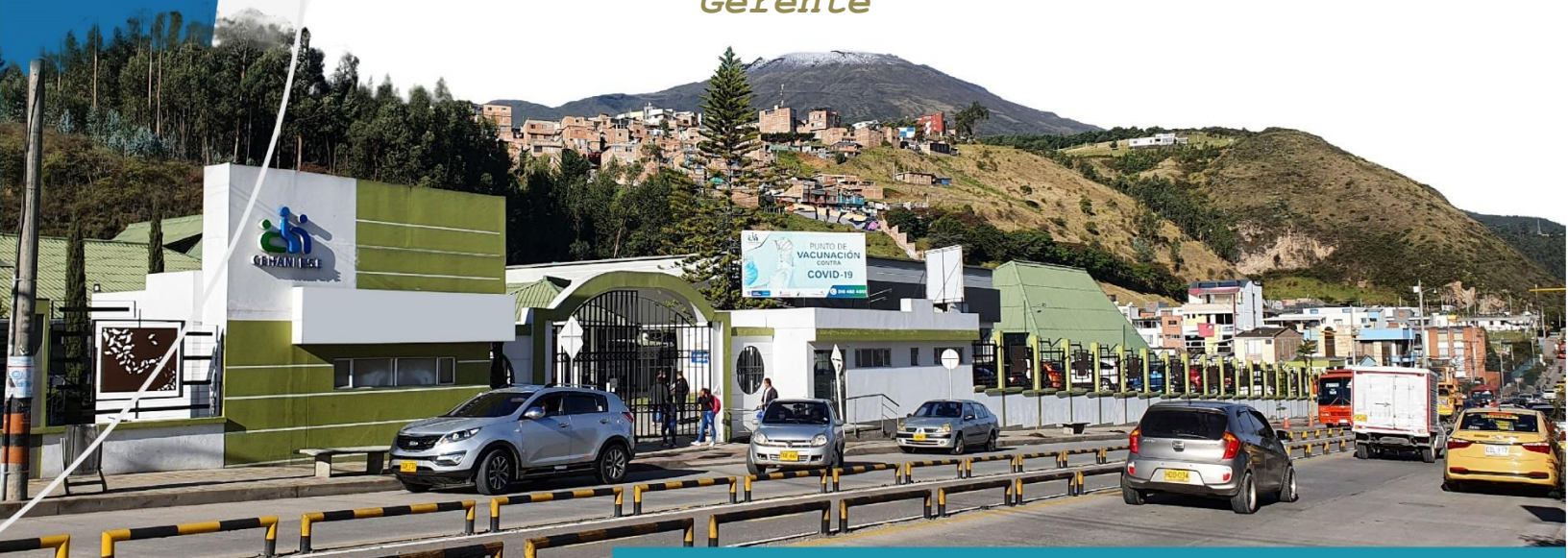
TR-CO16.00230

CEHANI E.S.E.

VIGILADO Supersalud

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – CEHANI ESE

Arley Realpe Chamorro
Gerente



Centro Integral de Atención Especializada

COPIA CONTROLADA

No.
COPIA

COPIA NO CONTROLADA

CICLO DE EVALUACIÓN Y MEJORAMIENTO			
REVISIÓN	**FECHA**	**DESCRIPCIÓN DE LA MODIFICACIÓN**	**MEJORAMIENTO**
Revisión del documento	Enero de 2020	Se actualizó el cronograma para la vigencia 2020.	Mejoramiento continuo
Revisión del documento	Junio de 2021	Se articula documento con la Guía básica de riesgos y oportunidades GU-CDG-001, Procedimiento de Gestión de riesgos y oportunidades PR-CDG-003 y Matriz de riesgos y oportunidades MA-CDG-003	Mejoramiento Continuo
Revisión del documento	Enero de 2022	Se actualiza nombres de procesos y oficinas en el documento para la vigencia 2022	Mejoramiento continuo
Revisión del documento	Enero de 2023	Se ajustan los códigos de los documentos referenciados	Mejoramiento continuo
Revisión del documento	Enero de 2024	En el Numeral 3.1 FASE 1: Planeación para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información (Definición de Estrategias) se actualizan las referencias de los documentos MA-SIG-007 por MA-GSI-002, se actualiza el numeral 4. Cronograma y el 5. Presupuesto.	Mejoramiento continuo

INTRODUCCIÓN

Uno de los objetivos del Sistema de Gestión de la Seguridad y Privacidad de la Información en las entidades es garantizar que los riesgos asociados a la seguridad de la información sean conocidos, gestionados y tratados por la Entidad y además de que estos deben quedar soportados en un documento, para que sea un ejercicio de gestión, sistemático, estructurado, repetible y eficiente, en este orden de ideas es fundamental que la entidad identifique y valore los riesgos que pueden afectar la seguridad y privacidad de la información y por consiguiente establecer los mecanismos más convenientes para darle protección.

La información que genera constantemente el CEHANI E.S.E. es crucial para su correcto desempeño y cumplimiento de los objetivos organizacionales, es por ello que la seguridad y privacidad de la información se convierte en prioridad para evitar cualquier posibilidad de ataque a la integridad, disponibilidad y/o confidencialidad entre otros eventos, los cuales pueden incidir en el normal funcionamiento y por ende redundar en la prestación de los servicios de salud.

