DISEÑO DE LAS POLITICAS DE SEGURIDAD PARA LA EMPRESA SOCIAL DEL ESTADO HOSPITAL INTEGRADO SAN ANTONIO DE PUENTE NACIONAL

TRABAJO DE GRADO

GERMAN ALBERTO CRUZ VARGAS

LEONEL PARRA NIEVES

NANCY MILENA ARIZA

Códigos

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2016

DISEÑO DE LAS POLITICAS DE SEGURIDAD PARA LA EMPRESA SOCIAL DEL ESTADO HOSPITAL INTEGRADO SAN ANTONIO DE PUENTE NACIONAL

TRABAJO DE GRADO

GERMAN ALBERTO CRUZ VARGAS

LEONEL PARRA NIEVES

NANCY MILENA ARIZA

Códigos

Asesor:
GIOVANNI ANDRES PIEDRAHITA SOLORZANO

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2016

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firmas de los jurados

Bogotá, 29 de abril de 2016

INTRODUCCION

Las organizaciones en busca de mejorar los procesos realizan esfuerzos grandes en reconocer la importancia que tiene la implementación del sistema de gestión de seguridad de la información. Esto hace necesario la identificación del recurso humano, financiero y tecnológico que son el insumo importante para la preparación y puesta en marcha del mismo.

A demás todas las empresas son susceptibles de mejora de algunos de sus procesos que ayudan a la productividad y a la prestación de un mejor servicio como lo es el manejo de la información.

El presente documento hace referencia al diseño de políticas de seguridad de la información de la Empresa Social del Estado Hospital San Antonio de puente nacional, para las áreas de Facturación, SIAU, contabilidad, Estadística y Gerencia.

INDICE

AGRADECIMIENTOS 6
1. RESUMEN EJECUTIVO 7
2. JUSTIFICACIÓN 9
3. MARCO TEÓRICO Y REFERENTES 10
4. METODOLOGÍA 13
5. RESULTADOS Y DISCUSIÓN 15
6. CONCLUSIONES 17
7. BIBLIOGRAFÍA 18
8. ANEXOS 19

AGRADECIMIENTOS

A Dios primeramente que me ha dado la sabiduría necesaria, me ha guiado y orientado para poder obtener un logro importante en mi vida diaria y mi vida profesional. Es la oportunidad para expresar los méritos hacia los Profesionales de la especialización en Seguridad De La Información del Politécnico Gran colombiano por querer compartir sus conocimientos con nosotros. También agradecer a los compañeros Ing. German Alberto Cruz, a mi querida Ing. Nancy Milena Ariza por haber compartido momentos gratos de trabajo que hicieron posible que lográramos obtener este logro importante en nuestras vidas ser Especialistas.

(Leonel)

Quiero agradecer infinitamente a Dios por haberme iluminado y guiado para alcanzar este nuevo logro en mi carrera como profesional, a mí mami y a mi Hija por su amor y apoyo incondicional, a mis compañeros el Ingeniero Germán Alberto Cruz y Leonel Parra Nieves por compartir sus experiencias en este proceso de formación, a mis profesores de la Especialización del Politécnico Gran Colombiano por aportar al enriquecimiento con calidad a mi conocimiento.

(Nancy)

Agradezco a mi familia que ha sabido guardarme espacio y tiempo en el proceso para obtener este logro.

(Germán)

1. RESUMEN EJECUTIVO

En el hospital integrado San Antonio De Puente Nacional Santander no existe un plan de políticas de seguridad que garantice la confidencialidad, integridad y disponibilidad de su información el cual presta de servicios médicos a la región. La institución administra información valiosa y confidencial la cual es operada sin ningún control de seguridad de la información poniendo en riesgo las operaciones de la empresa.

Con el desarrollo de este proyecto se pretende Diseñar Políticas Seguridad De la información Para El Hospital San Antonio De Puente Nacional Santander con el propósito de asegurar los activos de la empresa, manteniendo la eficiencia en la prestación del servicio, y se determina:

- Realizar un diagnóstico de la seguridad de la información para el hospital Integrado San Antonio con el fin de identificar puntos críticos.
- Determinar el estado actual de las políticas establecidas en la empresa con el fin de aplicar las medidas necesarias.
- Diseñar políticas de seguridad de la información para el hospital Integrado San Antonio de acuerdo al diagnóstico y las políticas actuales.

Con el fin de brindar un aseguramiento de la información al Hospital Integrado San Antonio se involucran las siguientes áreas:

- Contabilidad: Esta área dará alcance a los siguientes procesos: nómina, contratación externa, pago a proveedores, cartera.

