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 actualizo el cronograma para la vigencia 2020.	Mejoramiento continuo

1. 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.

La metodología para el tratamiento de riesgos de seguridad y privacidad de la información que se desarrolla en el presente Plan es la sugerida por el Departamento Administrativo de la Función Púbica denominada “Guía para la administración del riesgo y el diseño de controles en entidades públicas”, lo cual es complementado con el desarrollo de la Guía 7 del MSPI relacionada con la gestión de riesgos y la Guía 8 de controles de la seguridad de la información.

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.

2. OBJETIVOS

2.1. 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.

2.2. 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.

3. CONCEPTOS BASICOS

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 n 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.

4. PROCESO DE GESTION DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

4.1. 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 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, teniendo como base y metodología principal el documento del Departamento administrativo de la Función Pública.

Contexto externo e interno

Para determinar el contexto externo e interno de la entidad en temas relacionados con la seguridad y privacidad de la información, es pertinente revisar lo contemplado en los documentos del Plan de Desarrollo Institucional y en el Plan de Tecnologías de la Información, donde se encuentra claramente realizado el diagnóstico a nivel general como particular para el tema de TI, estos documentos son de gran ayuda para enfocar y determinar el campo de acción de la entidad y los componentes TI con los que cuenta en la actualidad.

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.

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

En este aspecto como la entidad debe promulgar una política de gestión del riesgo que sea integral, esta entonces debe incluir el compromiso para la gestión de riesgos de seguridad y privacidad de la información en todos los niveles.

Roles y responsabilidades

La entidad debe delegar la responsabilidad de la Seguridad y Privacidad de la Información 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.

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.

La alta dirección debe asignar los siguientes recursos:

- Personal capacitado e idóneo para la gestión de los riesgos de seguridad y privacidad de la información.
- Recursos económicos para la implementación de controles de mitigación de riesgos.
- Recursos para los aspectos de mejora continua, monitoreo y auditorías internas.

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 aumentando 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 por cada proceso

Tabla 1: Activos de Información.

PROCESO / Dependencia	ACTIVO	DESCRIPCION
Subgerencia Administrativa y financiera- no existe este proceso	Computador de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas
Subgerencia Administrativa y financiera	Bases de datos en Excel	Informes provenientes de todos los procesos y áreas a su cargo
Subgerencia Administrativa y financiera	Correo electrónico	Almacena el histórico de información enviada y recibida
Gestión Humana	Computadores de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas
Gestión Humana	Software COMPUCONTA - módulo nómina	Programa utilizado para realizar la liquidación de la nómina
Gestión Humana	Bases de datos en Excel	Bases de datos histórica de nómina
Gestión Humana	Documentos en Word	Documentos que soportan las actividades cotidianas
Gestión Humana	Memorias USB y CD	Dispositivos utilizados para el trabajo de información institucional
Gestión Humana	Software para controlar el acceso del personal	Programa utilizado para controlar la entrada y salida del personal de nómina de la entidad
Gestión Humana	Correo electrónico	Almacena el histórico de información enviada y recibida
Gestión de Habilitación y Rehabilitación	Computador de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas
Gestión de Habilitación y Rehabilitación	Correo electrónico	Almacena el histórico de información enviada y recibida
Gestión de Habilitación y Rehabilitación	Copias de seguridad	Almacenamiento utilizado para salvaguardar información relacionada con los servicios
Gestión de Habilitación y Rehabilitación	Bases de datos en Excel	Informes de producción de los diferentes servicios
Gestión de Habilitación y Rehabilitación	COMPUCONTA – Historia clínica digital	Software donde se almacena toda la información relacionada con la HC de los usuarios de los servicios
Gestión Documental	Computador de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas
Gestión Documental	Metadatos en archivos de Excel	Utilizados para guardar la información de archivo administrativo y de HC
Gestión Documental	Correos electrónicos	Almacena el histórico de información enviada y recibida
Gestión Documental	USB	Para almacenar información relacionada con la gestión del área
Gestión Jurídica y ABS	Computador de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas
Gestión Jurídica y ABS	Bases de datos en Excel	Información relacionada con la contratación
Gestión Jurídica y ABS	Carpeta compartida	Información para que cada proceso alimente con información de interés para la oficina jurídica, especialmente de contratos
Subgerencia Técnica	Computador de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas
Subgerencia Técnica	Bases de datos en Excel	Información que reportan los diferentes servicios, áreas y procesos
Subgerencia Técnica	Documentos en Word	Documentos que soportan las actividades cotidianas
Subgerencia Técnica	Carpeta compartida	Información para que cada proceso alimente con información de interés para la subgerencia y viceversa