Teniendo en cuenta lo anterior y tal como lo establece el Modelo de Seguridad y Privacidad de la información –MSPI del Min Tic, un tema decisivo, es la Gestión de riesgos asociados a la seguridad y privacidad de la información, la cual puede ser utilizada para la toma de decisiones en todos los niveles.

Es importante resaltar que para la evaluación de riesgos en seguridad y privacidad de la información un insumo vital es la clasificación de activos de información ya que una buena práctica es realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA dependiendo de los criterios de clasificación que se describirán en el presente plan.

1. OBJETIVOS

1.1. General

Definir un marco regulatorio interno que permita identificar, medir, controlar, monitorear y comunicar los riesgos asociados a la seguridad y privacidad de la información y que puedan afectar el cumplimiento de los objetivos estratégicos, minimizando las pérdidas para la entidad.

1.2. Específicos

Establecer los lineamientos y principios que lleven a la unificación de criterios para la gestión adecuada de los riesgos de seguridad y privacidad de la información.

Fortalecer el sistema de gestión de riesgos de la Entidad incorporando controles y medidas para la seguridad y privacidad de la información.

Contribuir para que se minimice la posibilidad de que un evento produzca determinado impacto bien sea en la información o cualquier otro activo de información asociado, a través de la gestión adecuada de los riesgos de la seguridad y privacidad de la información.

Dar pautas para que la implementación de controles sea adecuada y que el nivel de probabilidad e impacto se encuentren en niveles aceptables para la entidad.

2. CONCEPTOS BÁSICOS

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

Activo de Información: Se considera principalmente a cualquier conjunto de datos creado o utilizado por un proceso de la organización, así como el hardware y el software utilizado para su procesamiento o almacenamiento, los servicios utilizados para su transmisión o recepción y las herramientas y/o utilidades para el desarrollo y soporte de sistemas de información. En casos particulares, se puede considerar como un activo de información a personas que manejen datos, transacciones o un conocimiento específico muy importante para la organización.

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Confidencialidad: La confidencialidad es la garantía de que la información será protegida para que no sea divulgada sin consentimiento de la persona. Dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso a ésta información. Cada individuo tiene derecho a proteger su información personal.

Consecuencia: Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Disponibilidad: Una vez que la información ha sido capturada en un sistema de cómputo, debe ser almacenada de manera segura y estar disponible para los usuarios cuando la necesiten. La información también debe ser mantenida y utilizada de tal forma que su integridad no se vea comprometida.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del Riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Integridad: Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. Es decir, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

Riesgo de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la

soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo. Aceptación de la pérdida o ganancia proveniente de un riesgo particular

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación de los controles de seguridad de la información sobre cada uno de los procesos.
Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información.

3. PROCESO DE GESTIÓN DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

3.1. FASE 1: Planeación para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información (Definición de Estrategias)

Para el desarrollo de esta fase se aplican básicamente la Guía básica para la administración de riesgos y oportunidades GU-SIG-007 y el procedimiento Gestión de riesgos y oportunidades PR-SIG-013, los pasos 1,2 y 3 de la guía para la Administración de los Riesgo de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, emitida por la Función Pública, lo que implica las siguientes actividades con las cuales se busca profundizar en lo concerniente a riesgos de seguridad digital.

El adecuado manejo de los riesgos favorece el desarrollo y crecimiento de la entidad, con el fin de asegurar dicho manejo es importante que se establezca el entorno y ambiente organizacional de la entidad, la identificación, análisis, valoración y definición de las alternativas de acciones de mitigación de los riesgos, esto en desarrollo de los siguientes elementos:

- Contexto estratégico – MA-DRE-003
- Identificación de riesgos y oportunidades – MA-GSI-002
- Análisis de riesgos y oportunidades – MA-GSI-002
- Valoración de riesgos - MA-GSI-002

a. Alcance

El tratamiento de riesgos asociados a la Seguridad y Privacidad de la Información es extensible y aplicable a todos los procesos de la entidad por tratarse de riesgos transversales y que se enmarcarán dentro de los criterios del Modelo de Seguridad y Privacidad de la Información, que es el habilitador, en materia de seguridad digital, de la Estrategia de Gobierno Digital expedida por el MINTIC.

b. Política de tratamiento de riesgos de seguridad y privacidad de la información

En este aspecto la entidad cuenta con la Política de Riesgos DI-DRE-012, de una manera integral, más, sin embargo, no incluye el compromiso para la gestión de riesgos de seguridad y privacidad de la información en todos los niveles.

c. Roles y responsabilidades

La entidad cuenta con la Matriz de roles, responsabilidades y autoridades del sistema integrado de gestión MA-DRE-005, el cual se encuentra enfocado hacia el Sistema de Sistemas Integrados de gestión, Sistema de Gestión Ambiental y Sistema de Gestión de Seguridad y Salud en el trabajo. Para que el mismo se enfoque hacia el Sistema de Gestión de Seguridad de la información debe delegar la responsabilidad en una persona o funcionario que haga parte de la línea estratégica o de la alta dirección, quien tendrá como responsabilidades las siguientes:

- Definir el procedimiento para la Identificación y Valoración de Activos.
- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
- Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
- Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

Es importante tener presente la Guía 4: Roles y responsabilidades definida por el MSPI y que hace parte de la política Gobierno Digital para complementar el tema anterior.

d. Asignación de recursos:

La entidad debe disponer de los recursos suficientes para el tratamiento de riesgos de seguridad y privacidad de la información, estos recursos requeridos son capital, tiempo, personal, procesos, sistemas y tecnologías, con el fin de apoyar a los responsables en la implementación de controles y seguimiento de los riesgos.

e. Identificación de activos de seguridad y privacidad de la información

Para la entidad un activo es cualquier elemento que tenga valor, pero aplicado al contexto de seguridad y privacidad de la información hace referencia a elementos tales como aplicaciones de la entidad, servicios Web, redes, información física o digital, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO que utiliza la organización para su funcionamiento.