- Facturacion: Esta área dará alcance a: Formulas Medicas, Pagos de servicios médicos ambulatorios, exámenes, Ordenes de Medicamentos y procedimientos.
- Sistema de información de atención al usuario SIAU: Este proceso dará alcance a la atención y asignación de citas médicas, cancelaciones, reprogramación, PQR.
- Estadística: Este proceso dará alcance al registro de historias clínicas del pacientes es operado por 1 persona.
- Gerencia: Este proceso dará alcance a rendición de informes a los órganos de control y es dirigido por la junta directiva y el respectivo gerente.

Teniendo en cuenta la identificación de las áreas que manejan información confidencial en los diferentes procesos se realizó un diagnóstico inicial donde se detectaron vulnerabilidades en la administración de la información; posteriormente a esta situación se realizó un informe con el estado actual de las políticas que tenía la empresa y de cómo es la gestión de la seguridad de la información. Después de realizado el diagnóstico y analizado el estado actual se crea el documento con las Políticas de seguridad de la información que contienen: su contexto, objetivo, alcance, responsables, cumplimiento en las áreas Facturación, SIAU, Contabilidad, Estadística y Gerencia.

De acuerdo al desarrollo del proyecto la empresa social de estado hospital San Antonio de Puente Nacional se diseñaron las Políticas de seguridad de la información que contienen: su contexto, objetivo, alcance, responsables, cumplimiento.

2. JUSTIFICACIÓN

La seguridad de la información evoluciona constantemente al igual que las amenazas y otras formas de robo, alteración o pérdida de información. Con el ánimo de prevenir incidentes que puedan causar daños a los activos y procesos que manejan la empresa social de estado hospital San Antonio de Puente Nacional, se deben hacer esfuerzos que permitan asegurar los activos de información de la empresa.

Ante la falta de políticas que permitan asegurar los activos de información del hospital San Antonio de Puente Nacional se propone diseñar políticas de seguridad de la información que estén de acuerdo con los lineamientos del Gobierno en línea (GEL 3.1) con el fin de mantener la integridad, confiabilidad y disponibilidad de los activos de información del hospital.

Las políticas de seguridad de información establecen los límites y requerimientos para estructurar una conducta regulatoria que conlleve a asegurar en los activos de información del hospital; con el diseño de las políticas se pretende cubrir un 90% de las áreas que tiene alta gobernabilidad el hospital donde el activo de información es crucial para la continuidad de los procesos como son las áreas de Facturación, SIAU, contabilidad, Estadística y Gerencia correspondientes a nivel 1 del hospital.

3. MARCO TEÓRICO Y REFERENTES

El estándar internacional ISO/IEC 27002 define la seguridad de la información como “la preservación de la confidencialidad, integridad y disponibilidad de la información”.[1] La confidencialidad refiere a la garantía de que solo personas autorizadas pueden acceder a la información; la integridad refiere a que la información siempre es exacta y completa; la disponibilidad refiere usuarios autorizados tiene acceso a la información cuando lo requieran.

La guia técnica de seguridad y privacidad de la información de la estrategia del gobierno en líneadefine las politícas de seguridad como una forma de proteger los activos información de un amplio espectro de amenazas a través de directivas “a fin de: garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de las entidades del Estado”.[2]

El espectro de amenazas de los activos de información pueden ser internos o externos, Michael E Whitman, identifica 12 categorias que son: Actos resultado de errores humano o fallas, comprometer la propiedad intelectual, actos deliberados de espionaje, extorsión, sabotaje, robo, ataques por medio de software, desastres naturales, desviación de la calidad del servicio, fallas técnicas en hardware, software, y uso de tecnologías obsoletas. [3] Estas amenazas son genericas para la mayoría de empresas, entre ellas se resalta el sector de la salud.

La empresa social del estado Hospital Integrado San Antonio de Puente Nacional al ser una empresa del estado debe estar conforme a las estrategias del gobierno en línea las cuales se basan en la norma técnica colombiana NTC ISO/IEC 27001 [4] sin embargo, el hospital, al estar dedicado al sector de salud aplica al estándar ISO/IEC 27799 el cual define guias para interpretar e implementar seguridad de la información en el área de salud. [5]

El estándar ISO/IEC 27799 dentro de sus elementos para gestionar la seguridad de información considera a la política de seguridad de información en la cúspide de la piramide documental de la seguridad de información.

Imagen tomada de: http://mindfulsecurity.com/wp-content/uploads/2009/02/framework.jpg

La política de la seguridad de la informaciónal ser una declaración de alto nivel relacionado con la protección de los activos de información que soportan los procesos de la entidad [6], tiene la opción de ser formalizada en un documento que involucre el contexto,

objetivos, alcance definición de políticas y responsabilidades, cumplimiento, mecanismos de difusión y revisión de las políticas; esta estructura permite tener la integralidad en la definición de la política, ademas ser un control como se define en la ISO 27002:2013 Seccion 5.1.1 Documento de politicas de seguridad de la información.

