DE SEGURIDAD DE LA INFORMACIÓN: Probabilidad de que una amenaza ocasione daño o pérdida o afectación en la confidencialidad en un activo de información.

ACTIVO: Son todo aquellos recursos o componentes de la institución, tanto físico (tangibles), como lógicos (intangibles) que constituyen su infraestructura, patrimonio, conocimiento y reputación en el mercado.

DATOS: Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

PLAN DE CONTIGENCIA: Es una estrategia que se compone de una serie de procedimientos que facilitan una solución alternativa que permite restituir Rápidamente el funcionamiento de los servicios críticos ante la eventualidad que lo afecte de forma parcial o total.



4 GENERALIDADES DEL HOSPITAL

Específicamente, la Empresa Social del Estado Local de Piedecuesta, se creó mediante decreto Departamental N° 0018 de Enero 25 de 2006 emanada por las Gobernación de Santander como entidad descentralizada del orden departamental con personería jurídica, patrimonio propio y autonomía administrativa a la Secretaria de Salud de Santander. Con el objetivo último de garantizar la prestación de servicios de salud de baja complejidad, a la población más competencia privada y buscando ingresos oportunos que ayuden a su supervivencia.

La E.S.E es una Empresa Social de estado que soporta su operación con bienes sociales y que determinan la importancia de prestación de servicios de salud y de avanzar en procesos que permitan el alcance de niveles de sostenibilidad, garantizando la accesibilidad, oportunidad, eficiencia y la calidad en los mismos.

Desde su creación el enfoque de direccionamiento se basó en la utilización óptima de los recursos y en un proceso de planeación presupuestal que prioriza las actividades económicas y financieras, hacia el cumplimiento de la misión de la entidad, y la satisfacción de nuestros usuarios, además y de la rentabilidad social y económica de la E.S.E.

Los servicios que presta la E.S.E son de alta calidad ya que cuentan con los recursos técnicos, científicos, humanos, financieros para brindar la prestación como lo Establece la política Nacional de Prestación de Servicios de Salud acorde con nuestro nivel de complejidad.

Los clientes de la E.S.E son afiliados al Sistema de Seguridad Social; 105 vinculados mediante el sisben o listado censal, el régimen subsidiado, régimen contributivo, regímenes especiales y particulares a los cuales se les presta el servicio sin discriminación alguna.

Con este portafolio de servicios queremos que sirva de guía para la utilización de los servicios ofertados y a la vez reafirmar nuestro compromiso de fortalecer la

prestación de servicios de salud a toda la población de Piedecuesta, a través de un mejoramiento de las instalaciones, adquisición tecnológica y una atención digna y humanizada.



4.1 MISIÓN

Somos una Empresa Social del Estado del orden departamental de bajo nivel de complejidad con vocación académica enfocada en la prestación de servicios de salud de forma integral, segura y humanizada

4.2 VISIÓN

Nuestro hospital será en el año 2020 reconocido por ser líder en el modelo de atención primaria en salud en el Departamento, siendo formador de talento humano en salud, a través de la generación de conocimiento logrando experiencias positivas en nuestros usuarios.

4.3 OBJETIVOS ESTRATEGICOS

En el marco de la misión institucional de la Empresa Social del Estado Hospital Local de Piedecuesta, nos proponemos como objetivos Estratégicos:



OBJETIVOS ESTRATEGICOS

PERSPECTIVA	OBJETIVO
CLIENTE	Fortalecer la prestación de los servicios asistenciales por medio de la satisfacción del usuario y la integralidad con niveles superiores de complejidad
FINANCIERO	Lograr la sostenibilidad y competitividad del Hospital a través de una gestión oportuna y efectiva de los recursos.
PROCESOS	Lograr niveles de excelencia en los procesos institucionales
APRENDIZAJE Y CRECIMIENTO	Fortalecer los sistemas de información de la institución. Mantener el capital humano competente, comprometido y satisfecho en la institución.