Gestión financiera – tesorería	Computador de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas
Gestión financiera - tesorería	COMPUCONTA - Tesorería	Software donde se almacena toda la información relacionada con los pagos que realiza la entidad a los proveedores
Gestión de ayudas diagnósticas	Computador de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas
Gestión de ayudas diagnósticas	Bases de datos en Excel	Producción del servicio, control de agendas e informes
Gestión de ayudas diagnósticas	Memoria USB	Almacenar información relacionada con el servicio de neurología
Gestión de apoyo logístico	Computadores de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas
Gestión de apoyo logístico	Bases de datos en Excel	Registro de bitácoras y bases de datos varias
Gestión de apoyo logístico	COMPUCONTA – Almacén	Software donde se almacena toda la información relacionada con los activos de la entidad
GPSA	Computador de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas
GPSA	COMPUCONTA - PQRSF	Software donde se hace el control y seguimiento a las PQRSF que los usuarios interponen en la entidad
GPSA	Bases de datos en Excel	Tratamiento de la información relacionada con PQRSF y satisfacción del usuario
GPSA	Correo electrónico	Almacena el histórico de información enviada y recibida
Gestión servicio farmacéutico	Computador de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas
Gestión servicio farmacéutico	Lectores de código de barras	Utilizados para cargar a almacén
Gestión servicio farmacéutico	Lector de temperatura	Utilizado para recibir medicamentos
Gestión servicio farmacéutico	Bases de datos en Excel	Utilizado para el control de temperatura y control de entregas
Gestión de calidad	Computador de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas
Gestión de calidad	Informes y evidencias del SGC	Información relacionada con el SGC
Gestión de calidad	Partición de Disco Duro	Unidad utilizada para guardar información del SGC
Gestión de calidad	Bases de datos en Excel	Información de SARLAFT
Gestión de cirugía ambulatoria	Computador d escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas
Gestión de cirugía ambulatoria	Correo electrónico	Almacena el histórico de información enviada y recibida
Gestión de cirugía ambulatoria	Carpetas y archivos magnéticos	Información relacionada con el servicio de quirófanos
Gestión de cirugía ambulatoria	Carpetas compartidas	Utilizada para compartir información del servicio y alimentar los de otros procesos
Gestión de Sistemas de Información	Red de Datos	Utilizada para brindar acceso a los aplicativos y a internet
Gestión de Sistemas de Información	Servidores	Almacenar aplicativos y bases de datos
Gestión de Sistemas de Información	Switchs	Componentes para interconectar los equipos a la red
Gestión de Sistemas de Información	Routers	Componentes para brindar acceso a internet y aplicaciones de forma inalámbrica
Gestión de Sistemas de Información	Página WEB	Servicio utilizado para publicar información de interés en internet

Gestión de Sistemas de Información	Redes Sociales	Servicios utilizados para publicar u compartir información institucional
Gestión de Sistemas de Información	Cableado estructurado	Para brindar conexión a la red de datos
Gestión de Sistemas de Información	CCTV	Servicio utilizado para monitorear las instalaciones de la entidad
Gestión de Sistemas de Información	Rack	Componente que se utiliza para ubicar los componentes que interconectan la red de cableado estructurado
Gestión de Sistemas de Información	Centro de cableado	Lugar donde reposan servidores, rack, switches y demás componentes de red