Establecer este inventario de activos de información es importante ya que así se podrá saber lo que se debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, lo que redundará en el aumento de su confianza en el uso del entorno digital.

Para la entidad es importante determinar los riesgos asociados a seguridad y confidencialidad de la información por tanto se realizó valoración de activos de información de manera generalizada desde la Primera Línea de Defensa – Líderes de Proceso.

Para la generación de este inventario, la entidad pública debe tener en cuenta los siguientes pasos:

Paso 1: Listar los activos de información por cada proceso

Proceso	Nombre del activo	Descripción/Observaciones	Tipo	Ubicación
GSI	COMPUCONTA	ALMACENAMIENTO DE LA INFORMACIÓN ASISTENCIAL Y ADMINISTRATIVA	Software	SERVIDORES BASE DE DATOS
GSI	SALUDIPS	ALMACENAMIENTO DE LA INFORMACIÓN ASISTENCIAL Y ADMINISTRATIVA	Software	SERVIDORES BASE DE DATOS
SIG	DOCUMENTOS SISTEMA GESTIÓN INSTITUCIONAL	DOCUMENTOS Y FORMATOS DEL SIG	Información	SERVIDOR 172.20.1.248/Sistema Gestión Institucional

GJUC	CONTRATOS	Contratos Institucionales	Información	SERVIDOR 172.20.1.248/Jurídica 2019
ACME	ACME	Información relacionada con enfermedades huérfanas	Información	SERVIDOR 172.20.1.248/Acme
ASF	Actas entrega de medicamentos	Información relacionada las entregas de medicamentos	Información	SERVIDOR 172.20.1.248/Actas entrega de medicamentos
ASF	Actas de inicio de medicamentos	Información relacionada con los contratos de inicio de entrega de medicamentos	Información	SERVIDOR 172.20.1.248/Actas -inicio - medicamentos
GTH	Gestión Humana	Información relacionada con el proceso GTH	Información	SERVIDOR 172.20.1.248/Compartida2/ Gestión Humana
ATU	GPSA- GAR	Información relacionada con el proceso ATU	Información	SERVIDOR 172.20.1.248/GPSA-GAR
ACME	Estadística - 2018	Información relacionada con el proceso ACME	Información	SERVIDOR \\172.20.1.248\estadistica 2018
GFI- ASF	Facturacion farmacia	Información relacionada con el proceso de facturación en farmacia	Información	SERVIDOR \\172.20.1.248\facturacion-farmacia
GFI- ASF	Radicados 2021	Información relacionada con el proceso de facturación en farmacia	Información	SERVIDOR \\172.20.1.248\radicados2021
GAFT	almacen@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
ADI	Ayudasdiagnosticas@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
SIG	calidad@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
GFI	cartera@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
DRE	cehaniese@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
DRE	cid@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
ATU	citas@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
GSI	comunicacion@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
ACME	consultamedicaespecializada@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
GFI	contador@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
DRE	controlinterno@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
AHR	coordce@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
GFI	coordfacturacion@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
GFI	coordinacionfarmacia@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co

GJUC	denunciacorrupcion@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
GFI	facturacionelectronica@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
GAFT	gal@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
DRE	gerencia@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
GSI	gestiondocumental@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
GTH	gestionhumana@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
GJUC	juridica@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
GJUC	notificacionesjudiciales@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
SIG	oficialdecumplimiento@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
SIG	planeacion@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
ATU	pqrs@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
GFI	presupuesto@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
ASF	quimicofarmaceutico@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
ACA	quirofano@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
DRE	SECRETARIA@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
SIG	seguridadelpaciente@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
GSI	soportecnico@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
DRE	subadmitiva@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
DRE	subtecnica@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
GSI	sysadmin@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
GFI	tesoreria@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co
GSI	ucorrespondencia@cehani.gov.co	correo electrónico institucional	Servicio	www.google.com.co