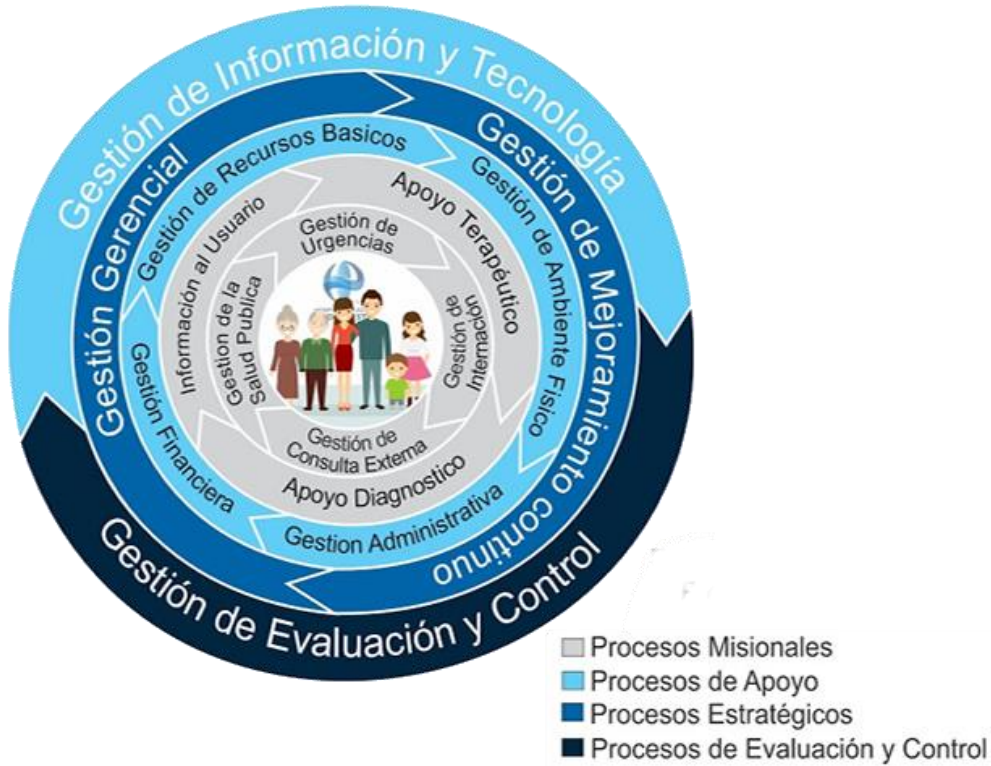
5 ESTRUCTURA ORGANIZACIONAL



La E.S.E. Hospital Local de Piedecuesta se encuentra conformada según el decreto 018 del 25 de Enero de 2006 expedido por la Gobernación de Santander.



5.1 MAPA DE PROCESOS



6 IDENTIFICACIÓN DE NECESIDADES DE INFORMACIÓN.

Para la identificación de necesidades de información se presentan diferentes mecanismos:

EVALUACIÓN DE SATISFACCIÓN DE USUARIOS

Mediante el indicador de Proporción Satisfacción Usuario se mide mensualmente y se evalúa la prestación del servicio en la E.S.E. Hospital Local de Piedecuesta.

Este indicador se alimenta de acuerdo a los resultados de las encuestas realizadas mensualmente a los usuarios en las áreas de Consulta Externa, Urgencias, Hospitalización y Promoción y Prevención.

Con este mecanismo se puede valorar la claridad, oportunidad y calidad de información transmitida al usuario en el servicio recibido.

Responsable: Oficina Amiga del Usuario.

REGISTRO DE PQRS

Mecanismos donde se registrar y gestionan las diferentes inquietudes, quejas y reclamos de los usuarios.

Con este mecanismo se pueden identificar las pqrs más frecuentes y la criticidad de las mismas para ejecutar acciones que permitan fortalecer la gestión de la información con los usuarios.

Responsable: Oficina Amiga del Usuario.





ANALISIS DOFA DE LA ENTIDAD

Mecanismo donde se identifican las debilidades, oportunidades, fortalezas y amenazas de la entidad, allí participan diferentes áreas y con base en éste se construye el plan de desarrollo.