4. METODOLOGÍA

La metodología a usar en el desarrollo de este proyecto describe las fases de: Identificación, planeación, diseño y socialización que cumpla con el objetivo general del proyecto y teniendo en cuenta el marco de referencia la norma ISO/IEC 27001 del gobierno el línea.

Esta metodología pretende dar cumplimiento a los objetivos específicos propuestos, donde se definen los entregables como productos para el desarrollo del proyecto; que cubra el alcance general como son las áreas de: Facturación, SIAU, contabilidad, Estadística y Gerencia, donde se diseñaran las políticas de seguridad de la entidad.

Para el desarrollo de la metodología se describen las actividades a realizar en cada una de las fases con su entregable:

- **Identificacion**: En esta fase se realizara la identificación y se hará una estadística del análisis de las vulnerabilidades, amenazas, que afectan la información de las áreas de: Facturación, SIAU, contabilidad, Estadística y Gerencia. Posteriormente se identificaran el personal encargado de cada una de las áreas y los permisos que tienen para gestionar la información; los procesos que serán involucrados en cada área y además del conocimiento de personal externo y el tipo de información al que tiene acceso.

Entregable: Documento con el diagnóstico sobre la situación actual de la empresa con respecto al aseguramiento de la información de las áreas de: Facturación, SIAU, contabilidad, Estadística y Gerencia.

- **Planeación**: En Esta fase se realizara de acuerdo al resultado del análisis un bosquejo de las políticas de seguridad a las amenazas de alto nivel identificadas que nos permitan asegurar la información en las áreas, especificando el alcance, contexto, cumplimiento y responsables.

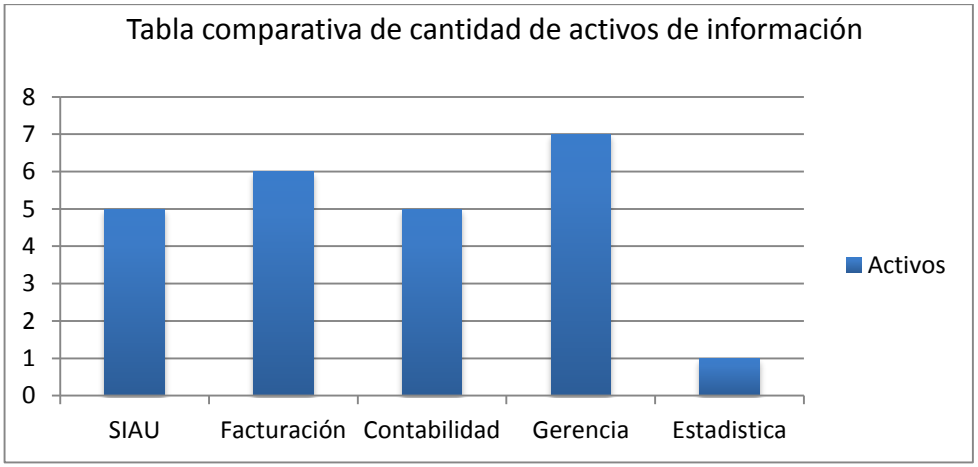
- **Diseño**: En esta fase se diseñaran las políticas de seguridad de acuerdo a la estrategia gobierno en línea según el formato de implementación de políticas de seguridad y privacidad de la información emanado del Ministerio de las Tecnologías de la Información y la Comunicación, que está conforme a la norma técnica colombiana NTC ISO /IEC 27001:2013.

Entregable: Formato Declaración de políticas de seguridad de la empresa social del estado hospital integrado san Antonio de puente nacional Santander.

5. RESULTADOS Y DISCUSIÓN

La generación de políticas de seguridad de información a través de la metodología propuesta inició con la recolección de información para ello se uso el manual de procedimientos de la empresa social de estado hospital integrado San Antonio de Puente Nacional donde se ilustra de manera formal cada uno de los pasos para completar un procedimiento en cada área entre ellas las áreas SIAU (Sistema de Información y Atención al Usuario), contabilidad, estadística, facturación, gerencia; incluidas en la declaración de políticas de seguridad de la información.

Con un análisis de los procedimientos descritos en el manual de procedimientos, además de observación directa en cada área, se identifican inicialmente los activos de información, posteriormente, con visita de campo a cada una de las áreas, se identificaron los actores involucrados.



Fuente: propia

Con este insumo se procede a identificar las vulnerabilidades y amenazas encontradas[1] en la áreas, dicho insumo esta anexo en el presente trabajo.

De acuerdo a los riesgos encontrados en las áreas del hospital se procede a implementar el uso de controles como son las políticas de seguridad que ayuden a la mitigación de esos riesgos y se garantiza la continuidad en la prestación de los servicios.

Además el diagnóstico permito detectar los riesgos asociados logrando determinar el estado actual de la empresa social del estado hospital integrado San Antonio de Puente Nacional a través de las incidencias encontradas, anexadas al presente trabajo.