GSI	Servidor de dominio 172.20.1.252	permite el acceso al dominio cehani.local en la red Institucional	Hadware	Data center principal
GSI	Servidor 172.20.1.248	Permite el acceso a carpetas compartidas (otros activos de información)	Hadware	Data center principal
GSI	Servidor 172.20.1.251	Permite el acceso al software Compuconta	Hadware	Data center principal
GSI	Servidor 172.20.1.240	Permite el almacenamiento automático de copias de seguridad de la información generada en diferentes equipos de computo	Hadware	Data center principal
GSI	Equipo NAS	Permite el almacenamiento automático de copias de seguridad de la información generada en diferentes equipos de computo	Hardware	Data center No 2
GSI	Dominio www.cehani.gov.co	Almacena y muestra información de la gestión institucional	Información	www.cehani.gov.co
GSI	Depósito 1 Archivo de Gestión (Historia Clínica)	Almacena información de la Historia clínica	Información	junto a farmacia
GSI	Depósito 2 Archivo de Gestión (Historia Clínica)	Almacena información de la Historia clínica	Información	junto a terapia física
GSI	Depósito 3 Archivo de Gestión (Historia Clínica)	Almacena información de la Historia clínica	Información	junto a la oficina subgerencia técnica
GSI	Depósito Administrativo y Central	Almacena información histórica administrativa y asistencial (Historias Clínicas)	Información	junto a la oficina de talento humano
GSI	Depósito Administrativo y Central	Almacena información histórica administrativa y asistencial (Historias Clínicas)	Información	junto a la oficina de talento humano
GSI	Depósito Administrativo y Central	Almacena información histórica administrativa y asistencial (Historias Clínicas)	Información	junto a la entrada principal
GSI	Depósito Administrativo y Central	Almacena información histórica administrativa y asistencial (Historias Clínicas)	Información	Oficina de Gestión documental
Todos los proceso	Equipos de computo	Para el ingreso y digitacion de informacion que se almacena en software/ y en el equipo	Hardware	Todas las áreas
Todos los proceso	Documentos de Word	Para el ingreso y digitacion de informacion que se almacena en software/ y en el equipo	Información	Todas las áreas
Todos los proceso	libros y hojas de cálculo de excel	Para el ingreso y digitacion de informacion que se almacena en software/ y en el equipo	Información	Todas las áreas
Todos los proceso	Presentaciones de Power Point	Para el ingreso y digitacion de informacion que se almacena en software/ y en el equipo	Información	Todas las áreas
Todos los proceso	Archivos pdf	Soportes de información	Información	Todas las áreas

Paso 2: Identificar el dueño y custodio de los activos

Proceso	Nombre del activo	Propietario	Custodio	Permiso de Acceso
GSI	COMPUCONTA	CEHANI ESE	GSI	Consulta de información según permisos del software
GSI	SALUDIPS	CEHANI ESE	Profesional Universitario GSI	Consulta de información según permisos del software
SIG	DOCUMENTOS SISTEMA GESTIÓN INSTITUCIONAL	CEHANI ESE	Profesional Universitario Planeación y Calidad	Lectura: Todos los proceso Modificacion y eliminacion: Profesional Universitario Planeación y Calidad
GJUC	CONTRATOS	CEHANI ESE	Profesional Universitario GJUC	Lectura: Todos los proceso Modificacion y eliminacion: Profesional Universitario GJUC
ACME	ACME	CEHANI ESE	Profesional Universitario ACME	Lectura y modificación: Todos los proceso
ASF	Actas entrega de medicamentos	CEHANI ESE	Profesional Universitario GSF	Lectura : Todos los proceso Modificación: Delegado proceso ASF
ASF	Actas de inicio de medicamentos	CEHANI ESE	Profesional Universitario GSF	Lectura : Todos los proceso Modificación:

				Delegado proceso ASF
GTH	Gestion Humana	CEHANI ESE	Profesional Universitario GTH	Lectura y escritura únicamente personal del proceso GTH
ATU	GPSA- GAR	CEHANI ESE	Profesional Universitario ATU	Lectura y escritura únicamente personal del proceso ATU
ACME	Estadística - 2018	CEHANI ESE	Profesional Universitario ACME	Lectura y escritura únicamente personal del proceso ACME
GFI-ASF	Facturacion farmacia	CEHANI ESE	Profesional Universitario Quimico Farmaceutico	Lectura y escritura únicamente personal del proceso ASF-Facturación
GFI-ASF	Radicados 2021	CEHANI ESE	Profesional Universitario Quimico Farmaceutico	Lectura y escritura únicamente personal del proceso ASF-Facturación
GAFT	almacen@cehani.gov.co	CEHANI ESE	TECNICO ADMINISTRATIVO ALMACEN	Únicamente al personal custodio o quien este delegue
ADI	Ayudasdiagnosticas@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO ADI	Únicamente al personal custodio o quien este delegue
SIG	calidad@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO SIG	Únicamente al personal custodio o quien este delegue
GFI	cartera@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO GFI	Únicamente al personal custodio o quien este delegue
DRE	cehaniese@cehani.gov.co	CEHANI ESE	SECRETARIA	Únicamente al personal custodio o quien este delegue
DRE	cid@cehani.gov.co	CEHANI ESE	CONTROL INTERNO DISCIPLINARIO	Únicamente al personal custodio o quien este delegue

ATU	citas@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO ATU	Únicamente al personal custodio o quien este delegue
GSI	comunicacion@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO GSI	Únicamente al personal custodio o quien este delegue
ACME	consultamedicaespecializada@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO ACME	Únicamente al personal custodio o quien este delegue
GFI	contador@cehani.gov.co	CEHANI ESE	CONTADOR	Únicamente al personal custodio o quien este delegue
DRE	controlinterno@cehani.gov.co	CEHANI ESE	JEFE OFICINA CONTROL INTERNO	Únicamente al personal custodio o quien este delegue
AHR	coordce@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO AHR	Únicamente al personal custodio o quien este delegue
GFI	coordfacturacion@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO COORDINADOR FACTURACIÓN	Únicamente al personal custodio o quien este delegue
GFI	coordinacionfarmacia@cehani.gov.co	CEHANI ESE	SUBGERENCIA ADMINISTRATIVA	Únicamente al personal custodio o quien este delegue
GJUC	denunciacorrupcion@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO GJUC	Únicamente al personal custodio o quien este delegue
GFI	facturacionelectronica@cehani.gov.co	CEHANI ESE	CONTADOR	Únicamente al personal custodio o quien este delegue
GAFT	gal@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO GAFT	Únicamente al personal custodio o quien este delegue
DRE	gerencia@cehani.gov.co	CEHANI ESE	GERENTE	Únicamente al personal custodio o quien este delegue