Con este mecanismo es posible valorar las debilidades y amenazas en el tratamiento de información para fortalecer el sistema de información de la entidad y con ello dar cumplimiento al direccionamiento estratégico.

Responsable: Oficina de Planeación

MATRIZ DE COMUNICACIONES

Es una herramienta de evaluación diseñada para determinar qué comunica cada una de las áreas de la institución especificando el cómo, cuándo y a quién. Su objetivo es dar a conocer las necesidades de comunicación para contribuir en el afianzamiento de la cultura de calidad.

Responsable: Todos los procesos.

AUDITORIAS DE SERVICIO

Con este mecanismo se puede monitorear y hacer seguimiento a la prestación de los servicios en la institución e identificar hallazgos relacionados con el tratamiento de la información.

Responsable: Mejoramiento continuo, Control interno, Auditor médico

BRIEFING

Rondas realizadas en los servicios asistenciales para conocer las necesidades de los usuarios y colaboradores.

Responsable: Auditor médico.



INDICADORES

Este mecanismo permite evaluar hasta qué punto o en qué medida se están cumpliendo los objetivos estratégicos del Hospital y de allí se generan las necesidades de información en la institución.

Responsable: Todos los procesos.

7 CONFIDENCIALIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

7.1 POLITICA

Resolución 068 de Diciembre 31 de 2018 por medio de la cual la E.S.E. Hospital Local de Piedecuesta adopta el sistema de Gestión de Seguridad de la información como una herramienta para garantizar la confidencialidad, integridad y privacidad de la información, administrando los riesgos, cumpliendo con la legislación vigente y generando cultura de seguridad de la información en los servidores públicos y demás partes interesadas.

El objetivo general de esta política es mantener la confidencialidad, integridad, disponibilidad de los activos de información y la protección de datos personales, mediante la gestión de los riesgos, que permita establecer un marco de confianza a las partes interesadas en concordancia con la misión y visión del Hospital.

7.2 RESPONSABILIDAD DE LOS USUARIOS

El personal del área de sistemas es el responsable de almacenar y custodiar la información de la entidad, realizar copias de seguridad diariamente y llevar el control del almacenamiento en la nube, verificar que la información se está sincronizando correctamente.

Los usuarios deberán seguir las recomendaciones del personal de sistemas y guardar la información en una ubicación predeterminada con el fin de que ésta se sincronice automáticamente en las cuentas de almacenamiento de Nextcloud asignada a cada uno.



Los usuarios deben evitar descargar información e instalar software que no esté autorizado por el área de sistemas.

Los usuarios no deberán intercambiar las contraseñas asignadas para el acceso al software institucional con el fin de evitar suplantación e incurrir en inconvenientes que puedan llegar a ser de carácter legal.

Se firmará un compromiso de confidencialidad donde el usuario se compromete a usar con responsabilidad la información que tenga bajo su custodia a lo largo de su relación como colaborador de la ESE Hospital Local de Piedecuesta, y a no divulgar la información que se encuentre dentro de la historia clínica o datos que puedan afectar la integridad del paciente.

Si un colaborador deja de prestar sus servicios en la ESE deberá firmar un paz y salvo por parte del área de sistemas quienes deberán verificar que tanto los equipos como la información se entreguen de manera correcta.

7.3 GESTIÓN Y TRATAMIENTO DE LOS RIESGOS

Cada uno de los procesos dentro de la institución cuenta con una matriz de riesgos donde se realiza la evaluación del diagnóstico de la información, se analizan los riesgos y se plantean las acciones que deben ser realizadas por la entidad para mitigar de una manera efectiva todo el conjunto de riesgos.