4.1.1. Paso 2: Identificar el dueño de los activos

Dueño de los Activos

ACTIVO	DESCRIPCION	DUEÑO DEL ACTIVO / CUSTODIO.
Computador de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas	Subgerente administrativo y financiero
Bases de datos en Excel	Informes provenientes de todos los procesos y áreas a su cargo	Subgerente administrativo y financiero
Correo electrónico	Almacena el histórico de información enviada y recibida	Subgerente administrativo y financiero
Computadores de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas	Profesional Universitario de Recursos Humanos
Software COMPUCONTA - módulo nómina	Programa utilizado para realizar la liquidación de la nómina	Profesional Universitario de Gestión Humana
Bases de datos en Excel	Bases de datos histórica de nómina	Profesional Universitario de Gestión Humana
Documentos en Word	Documentos que soportan las actividades cotidianas	Profesional Universitario de Gestión Humana
Memorias USB y CD	Dispositivos utilizados para el trabajo de información institucional	Profesional Universitario de Gestión Humana
Software para controlar el acceso del personal	Programa utilizado para controlar la entrada y salida del personal de nómina de la entidad	Profesional Universitario de Recursos Humanos
Correo electrónico	Almacena el histórico de información enviada y recibida	Profesional Universitario de Recursos Humanos

ACTIVO	DESCRIPCION	DUEÑO DEL ACTIVO / CUSTODIO.
Correo electrónico	Almacena el histórico de información enviada y recibida	Coordinadora de consulta externa
Copias de seguridad	Almacenamiento utilizado para salvaguardar información relacionada con los servicios	consulta externa
Bases de datos en Excel	Informes de producción de los diferentes servicios	consulta externa
COMPUCONTA – Historia clínica digital	Software donde se almacena toda la información relacionada con la HC de los usuarios de los servicios	consulta externa
Computador de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas	Técnico Administrativo en gestión documental
Metadatos en archivos de Excel	Utilizados para guardar la información de archivo administrativo y de HC	Técnico Administrativo en gestión documental
Correos electrónicos	Almacena el histórico de información enviada y recibida	Técnico Administrativo en gestión documental
USB	Para almacenar información relacionada con la gestión del área	Técnico Administrativo en gestión documental
Computador de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas	Profesional Universitario Gestión Jurídica y Contratación
Bases de datos en Excel	Información relacionada con la contratación	Profesional Universitario Gestión Jurídica y Contratación
Carpeta compartida	Información para que cada proceso alimente con información de interés para la oficina jurídica, especialmente de contratos	Profesional Universitario Gestión Jurídica y Contratación
Computador de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas	Subgerente técnico
Bases de datos en Excel	Información que reportan los diferentes servicios, áreas y procesos	Subgerente técnico
Documentos en Word	Documentos que soportan las actividades cotidianas	Subgerente técnico

ACTIVO	DESCRIPCION	DUEÑO DEL ACTIVO / CUSTODIO.
Carpeta compartida	Información para que cada proceso alimente con información de interés para la subgerencia y viceversa	Subgerente técnico
Computador de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas	Tesorero General
COMPUCONTA - Tesorería	Software donde se almacena toda la información relacionada con los pagos que realiza la entidad a los proveedores	Tesorero General
Computador de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas	Coordinadora ayudas diagnósticas y oftalmología
Bases de datos en Excel	Producción del servicio, control de agendas e informes	Coordinadora ayudas diagnósticas y oftalmología
Memoria USB	Almacenar información relacionada con el servicio de neurología	Coordinadora ayudas diagnósticas y oftalmología
Computadores de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas	Profesional Universitario de Apoyo Logístico
Bases de datos en Excel	Registro de bitácoras y bases de datos varias	Profesional Universitario de Apoyo Logístico
COMPUCONTA – Almacén	Software donde se almacena toda la información relacionada con los activos de la entidad	Profesional Universitario de Apoyo Logístico
Computador de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas	Líder de gestión de participación social y atención al usuario
COMPUCONTA - PQRSF	Software donde se hace el control y seguimiento a las PQRSF que los usuarios interponen en la entidad	Líder de gestión de participación social y atención al usuario
Bases de datos en Excel	Tratamiento de la información relacionada con PQRSF y satisfacción del usuario	Líder de gestión de participación social y atención al usuario
Correo electrónico	Almacena el histórico de información enviada y recibida	Líder de gestión de participación social y atención al usuario