GSI	gestiondocumental@cehani.gov.co	CEHANI ESE	TÉCNICO ADMINISTRATIVO GESTIÓN DOCUMENTAL	Únicamente al personal custodio o quien este delegue
GTH	gestionhumana@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO GTH	Únicamente al personal custodio o quien este delegue
GJUC	juridica@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO GJUC	Únicamente al personal custodio o quien este delegue
GJUC	notificacionesjudiciales@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO GJUC	Únicamente al personal custodio o quien este delegue
SIG	oficialdecumplimiento@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO SIG	Únicamente al personal custodio o quien este delegue
SIG	planeacion@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO SIG	Únicamente al personal custodio o quien este delegue
ATU	pqrs@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO ATU	Únicamente al personal custodio o quien este delegue
GFI	presupuesto@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO GFI	Únicamente al personal custodio o quien este delegue
ASF	quimicofarmaceutico@cehani.gov.co	CEHANI ESE	QUIMICO FARMACEUTICO	Únicamente al personal custodio o quien este delegue
ACA	quirofano@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO ACA	Únicamente al personal custodio o quien este delegue
DRE	SECRETARIA@cehani.gov.co	CEHANI ESE	SECRETARIA	Únicamente al personal custodio o quien este delegue
SIG	seguridadelpaciente@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO SIG	Únicamente al personal custodio o quien este delegue

GSI	soportecnico@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO GSI	Únicamente al personal custodio o quien este delegue
DRE	subadmitiva@cehani.gov.co	CEHANI ESE	SUBGERENCIA ADMINISTRATIVA	Únicamente al personal custodio o quien este delegue
DRE	subtecnica@cehani.gov.co	CEHANI ESE	SUBGERENCIA TÉCNICA	Únicamente al personal custodio o quien este delegue
GSI	sysadmin@cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO GSI	Únicamente al personal custodio o quien este delegue
GFI	tesoreria@cehani.gov.co	CEHANI ESE	TESORERO	Únicamente al personal custodio o quien este delegue
GSI	ucorrespondencia@cehani.gov.co	CEHANI ESE	TÉCNICO ADMINISTRATIVO GESTIÓN DOCUMENTAL	Únicamente al personal custodio o quien este delegue
GSI	Servidor de dominio 172.20.1.252	CEHANI ESE	PROFESIONAL UNIVERSITARIO GSI	Únicamente al personal custodio o quien este delegue
GSI	Servidor 172.20.1.248	CEHANI ESE	PROFESIONAL UNIVERSITARIO GSI	Únicamente al personal custodio o quien este delegue
GSI	Servidor 172.20.1.251	CEHANI ESE	PROFESIONAL UNIVERSITARIO GSI	Únicamente al personal custodio o quien este delegue
GSI	Servidor 172.20.1.240	CEHANI ESE	PROFESIONAL UNIVERSITARIO GSI	Únicamente al personal custodio o quien este delegue
GSI	Equipo NAS	CEHANI ESE	PROFESIONAL UNIVERSITARIO GSI	Únicamente al personal custodio o quien este delegue
GSI	Dominio www.cehani.gov.co	CEHANI ESE	PROFESIONAL UNIVERSITARIO GSI	Todas las partes interesadas pueden consultarla

GSI	Depósito 1 Archivo de Gestión (Historia Clínica)	CEHANI ESE	Tecnico Administrativo en Gestion documental	Técnico Administrativo de gestión documental o quien él designe
GSI	Depósito 2 Archivo de Gestión (Historia Clínica)	CEHANI ESE	Tecnico Administrativo en Gestion documental	Técnico Administrativo de gestión documental o quien él designe
GSI	Depósito 3 Archivo de Gestión (Historia Clínica)	CEHANI ESE	Tecnico Administrativo en Gestion documental	Técnico Administrativo de gestión documental o quien él designe
GSI	Depósito Administrativo y Central	CEHANI ESE	Tecnico Administrativo en Gestion documental	Técnico Administrativo de gestión documental o quien él designe
GSI	Depósito Administrativo y Central	CEHANI ESE	Tecnico Administrativo en Gestion documental	Técnico Administrativo de gestión documental o quien él designe
GSI	Depósito Administrativo y Central	CEHANI ESE	Tecnico Administrativo en Gestion documental	Técnico Administrativo de gestión documental o quien él designe
GSI	Depósito Administrativo y Central	CEHANI ESE	Tecnico Administrativo en Gestion documental	Tecnico Administrativo de gestión documental o quien él designe
Todos los proceso	Equipos de computo	CEHANI ESE	Delegado según inventario de equipo	No requiere permiso de acceso
Todos los proceso	Documentos de Word	CEHANI ESE	Delegado según inventario de equipo	No requiere permiso de acceso
Todos los proceso	libros y hojas de calculo de excel	CEHANI ESE	Delegado según inventario de equipo	No requiere permiso de acceso

Todos los proceso	Presentaciones de Power Point	CEHANI ESE	Delegado según inventario de equipo	No requiere permiso de acceso
Todos los proceso	Archivos pdf	CEHANI ESE	Delegado según inventario de equipo	No requiere permiso de acceso

Paso 3: Clasificar los activos

TIPO DE ACTIVO	DESCRIPCIÓN
INFORMACIÓN	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
SOFTWARE	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades.
HARDWARE	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información.
SERVICIOS	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software).
INTANGIBLES	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el good will, entre otros.
COMPONENTES DE RED	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros
PERSONAS	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades.
INSTALACIONES	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa.