IDENTIFICACIÓN DEL RIESGO		ANÁLISIS DE RIESGOS				VALORACIÓN DEL RIESGO		SEGUIMIENTO AL RIESGO											
QUE PUEDE FALLAR (RIESGO)	CAUSAS (RMV) (Persona, Método, Materiales/ Insumos, Equipos, Medición y Ambiente)	EFECTOS	CALIFICACIÓN DEL RIESGO		CRITICIDAD	CONTROLES	CALIFICACIÓN DEL CONTROL	NPR	CLASIFICACIÓN DEL RIESGO	ACCIONES PLANTEADAS	ESTADO DE LAS ACCIONES	FECHA SEGUIMIENTO	CALIFICACIÓN DEL RIESGO			NPR	CLASIFICACIÓN DEL RIESGO	EVIDENCIAS	RESPONSABLE
			1	2									1	2	3				
Robo, alteración y/o pérdida de información.	Materiales: Uso de software malicioso, suplantación de sitios web, daño informático.	Interrupción del servicio y pérdidas económicas. Mala imagen institucional.	1	4	4	Procedimiento copias de Seguridad. Uso de antivirus	4	16	RIESGO MEDIO (Establecer Controles)	controles de acceso en la red. Documentar plan de contingencia en caso de robo y pérdida de información. Antivirus actualizado	C C C	Diciembre de 2018 nov-18 Diciembre de 2018						Plan de contingencia	Juliana Márquez
	Medición: No se tiene definido la medición para el sistema de seguridad de la información.	Entropamiento de los procesos en las diferentes áreas del hospital.				Controles de acceso a los sistemas de información				Antivirus actualizado	C	Diciembre de 2018						Licencias de Kaspersky	Eddison Narazán
	Persona: Acceso no autorizado al sistema de información, descarga de información no autorizada, violación de datos personales.	Insatisfacción de los clientes, quejas y reclamos								Algar la información de los equipos en la Nube en caso de daño en el equipo se ingresa a la cuenta de nexcloud y se restaura la información.	C	Diciembre de 2018						Licencias de Nextcloud	Juliana Márquez
	Ambiente: Daños y pérdidas en equipos tecnológicos por castrotes naturales.																		



- Todos los servidores estarán ubicados en lugares con acceso solo para personal autorizado.
- Mantener actualizado el antivirus en cada estación de trabajo.
- Los equipos de la institución se encuentran dentro de un dominio con el fin de restringir permisos para instalación de software no autorizado.
- Todos los equipos servidores deberán tener controles de acceso para garantizar la integridad y disponibilidad de la información y de los sistemas de información. Solo el personal de sistemas tendrá acceso a los cuartos de telecomunicaciones donde se encuentran ubicados estos equipos.
- Se realizará mantenimiento preventivo y correctivo a los equipos de cómputo de acuerdo al plan y cronograma de mantenimiento de equipos. GIT-ST-PL-2

7.2 CONTROL DE ACCESO.

- Se crearán mecanismos de identificación, autenticación, y roles de usuario de acuerdo a la información que maneje.
- Se crearán cuentas de usuario en el dominio para el ingreso a los equipos de cómputo para evitar que personal no autorizado acceda a ellos.
- Se crean cuentas de usuario al software institucional y se asignan los perfiles de acuerdo al rol que desempeña de manera que no se pueda tener acceso a información que no se maneje desde su área.
- Cada usuario debe crear y definir una contraseña combinando caracteres alfanuméricos y con una longitud mínima de 8 caracteres.



- El sistema de información de la ESE Hospital Local de Piedecuesta tendrá registro de actividades cada vez que los usuarios accedan, con el fin de llevar una trazabilidad de las operaciones ejecutadas.
- Los líderes de proceso o enlace de la empresa contratista, solicitará al administrador del sistema la creación o activación de usuarios en el sistema de información de la institución indicando nombres y apellidos, número de identificación, dirección, teléfono, fecha de nacimiento y tarjeta profesional de ser necesario. De igual forma el colaborador debe firmar el formato de creación de usuarios donde queda evidencia de que el usuario se creó y la fecha de creación.