Se diseñaron las políticas de seguridad de la información basado tanto en el estado actual como en el modelo de seguridad adoptado por el gobierno en línea como estrategia de aseguramiento sustentado en norma ISO/IEC 27001, apuntado a mitigar los riesgos, cubriendo las áreas especificadas de manera integral.

El diseño de las políticas tuvo en cuenta el formato sugerido en el modelo de seguridad vigente del ministerio de las tecnologías de la información y comunicaciones, además del diseño de políticas específicas para cada área según los riesgos asociados.

[1] Basado en lista de amenazas del documento Magerit v3 Libro 2 Catalogo de Elementos Capítulo 5, Pag 25, disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

6. CONCLUSIONES

Se realizó un análisis del estado actual de la empresa Social Del Estado Hospital San Antonio de Puente Nacional Santander, donde se identificaron los activos de información con su descripción, los actores involucrados en las áreas de: Facturación, SIAU, contabilidad, Estadística y Gerencia

Posteriormente al análisis del estado actual de la empresa se generó un documento con las incidencias encontradas donde se describieron las vulnerabilidades, amenazas y riesgos a que los activos se exponen en las áreas.

De acuerdo al documento con el diagnóstico del estado actual de la empresa se planearon y diseñaron las políticas de seguridad basándonos en las plantillas y siguiendo los lineamientos del Gobierno en línea (GEL 3.1).

7. BIBLIOGRAFÍA

[1] Código de prácticas para los controles de seguridad de la información, Términos y definiciones. ISO/IEC 27002.2013, p 8.

[2] Ministerio de tecnologías de la información y las comunicaciones (2015). Controles de Seguridad. [En línea]. Disponible en: http://www.mintic.gov.co/gestionti/615/articles-5482_Controles.pdf

[3] Michael E. Withman (2003, Ago.) Enemy at the gate: Threats to information security. ACM Digital Library [En línea]. 46(8).Disponible WWW: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.197.1883&rep=rep1&type=pdf

[4] Ministerio de tecnologías de la información y las comunicaciones (2015). Modelo de Seguridad. [En línea]. Disponible en: http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf

[5] Gestión de la seguridad de la información en sanidad usando la norma ISO/IEC 27002. UNE-EN ISO 27799. 2010

[6] Ministerio de tecnologías de la información y las comunicaciones. (2015). Modelos de seguridad. MinTic. [En línea]. Disponible en: http://www.mintic.gov.co/gestionti/615/articles-5482_Implementacion_politicas.pdf

[7] Michael McNikle, "Five Security vulnerabilities could mean trouble". Healtcare IT News. US. Reporte http://www.healthcareitnews.com/news/5-security-vulnerabilities-could-mean-trouble , Ago. 9, 2012

[8] Department of Health Goverment of Western Australia. (2012). Information Security Policy.[En línea]. Disponible: http://www.health.wa.gov.au/circularsnew/ attachments/697.pdf

8. ANEXOS

DIAGNOSTICO DE LA EMPRESA SOCIAL DEL ESTADO HOSPITAL INTEGRADO SAN ANTONIO PUENTE NACIONAL SDER.

El diagnóstico de esta empresa nos permitirá la implementación de controles que ayuden a mitigar los riesgos a que se expone el hospital. A continuación relacionaremos los activos de la empresa por áreas, sus amenazas y vulnerabilidades que se presentan.

ACTIVOS DE LA EMPRESA

La identificación de los activos con su respectiva valoración para el Hospital es importante ya que permite identificar y valorar las amenazas y vulnerabilidades a las que están expuestos dichos activos.

ElHospital Integrado San Antonio maneja una gran cantidad de activos importantes que hacen el buencumplimiento de sus funciones. Para este caso identificaremos los activos de las áreas como:Facturación, SIAU, contabilidad, Estadística y Gerencia.

- **Aplicaciones Software**: Hace referencia a las aplicaciones que el Hospital San Antonio De Puente Nacional maneja para el desarrollo de sus funciones para este caso lo realizaremos sobre la plataforma **ASIS Y GD** donde se realiza la administración y ejecución presupuestal.
- **Servicios**: Hace referencia a los servicios que el Hospital ofrece y para este caso nos ubicaremos sobres las áreas de: Facturación, SIAU, contabilidad, Estadística y Gerencia.