Paso 4: Clasificar la información

a. **Según la confidencialidad**: Se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, Esta se debe definir de acuerdo con las características de los activos que se manejan en la entidad, para el

caso de CEHANI E.S.E. Se definen tres (3) niveles alineados con los tipos de información declarados en la ley 1712 del 2014.

INFORMACIÓN PÚBLICA RESERVADA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
INFORMACIÓN PÚBLICA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACIÓN PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PÚBLICA RESERVADA.

b. **Según la integridad**: Se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción. Para el caso de CEHANI E.S.E se utilizará el siguiente esquema de clasificación de tres (3) niveles.

A (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
M (MEDIA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderada a funcionarios de la entidad.
B (BAJA)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

c. **Según la disponibilidad**: Es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso

autorizado cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso. Para el caso de CEHANI E.S.E. es recomendable utilizar el siguiente esquema de clasificación de tres (3) niveles

A (ALTA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
M (MEDIA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
B (BAJA)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

d. Clasificación de los Activos Según las Normas

ACTIVO	TIPO DE ACTIVO	LEY 1712 / 2014	LEY 1581 / 2012
Computador de escritorio	Hardware	NA	NA
Bases de datos en Excel	Información	Información Reservada	No contiene datos personales
Correo electrónico	Servicio	Información Reservada	Contiene datos personales
Software SALUDIPS/COMPUCONTA - Todos los Módulos	Software	Información Reservada	Contiene datos personales
Software en comodato (Bionexo, GyS)	Software	Información Reservada	Contiene datos personales
Documentos en Word	Información	Información Reservada	No contiene datos personales
Memorias USB y CD	Hardware	NA	NA
Software para controlar el acceso del personal	Software	NA	Contiene datos personales
Copias de seguridad	Información	Información Reservada	No contiene datos personales
Metadatos en archivos de Excel	Información	Información Reservada	No contiene datos personales
Carpeta compartida	Servicio	NA	NA

ACTIVO	TIPO DE ACTIVO	LEY 1712 / 2014	LEY 1581 / 2012
Lectores de código de barras	Hardware	NA	NA
Lector de temperatura	Hardware	NA	NA
Partición de Disco Duro	Hardware / Información	NA	NA
Impresoras	Hardware	NA	NA
Red de Datos	Componentes de Red	NA	NA
Servidores y NAS	Hardware / Componentes de Red	NA	NA
Switches	Componentes de red	NA	NA
Routers y Microtik	Componentes de red	NA	NA
Página WEB	Servicio	Información Clasificada y Pública	NA
Redes Sociales	Servicio	Información Pública	NA
Cableado estructurado	Componentes de red	NA	NA
CCTV	Componentes de red	NA	NA
Rack	Componentes de red	NA	NA
Centro de cableado	Componentes de red	NA	NA

Paso 5: Determinar la criticidad del activo

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PÚBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PÚBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Para determinar el nivel de criticidad se utiliza los siguientes criterios:

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.

MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Identificación de los niveles de criticidad de los activos de CEHANI E.S.E.

Proceso	Nombre del activo	Criticidad
GSI	COMPUCONTA	30
GSI	SALUDIPS	30
SIG	DOCUMENTOS SISTEMA GESTIÓN INSTITUCIONAL	25
GJUC	CONTRATOS	21
ACME	ACME	12
ASF	Actas entrega de medicamentos	16
ASF	Actas de inicio de medicamentos	16
GTH	Gestion Humana	25
ATU	GPSA- GAR	20
ACME	Estadistica – 2018	20
GFI- ASF	Facturacion farmacia	20
GFI- ASF	Radicados 2021	20
GAFT	almacen@cehani.gov.co	15
ADI	Ayudasdiagnosticas@cehani.gov.co	15
SIG	calidad@cehani.gov.co	15
GFI	cartera@cehani.gov.co	15
DRE	cehaniese@cehani.gov.co	15
DRE	cid@cehani.gov.co	15
ATU	citas@cehani.gov.co	15
GSI	comunicacion@cehani.gov.co	15
ACME	consultamedicaespecializada@cehani.gov.co	15
GFI	contador@cehani.gov.co	15

DRE	controlinterno@cehani.gov.co	15
AHR	coordce@cehani.gov.co	15
GFI	coordfacturacion@cehani.gov.co	15
GFI	coordinacionfarmacia@cehani.gov.co	15
GJUC	denunciacorrupcion@cehani.gov.co	15
GFI	facturacionelectronica@cehani.gov.co	15
GAFT	gal@cehani.gov.co	15
DRE	gerencia@cehani.gov.co	15
GSI	gestiondocumental@cehani.gov.co	15
GTH	gestionhumana@cehani.gov.co	15
GJUC	juridica@cehani.gov.co	15
GJUC	notificacionesjudiciales@cehani.gov.co	15
SIG	oficialdecumplimiento@cehani.gov.co	15
SIG	planeacion@cehani.gov.co	15
ATU	pqrs@cehani.gov.co	15
GFI	presupuesto@cehani.gov.co	15
ASF	quimicofarmaceutico@cehani.gov.co	15
ACA	quirofano@cehani.gov.co	15
DRE	SECRETARIA@cehani.gov.co	15
SIG	seguridadelpaciente@cehani.gov.co	15
GSI	soportecnico@cehani.gov.co	15
DRE	subadmitiva@cehani.gov.co	15
DRE	subtecnica@cehani.gov.co	15
GSI	sysadmin@cehani.gov.co	15
GFI	tesoreria@cehani.gov.co	15
GSI	ucorrespondencia@cehani.gov.co	15
GSI	Servidor de dominio 172.20.1.252	30
GSI	Servidor 172.20.1.248	30
GSI	Servidor 172.20.1.251	30
GSI	Servidor 172.20.1.240	16
GSI	Equipo NAS	16
GSI	Dominio www.cehani.gov.co	12
GSI	Depósito 1 Archivo de Gestión (Historia Clínica)	30
GSI	Depósito 2 Archivo de Gestión (Historia Clínica)	30
GSI	Depósito 3 Archivo de Gestión (Historia Clínica)	30