7.3 **PROTECCIÓN CONTRA SOFTWARE MALICIOSO.**

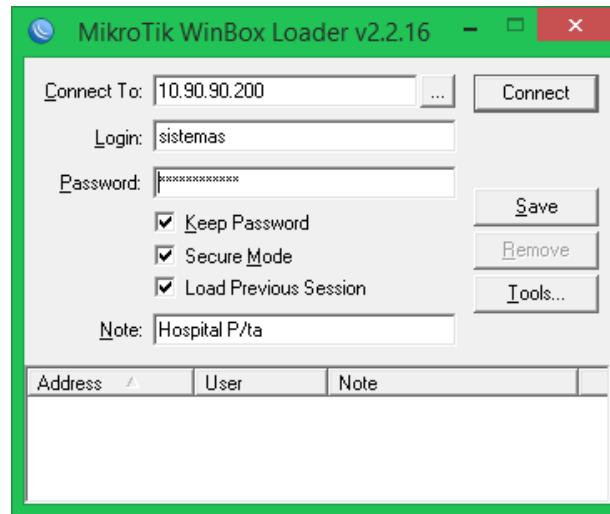
Todos los equipos de la E.S.E. cuentan con antivirus licenciado para garantizar protección contra virus, gusanos, troyanos, spyware, phishing y otra amenazas que provengan de la red o dispositivos externos.

Los equipos de la ESE se encuentran incluidos en un dominio con permisos limitados para evitar la descarga e instalación de software no autorizado.

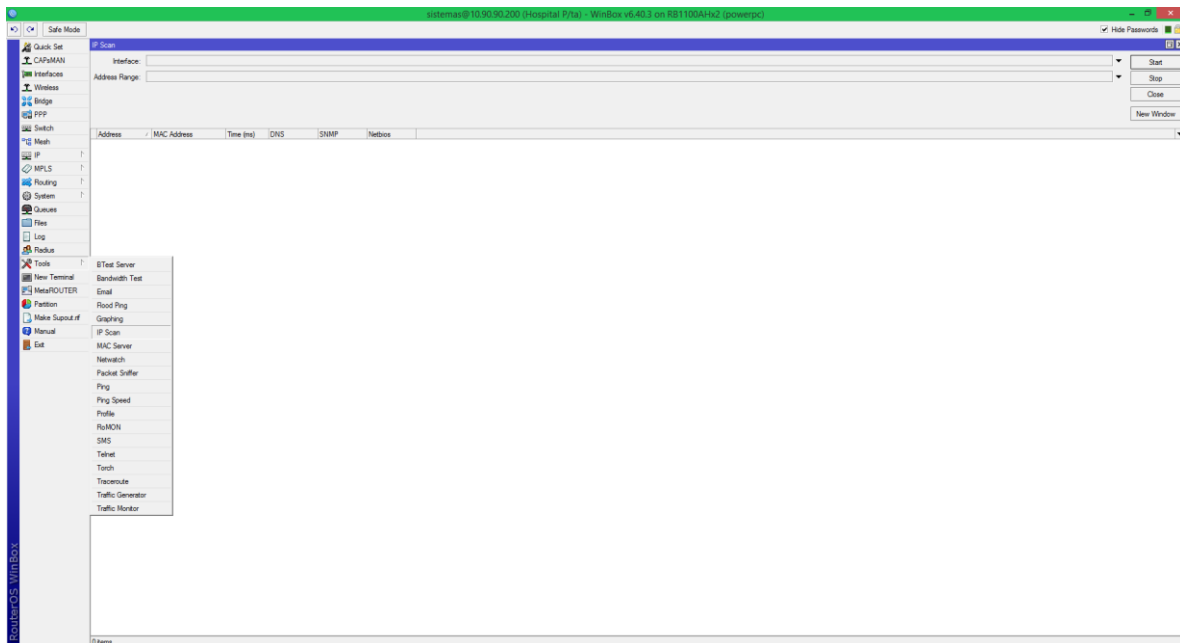
7.4 **ESCANEO DE LA RED**

Para realizar supervisión y exploración de la red del hospital se utiliza el router mikrotik accediendo desde el aplicativo Winbox.