9. DESCRIPCIÓN DE LOS ACTIVOS DE LAS ÁREAS HOSPITAL**:**

AREA	ACTIVOS	DESCRIPCION
FACTURACION	Facturas.	Hace referencia al comprobante que se entrega al paciente por la prestación del servicio.
	Remisiones	Formato que contiene la aprobación del traslado de pacientes según ordene la EPS
	Orden de servicios médicos ambulatorios.	Formato donde se registran los procedimientos ordenados por el médico y que se realicen en la misma entidad.
	Ordenes De remisión.	Formato que legaliza la remisión del paciente.
	Formulas Médicas.	Formato que expide el medico con el diagnostico emitido al paciente.
	Cartera	Informes que describen los recaudados por el área de Facturación semanalmente donde se evidencia cuentas por cobrar a las EPS con las que tiene convenio, y la facturación que se realiza diariamente.
SIAU **(**Sistema De Información Y Atención Al Usuario**)**	Citas Medicas	Formato donde se registra los pacientes para asignar citas médicas, posteriormente se imprime la ficha que se entrega al paciente para presentarlo al médico y pueda ser atendido. .
	Afiliaciones	Hoja de verificación que se realiza en el sistema para constatar que un paciente está afiliado al Sistema General En Salud.
	Programador de Médicos	Formato que contiene la disponibilidad de los médicos semanalmente, para ser programados en las áreas de consulta externa y urgencias.
	Informe a EPS	Formato donde se diligencia la cantidad de pacientes que cumplieron con la prestación del servicio por parte del hospital a sus respectivas EPS.
	PQR	El documento que contiene la sugerencia o queja por parte de algún usuario.
	Contratos	Documento que contiene la minuta para la contratación.

CONTABILIDAD	Nomina	Documento queContiene los datos de los empleados referentes a los pagos que se realizan mensualmente.
	Cartera	Documentoque contiene las cuentas por pagar que tiene la empresa a proveedores y funcionarios. .
	Listado Proveedores	Documento que detalla los listados de los proveedores.
	Cuentas por Cobrar.	Documento que detalla las cuentas por cobrar a las diferentes EPS.
ESTADISTICA	Historias Clínicas	Este activo permite registrar las historias clínicas de los pacientes, es administrado por 1 funcionario de planta. Este activo es requerido frecuentemente por los médicos O por órdenes judiciales en procesos legales.
GERENCIA	Firma Digital.	Este activo permite que se garantice la integridad, confidencialidad y el no repudio de los informes que son remitidos ante la secretaria de salud del departamento.
	Informe De Rendición de Cuentas	Informe que contiene el registro de lo ejecutado.
	Listado De Proveedores	Documento con el listado de los proveedores.
	Listado De Cuentas Por Cobrar Y Por Pagar	Documento que contiene las cuentas por pagar y por cobrar de la entidad.
	Contratos	Formato donde se describe la minuta a cada empleado, posteriormente redactado, aprobado por la gerencia y firmado por el funcionario; es firmado digitalmente.
	Listado De Servicios Prestados	Portafolio de servicios que presta la entidad.
	Presupuesto General Del Año.	Documento que detalla el listado de presupuesto general del hospital.

Actores involucrados en las Áreas:

AREA	ACTORES
FACTURACION	3 Funcionarios. Control Interno. Pacientes. EPS Médicos Jefes de Enfermería.
SIAU **(**Sistema De Información Y Atención Al Usuario**)**	Asesor de citas Pacientes. Control Interno. EPS Médicos.
CONTABILIDAD	Contador. Auxiliar Contable. Pacientes. Proveedores. Gerente Subgerente.
ESTADISTICA:	Funcionario de planta Médicos. Subgerente
GERENCIA	Gerente Clientes Externos Proveedores Personal Administrativo y funcionarios EPS.

Amenazas: La amenazas que los activos se exponen se relacionan una vez se hallan detectado los activos realmente importantes y relevantes para el desarrollo delproyecto.

Vulnerabilidades: Una vulnerabilidad se define en este método de Gestión del Riesgo, como un estado de debilidad oincapacidad para resistir un fenómeno amenazante y que al ser explotado afecta el estado de losactivos del proyecto, dicho en otras palabras es la potencialidad o 'cercanía' previsible de lamaterialización de la Amenaza en Agresión.

A continuación registramos las amenazas y vulnerabilidades a los que los activos se exponen en la gestión de los procesos.

AREA	AMENAZAS	VULNERABILIDADES
FACTURACION	1. Alteración en la facturación, formulas medicas 2. Acceso no autorizado al registro de la cartera, remisiones y órdenes de remisión. 3. Daño físico a equipos donde reposa Los archivos. 4. Espionaje 5. Ausencia de respaldo de los datos donde reposan los archivos. 6. Divulgación no autorizada. 7. Falla en la red interna que afecte la prestación del servicio. 8. Robo de facturas	1. Deficiencia en el control de cambios en la facturación. 2. Deficiencia en los controles de acceso al sistema 3. Carencia de planes de mantenimiento a los equipos. 4. Deficiencia en los controles de seguridad física de la empresa. 5. Desconocimiento del proceso para realizar Backus. 6. Deficiencia en los contratos de acuerdos de confidencialidad para el manejo de la información confidencial. 7. Deficiencia en Políticas de seguridad para Planes de mantenimiento a la red que garantice la continuidad del negocio. 8. Ausencia o desconocimiento de políticas de seguridad de la información.
SIAU **(**Sistema De	1. Ingeniería social	1. Ausencia de políticas, en los procedimientos y/o directrices de