GSI	Depósito Administrativo y Central	30
GSI	Depósito Administrativo y Central	30
GSI	Depósito Administrativo y Central	30
GSI	Depósito Administrativo y Central	25
Todos los proceso	Equipos de computo	11
Todos los proceso	Documentos de Word	11
Todos los proceso	libros y hojas de calculo de Excel	11
Todos los proceso	Presentaciones de Power Point	11
Todos los proceso	Archivos pdf	11

3.1.1. Metodología para la identificación de riesgos Identificación de riesgos a la seguridad y privacidad de la información – MA-GDC-003

Para identificar los riesgos relacionados a seguridad y privacidad de la información, es necesario previamente identificar las amenazas que pueden materializarse. Los tipos de amenazas se han clasificado en 2: amenazas comunes y amenazas dirigidas por el hombre.

Amenazas Comunes

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	F, D, A
	Agua	F, D, A
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua	E
	Fallas en el suministro de aire acondicionado	F, D, A
Perturbación debida a la radiación	Radiación electromagnética	F, D, A
	Radiación térmica	F, D, A
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida	D
	Espionaje remoto	D
Fallas técnicas	Fallas del equipo	D, F

	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F
Acciones no autorizadas	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F
Compromiso de las funciones	Error en el uso o abuso de derechos	D, F
	Falsificación de derechos	D

F: Fortuito
D: Deliberada
A: Ambiental

Amenazas Dirigidas Por El hombre

FUENTE DE AMENAZA	MOTIVACIÓN	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto Ego	Piratería Ingeniería social
Criminal de la computación	Destrucción de la información Modificación de la integridad de la información Divulgación ilegal de la información	Crimen por computador Acto fraudulento
Terrorismo	Chantaje Destrucción	Ataques contra el sistema DDoS Penetración en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa Hurto de información
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ganancia monetaria	Asalto a un empleado Chantaje

Vulnerabilidades

TIPO	VULNERABILIDADES
Hardware	Mantenimiento insuficiente

TIPO	VULNERABILIDADES
	Ausencia de esquemas de reemplazo periódico Sensibilidad a la radiación electromagnética Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad) Almacenamiento sin protección Falta de cuidado en la disposición final Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software Ausencia de terminación de sesión Ausencia de registros de auditoría Asignación errada de los derechos de acceso Interfaz de usuario compleja Ausencia de documentación Fechas incorrectas Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes Líneas de comunicación sin protección Conexión deficiente de cableado Tráfico sensible sin protección Punto único de falla
Personal	Ausencia del personal Entrenamiento insuficiente Falta de conciencia en seguridad Ausencia de políticas de uso aceptable Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio Áreas susceptibles a inundación Red eléctrica inestable Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios Ausencia de proceso para supervisión de derechos de acceso Tipo Vulnerabilidades Ausencia de control de los activos que se encuentran fuera de las instalaciones Ausencia de acuerdos de nivel de servicio (ANS o SLA) Ausencia de mecanismos de monitoreo para brechas en la seguridad Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Es de tener presente que la sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

Amenazas y Vulnerabilidades

TIPO DE ACTIVO	VULNERABILIDAD	AMENAZA
Hardware	Mantenimiento insuficiente Almacenamiento sin protección	Hurto de equipos y documentos Falla y/o mal funcionamiento de los equipos Uso no autorizado
Software	Insuficiencia en las pruebas del software Interfaz de usuario compleja Contraseñas sin protección Software en módulos asistenciales inmaduro	Mal funcionamiento del software Falta de mantenimiento del sistema de información Falsificación de derechos de acceso al sistema
Componentes de red	Líneas de comunicación sin protección Tráfico sensible sin protección	Piratería informática
Información	Copias no controladas	Espionaje remoto Hurto de información
Personal	Entrenamiento insuficiente Falta de conciencia en seguridad Ausencia de políticas relacionadas con la información	Ingeniería social
Organización	Ausencia de políticas de seguridad	Abuso de derechos
Lugar	Control de acceso insuficiente Ausencia de protección en puertas y ventanas	Fuego, inundación, fenómenos sísmicos

Escala de Probabilidades, Impacto y Metodología de Valoración

La escala de probabilidades o frecuencias en que se puede presentar la materialización del riesgo, el impacto o consecuencias que se pueden presentar y la metodología establecida para su análisis y valoración se encuentran definidos en la Guía básica de gestión de riesgos y oportunidades de CEHANI ESE GU-SIG-007.