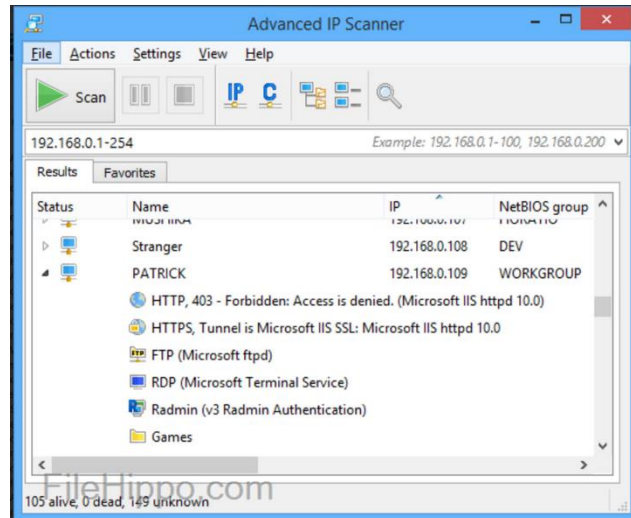
Una vez dentro de winbox se selecciona la opción Tools y luego IP Scan.



Dentro de esta ventana se selecciona la interface y clic al botón start para iniciar el escaneo.



Otra de las aplicaciones utilizadas para el monitoreo de la red es Advance IP Scanner que es una herramienta de código libre y que permite recopilar información de los dispositivos conectados, carpetas compartidas, servidores HTTP y servidores FTP.



7.5 COPIAS DE SEGURIDAD.

El servidor donde se encuentra instalado el software misional realiza copias de seguridad automáticamente en horas de la noche. De igual forma el Líder de Gestión de la Información y la Tecnología realiza copias manualmente todos los días al terminar la jornada laboral las cuales quedan almacenadas en la nube en una cuenta de Nextcloud.

Los equipos de los colaboradores con más uso de información cuentan con licencias de almacenamiento en la nube, con el fin de poder restaurarla en caso de daño del equipo o pérdida de la información.

8 INTRANET

La E.S.E. Hospital Local de Piedecuesta cuenta con una intranet que permite compartir con los colaboradores la información de cada uno de los procesos institucionales, lo que genera gran valor a la organización.

Dentro de la intranet se encuentra almacenada la información de los procedimientos de cada una de las áreas, la matriz de riesgos, el plan de acción, la caracterización, el plan operativo anual y la matriz de comunicaciones de cada uno de los 15 procesos de la institución.



De igual forma se encuentran habilitados los formatos para reportes de fallas de la atención, falla de equipos biomédicos y reporte de identificación de hallazgos lo que permite identificar las debilidades y necesidades y ejecutar acciones para fortalecer los procedimientos y mejorar la prestación del servicio.



RIESGOS DE INFORMACIÓN Y LA TECNOLOGÍA
PLAN OPERATIVO ANUAL DE LA INFORMACIÓN Y LA TECNOLOGÍA
MATRIZ DE COMUNICACIONES INFORMACIÓN Y TECNOLOGÍA
PLAN DE ACCIÓN POR PROCESOS DE INFORMACIÓN Y TECNOLOGÍA
CARACTERIZACIÓN DE LA INFORMACIÓN Y TECNOLOGÍA

9. CONCLUSIONES

La información es un activo que tiene un gran valor para las organizaciones y por ende debe protegerse debidamente.

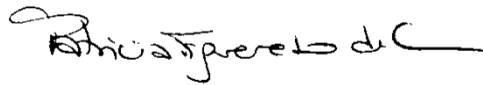
El resguardo de la información y la continuidad de las operaciones ante eventualidades o desastres, constituye una de las principales estrategias que deben desarrollar y procurar las organizaciones modernas ya sean públicas o privadas, ya que de ello depende en la mayoría de los casos la continuidad o cese de los servicios entregados por la organización a la comunidad.

El presente Plan de Gerencia de la Información, tiene como objetivo principal proteger la información, tomando las medidas de seguridad pertinentes ante una contingencia de cualquier tipo y llevar un proceso de recuperación de la información y las actividades laborales en el menor tiempo posible.



ARTICULO SEGUNDO. VIGENCIA. La presente resolución rige a partir de la fecha de su expedición.

Dado en la ciudad de Piedecuesta, a los veintiocho (28) días del mes de enero del año 2021.



MARIA PATRICIA FIGUEREDO MACIAS
Gerente

Apoyo: Sergio Mauricio Ramírez Ramírez.
Asesor de control interno