Información Y Atención Al Usuario**)**	2. Uso inadecuado de la documentación en la programación de citas, Informes de EPS, afiliaciones y PQR. 3. Ataques contra el software. 4. Ausencia de copias de respaldo.	seguridad de la información. 2. Acceso no controlado sobre la información confidencial 3. Software Antivirus desactualizado 4. Desconocimiento del proceso para realizar Backus
CONTABILIDAD .	1. Código malicioso que afecte la nómina. 2. Falla en la red interna que afecte la contratación. 3. Divulgación no autorizada de la información para contratación. 4. Inactividad del servicio de energía. 5. Acceso no controlado al sistema donde reposan los activos de: cartera, cuentas por cobrar, nómina y cuentas por cobrar.	1. Deficiencia de actualizaciones del sistema operativo y antivirus. 2. Deficiencia en Políticas de seguridad para Planes de mantenimiento a la red que garantice la continuidad del negocio. 3. Deficiencia en las políticas de seguridad de los contratos de acuerdos de confidencialidad para el manejo de la información confidencial 4. Cortes del servicio eléctrico 5. Deficiencia en las políticas de seguridad para el manejo de Usuarios y contraseñas con nivel mínimo de caracteres.

ESTADISTICA	1. Hurto de información. 2. Manipulación errónea de la administración de las historias clínicas. 3. Confidencialidad y seguridad de los documentos.	1. Ausencia del procedimiento para la autorización de la información disponible al público. 2. Deficiencia en las políticas de seguridad para el manejo de control de modificaciones al archivo. 3. Ausencia o desconocimiento de políticas de seguridad en la información.
GERENCIA	1. Incumplimiento de políticas o procesos internos para la rendición de cuentas. 2. Acceso no controlado al sistema donde reposa el activo firma digital. 3. Confidencialidad de los documentos propios de la empresa. 4. Trafico de influencias para la contratación. 5. Incumplimiento en los servicios ofertados. 6. Desvío de dineros del POA anual de la entidad.	. 1. Deficiencia en el presupuesto para el próximo año. 2. Deficiencia en las políticas de seguridad para el manejo de Usuarios y contraseñas con nivel mínimo de caracteres. 3. Ausencia de políticas, en los procedimientos y/o directrices de seguridad de la información 4. Mala prestación de los servicios de salud 5. Ofertar servicios no contemplados en el portafolio 6. Deficiencia en los controles de políticas para el área de control interno.

De acuerdo alos activos descritos anteriormente se exponen alos siguientes riesgos que impiden prestación de un buen servicio. Lo que se buscara es mitigarlos haciendo uso de los controles como políticas de seguridad.

Riegos Asociados a estos activos:

1) Alteración de la integridad de los datos debido a las amenazas en los equipos.
2) Indisponibilidad de la información debido a la inactividad del servicio.
3) Pérdida de la información debido a errores en los sistemas de respaldo.
4) Acceso no autorizado al sistema debido a la deficiencia en los controles de acceso al sistema.
5) Fuga de información confidencial en la contratación.
6) Indisponibilidad presupuestal debido a la ausencia de entrega de los informes anuales.
7) Baja demanda para la oferta del servicio debido al desconocimiento, interés o afinidad por parte de la población.
8) Falta de personal profesional debido al tráfico de influencias.

De acuerdo a la descripción de los activos, las amenazas, vulnerabilidades y riesgos descritos anteriormente relacionamos las incidencias que se presentan en el hospital en cada una de las áreas como son: Facturación, SIAU, contabilidad, Estadística y Gerencia.

AREA	DESCRIPCION
FACTURACION	• Los computadores son compartidos por parte de los 3 funcionarios para la realización de las labores.

	• Las contraseñas son compartidas para el ingreso a los computadores. • Dejan el sistema abierto al momento de ausentarse de la oficina. • La oficina no cuenta con una puerta de seguridad que permita tener control sobre las personas que ingresan, lo que hace que ingrese personal a esta área sin ningún control. • El sistema es gestionado por las 3 personas lo que hace poner en riesgo la integridad de la información. • La información confidencial de esta área es divulgada entre los funcionarios.
SIAU **(**Sistema De Información Y Atención Al Usuario**)**	• No se cuenta con una oficina adecuada para la prestación del servicio lo que poner en riesgo la perdida de los activos físicos. • EL equipo de cómputo no cuenta con seguridad de acceso lo que hace que cualquier funcionario tenga acceso al sistema. • Divulgue informes de los convenios con las EPS. • Se han perdido los documentos de PQR. • Desinformación en la programación de citas médicas.
CONTABILIDAD .	• Se ha divulgado información de contratación tanto con proveedores con personal interno. • La información en algunas situaciones se ha compartido a usuarios de otras dependencias.