Riesgos de seguridad y privacidad de la información:

Los riesgos de seguridad y privacidad de la información se obtienen de los niveles de criticidad de los activos de información, las amenazas comunes y aquellas dirigidas por el hombre, y las vulnerabilidades identificadas, lo riesgos obtenidos son:

AMENAZA O VULNERABILIDAD	RIESGO IDENTIFICADO	IMPACTO O CONSECUENCIA
Fuego Agua Fenómenos sísmicos Fenómenos climáticos Fallas en el suministro de Agua Fallas en el suministro de aire acondicionado Radiación electromagnética Radiación Térmica Interceptación de servicios de señales de interferencia comprometida Espionaje remoto Fallas del equipo Mal funcionamiento de equipos Saturación del sistema de información Mal funcionamiento del software Incumplimiento en el mantenimiento del sistema de información Uso no autorizado del equipo Copia fraudulenta del software Error en el uso o abuso de derechos Falsificación de derechos No copias de seguridad Virus tecnológicos Pérdida de documentos contables y presupuestales o soportes Adulteración de historia clínica	Pérdida de la integridad de la información	Pérdida de memoria documental física y electrónica Imposibilidad de acceder y recuperar la información
Espionaje Remoto Fallas en el equipo Mal funcionamiento del software	Pérdida de la confidencialidad de la información	Sanciones. Extravío de la información. Incumplimiento legal.

Incumplimiento en el mantenimiento del sistema de información Uso no autorizado del equipo Copia fraudulenta del software Error en el uso o abuso de derechos Falsificación de derechos Acceso sin permisos a la Historia clínica		
Radiación electromagnética Radiación térmica Interceptación de servicios de señales de Interferencias comprometida Espionaje remoto Fallas en el equipo Mal funcionamiento del equipo Saturación del sistema de información Mal funcionamiento del software Incumplimiento en el mantenimiento del sistema de información Copia fraudulenta del software No acceso oportuno a la historia clínica al personal autorizado	Pérdida de la disponibilidad de la información	Eventos adversos Insatisfacción del paciente Demandas Sanciones

Los riesgos identificados se encuentran analizados y valorados en la Matriz de riesgos y oportunidades MA-SIG-007.

3.1.2. Indicadores para la gestión de los riesgos

En los planes operativos anuales de la vigencia 2022 se tiene establecido el indicador de cumplimiento de la evaluación de riesgos por proceso.

3.2. FASE 2: Ejecución

Fase que corresponde a la implementación de los controles del cuadro anterior, conservando los tiempos de ejecución y llevar a cabo lo planeado.

En esta fase es importante el compromiso de la Alta dirección de brindar los recursos necesarios para iniciar con el tratamiento de los riesgos y por otra parte el liderazgo del responsable del proceso de GSI.

3.3. FASE 3: Monitoreo y Revisión

La entidad y sus Tres Líneas de defensa definidas en el MIPG deben hacer un seguimiento a los planes de tratamiento para determinar su efectividad, según lo siguiente:

- Realizar monitoreo de los riesgos y controles tecnológicos.

- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

3.4. FASE 4: Mejoramiento Continuo

La Entidad garantiza la mejora continua de la gestión de los riesgos de seguridad y privacidad de la información, estableciendo las acciones de mejora según lo definido en el Procedimiento de Mejora Continuo PR-SIG-005 el cual aplica para cuando existan hallazgos, falencias o incidentes de seguridad y privacidad de la información, se identifica la fuente de la no conformidad, se mitiga el impacto de su existencia y se toman acciones para controlarlos y prevenirlos.

4. CRONOGRAMA

ACTIVIDAD	RESPONSABLE	FECHA MAXIMA DE IMPLEMENTACION	PRODUCTO
Revision de la matriz de riesgos del proceso GSI	Lider GSI Jefe Oficina Control Interno	30-04-2024	Matriz de riesgos verificada y/o ajustada
Analisis de controles establecidos para los riesgos de seguridad y privacidad de la inforamación	Lider GSI Jefe Oficina Control Interno	30-05-2024	Informe
Moniterero de Riesgos de Seguridad y privacidad de la Informacion	Lider GSI Jefe Oficina Control Interno	30-08-2024	Informe
Implementacion de software en gestion de riesgos institucional (enfoque a riesgos del SGSI)	Gerencia Lider GSI	30-12-2024	Software implementado

5. PRESUPUESTO

El presupuesto establecido para la ejecución del presente plan se encuentra determinado desde el Plan Anual de Adquisiciones en los siguientes ítems:

DETALLE	CANTIDAD PRESUPUESTADA	VALOR UNITARIO	VALOR TOTAL PRESUPUESTADO	RUBRO PRESUPUESTAL

Arrendamiento sistema integrado de gestión de riesgos	1.0	100,000,000	100,000,000	2.1.2.02.02.007.02.21.1.1. 1.2.3.2.27
TOTAL			**100,000,000**	

NOTA: El valor informado corresponde a la totalidad definido en el rubro presupuestal, y corresponde a la totalidad del software para el manejo de riesgos, mas sin embargo para la implementación de este plan correspondería a $7.142.857.

	Actualizado por:	**Revisado por:**	**Aprobado por:**
Firma			
Nombre	JHON JAIRO FIGUEROA	SANDRA GOMEZ TULCAN	ARLEY REALPE CHAMORRO
Cargo / Rol	Profesional Universitario - Líder Proceso GSI	Subgerente Administrativo y Financiero	Presidente – Comité Institucional de Gestión y Desempeño

	Visto Bueno
Firma	
Nombre	CRISTIAN JIMÉNEZ QUINTERO
Cargo	Profesional de Apoyo - SGC