	• Se ha divulgado las cuentas por pagar que tiene la empresa con los proveedores. • Se presentaron perdidas de facturas y eliminación de registros en el sistema de información.
ESTADISTICA	• .Se ha tenido acceso no autorizado de personal de la entidad a esta área. • Se han entregado historias clínicas a familiares de pacientes por parte de personal no autorizado de la empresa. • El computador que se encuentra en esta área no tiene ningún tipo de protección físico ni de acceso al sistema. • Debido al cambio de personal frecuentemente se ha puesto en riesgo los archivos de historias clínicas.
GERENCIA	• Delegan funciones para el proceso de la firma digital. • Se ha divulgado información confidencial en temas de rendición de cuentas. • Se ha presentado en algunas situaciones el tráfico de influencias para beneficiar a terceros. • Se han presentado demoras en la presentación de informes ante la secretaria de salud. • Se ha delegado a un solo funcionario las gestiones para la rendición de informes, y la verificación de los mismos. • Se han firmado contratos a personal que no tiene vínculos con la entidad y son ejecutados por

	personal que ya no laboran en el entidad. • La confidencialidad de usuarios y contraseñas es entregada a 1 solo funcionario sin un respaldo que garantice la honestidad, integridad, confidencialidad de la información.

DECLARACION POLITICAS DE SEGURIDAD DE LA EMPRESA SOCIAL DEL ESTADO HOSPITAL INTEGRADO SAN ANTONIO DE PUENTE NACIONAL

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de la empresa social del estado hospital integrado San Antonio de Puente Nacional con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

La empresa social del estado hospital integrado San Antonio de Puente Nacional, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionalesde la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicants y clientes de la empresa social del estado hospital integrado San Antonio de Puente Nacional

- Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad

Esta política aplica a las areas de gerencia, SIAU, facturación, estadistica y contabilidad a sus funcionarios, contratistas y terceros de la empresa social del estado hospital integrado San Antonio de Puente Nacional y la ciudadanía en general.

Nivel de cumplimiento

Todas las personascubiertas por el alcance y aplicabilidad deberán dar cumplimientoun 100% de la política.

Politicas Generales:

A continuación se establecen las 12 políticas de seguridad que soportan el SGSI de la empresa social del estado hospital integrado San Antonio de Puente Nacional:

- La empresa social del estado hospital integrado San Antonio de Puente Nacional ha decidido **definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatoriosque le aplican a su naturaleza.
- Las **responsabilidades**frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de **los empleados, contratistaso terceros**.
- La empresa social del estado hospital integrado San Antonio de Puente Nacional **protegerá la información**generada, procesada o resguardada por los procesos de negocioy activos de información que hacen parte de los mismos.
- La empresa social del estado hospital integrado San Antonio de Puente Nacional protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- La empresa social del estado hospital integrado San Antonio de Puente Nacional protegerá su informaciónde las amenazas originadas por parte del personal.
- La empresa social del estado hospital integrado San Antonio de Puente Nacional **protegerá las instalaciones** de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La empresa social del estado hospital integrado San Antonio de Puente Nacional **controlará la operación** de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La empresa social del estado hospital integrado San Antonio de Puente Nacional **implementará control de acceso** a la información, sistemas y recursos de red.
- La empresa social del estado hospital integrado San Antonio de Puente Nacional garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La empresa social del estado hospital integrado San Antonio de Puente Nacional garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La empresa social del estado hospital integrado San Antonio de Puente Nacional **garantizará la disponibilidad** de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
- La empresa social del estado hospital integrado San Antonio de Puente Nacional garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

Politicas específicas del area de Facturación

- El personal que labora en el área de facturación de la empresa social del estado hospital integrado San Antonio de Puente Nacional protegerá la integridad de la información contenida en los documentos soportes de de facturación (factura, recibo de pago, liquidación del servicio) implementando hash visible conforme al estándar ISO/IEC 18004.
- El personal que labora en el área de facturación de la empresa social del estado hospital integrado San Antonio de Puente Nacional garantizará la integridad y disponibilidad de las facturas para servicios POS, NO POS y SOAT correspondientes al nivel 1 del hospital que se encuentren transitando dentro del área.
- El personal que labora en el área de facturación de la empresa social del estado hospital integrado San Antonio de Puente Nacional garantizará la integridad y disponibilidad de los comprobantes de recibo de pago del usuario que se encuentren transitando dentro del área.
- El persona que labora en el área de facturación de la empresa social del estado hospital integrado San Antonio de Puente Nacional garantizará la integridad y disponibilidad de la fórmula o receta médica en tránsito dentro del área.
- El personal que labora en el área de facturación de la empresa social del estado hospital integrado San Antonio de Puente Nacional garantizará la integridad y disponibilidad de las ordenes de servicios médicos que se encuentren transitando dentro del área.
- El persona que labora en el área de facturación de la empresa social del estado hospital integrado San Antonio de Puente Nacional controlará la confidencialidad de los documentos manejados internamente y que esten en tránsito de personal ajeno a los destinatarios de los documentos.

Políticas específicas del área de SIAU

- El personalque labora en el área de SIAU de la empresa social del estado hospital integrado San Antonio de Puente Nacional propenderá por la integridad y disponibilidad de la sugerencias que esten en el buzón de sugerencias y en tránsito.
- El personal que labora en el área de SIAU de la empresa social del estado hospital integrado San Antonio de Puente Nacional garantizara la integridad, la confidencialidad, disponibilidad y el no repudio de las PQR radicadas por los usuarios desde la recepción hasta la respuesta.

Políticas específicas del área de contabilidad

- El persona que labora en el área de contabilidad de la empresa social del estado hospital integrado San Antonio de Puente Nacional controlará la confidencialidad de las información contable manejada internamente de personal ajeno a los destinatarios designados por ley.
- El personal que labora en el área de Contabilidad de la empresa social del estado hospital integrado San Antonio de Puente Nacional garantizará la integridad y disponibilidad de la información contenido en los estados financieros de la empresa.
- El personal que labora en el área de Contabilidad de la empresa social del estado hospital integrado San Antonio de Puente Nacional garantizará que la integridad y disponibilidad de información de cartera con las EPS con las que el hospital tiene convenio.
- El personal que labora en el área de Contabilidad de la empresa social de estado hospital integrado San Antonio de Puente Nacional propenderá por la disponibilidad e integridad de la información de las cuentas por pagar de la empresa.

Políticas específicas de Estadística

- El personal que labora en el área de Estadística de la empresa social del estado hospital integrado San Antonio de Puente Nacional garantizará la confidencialidad, integridad, disponibilidad y no repudio de la información contenida en las historias clínicas de los pacientes del hospital.

- El personal que labora en el área de Estadística de la empresa social del estado hospital integrado San Antonio de Puente Nacional garantizará la confidencialidad, integridad, disponibilidad y no repudio de la información consignada en la epicrisis de los pacientes del hospital.
- El personal que labora en el área de Estadística de la empresa social del estado hospital integrado San Antonio de Puente Nacional controlará el acceso de la información generado sobre los índices de morbilidad y mortalidad.
- El personal que labora en el área de Estadística de la empresa social del estado hospital integrado San Antonio de Puente Nacional propenderá por el acceso autenticado y trazable a personal misional del hospitalque requiera disponibilidad de la información contenida en las historias clínicas para iniciar transito circular dentro de las áreas

Políticas específicas de Gerencia

- La Gerencia de la empresa social del estado hospital integrado San Antonio de Puente Nacional haciendo uso de las facultades otorgadas por la junta directiva adaptará un sitio alineado con la norma ISO 30301 paragarantizar la disponibilidad y el control de acceso al archivo físico solo a personal autorizado mediante acta.
- La Gerencia de la empresa social del estado hospital integrado San Antonio de Puente Nacional garantizará la integridad, confidencialidad y disponibilidad de la información contenida en los convenios legalizados ysuscritos por el hospital.
- La Gerencia de la empresa social del estado hospital integrado San Antonio de Puente Nacional garantizará la integridad, disponibilidad de la información contenido en el plan de acción para lograr objetivamente las metas del periodo fiscal.
- La Gerencia de la empresa social del estado hospital integrado San Antonio de Puente Nacional garantizar la integridad, disponibilidad, confidencialidad y no repudio de los actos administrativos

Roles y responsabilidades

- La gerencia es responsable impulsar la implementación y el cumplimiento de la presente política.
- El personal del área de facturación, contabilidad es responsable del buen uso de los sistema de información existentes para gestión de la información que incluye la administración (acceso, copias de seguridad) relacionada con dichas áreas.
- El personal del área de SIAU y Estadística es responsable custudiar la documentación que contenga información relacionadas con las funciones de dichas áreas que fluyan por estas oficinas.

Revisión de la política

La gerencia deberá revisar periodicamente las políticas de seguridad de la información cada 4 años o el mismo periodo del mandato del gobernador actual, además de reforzarlas, sin perjuicio de actualizarlas respondiendo a las necesidades que surjan en el desarrollo de los objetivos del hospital.

Difusión de la politica

La presente política sera difundida en la cartelera interna del hospital y en las sesiones de sensibilizacion anuales programadas por la gerencia.

Incumplimiento de la política

El incumplimiento de la presente política conllevará a la aplicación de las sanciones dentro del marco del régimen disciplinario para empresas públicas del sector salud o el régimen superior de acuerdo a la magnitud del incumplimiento.