ACTIVO	DESCRIPCION	DUEÑO DEL ACTIVO / CUSTODIO.
Computador de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas	Coordinador Servicio Farmacéutico
Lectores de código de barras	Utilizados para cargar a almacén	Coordinador Servicio Farmacéutico
Lector de temperatura	Utilizado para recibir medicamentos	Coordinador Servicio Farmacéutico
Bases de datos en Excel	Utilizado para el control de temperatura y control de entregas	Coordinador Servicio Farmacéutico
Computador de escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas	Profesional Universitario de Calidad
Informes y evidencias del SGC	Información relacionada con el SGC	Profesional Universitario de Calidad
Partición de Disco Duro	Unidad utilizada para guardar información del SGC	Profesional Universitario de Calidad
Bases de datos en Excel	Información de SARLAFT	Profesional Universitario de Calidad
Computador d escritorio	Equipo utilizado para apoyar el desarrollo de las actividades cotidianas	Coordinadora de Quirófano
Correo electrónico	Almacena el histórico de información enviada y recibida	Coordinadora de Quirófano
Carpetas y archivos magnéticos	Información relacionada con el servicio de quirófanos	Coordinadora de Quirófano
Carpetas compartidas	Utilizada para compartir información del servicio y alimentar los de otros procesos	Coordinadora de Quirófano
Red de Datos	Utilizada para brindar acceso a los aplicativos y a internet	Coordinador de Gestión de Sistemas de Información
Servidores	Almacenar aplicativos y bases de datos	Coordinador de Gestión de Sistemas de Información
Switchs	Componentes para interconectar los equipos a la red	Coordinador de Gestión de Sistemas de Información
Routers	Componentes para brindar acceso a internet y aplicaciones de forma inalámbrica	Coordinador de Gestión de Sistemas de Información

ACTIVO	DESCRIPCION	DUEÑO DEL ACTIVO / CUSTODIO.
Página WEB	Servicio utilizado para publicar información de interés en internet	Coordinador de Gestión de Sistemas de Información
Redes Sociales	Servicios utilizados para publicar u compartir información institucional	Coordinador de Gestión de Sistemas de Información
Cableado estructurado	Para brindar conexión a la red de datos	Coordinador de Gestión de Sistemas de Información
CCTV	Servicio utilizado para monitorear las instalaciones de la entidad	Coordinador de Gestión de Sistemas de Información
Rack	Componente que se utiliza para ubicar los componentes que interconectan la red de cableado estructurado	Coordinador de Gestión de Sistemas de Información
Centro de cableado	Lugar donde reposan servidores, rack, switches y demás componentes de red	Coordinador de Gestión de Sistemas de Información

4.1.2. Paso 3: Clasificar los activos

Tipo de Activos

TIPO DE ACTIVO	DESCRIPCION
INFORMACION	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.
COMPONETES 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.

Clasificación delos Activos

ACTIVO	TIPO DE ACTIVO
Computador de escritorio	Hardware
Bases de datos en Excel	Información
Correo electrónico	Servicio
Software COMPUCONTA - Todos los Módulos	Software
Documentos en Word	Información
Memorias USB y CD	Hardware
Software para controlar el acceso del personal	Software
Copias de seguridad	Información
Metadatos en archivos de Excel	Información
Carpeta compartida	Servicio
Lectores de código de barras	Hardware
Lector de temperatura	Hardware
Partición de Disco Duro	Hardware / Información
Impresoras	Hardware
Red de Datos	Componentes de Red
Servidores	Hardware / Componentes de Red
Switches	Componentes de red
Routers	Componentes de red
Página WEB	Servicio
Redes Sociales	Servicio
Cableado estructurado	Componentes de red
CCTV	Componentes de red
Rack	Componentes de red
Centro de cableado	Componentes de red

4.1.3. Paso 4: Clasificar la información

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.

Clasificación de la Información Según la Confidencialidad

INFORMACION PUBLICA 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.
INFORMACION PUBLICA 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.
INFORMACION PUBLICA	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 PUBLICA RESERVADA.

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.

Clasificación de la Información Según la Integridad

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 moderado 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.

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

Clasificación de la Información Según la Disponibilidad

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.

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 COMPUCONTA - Todos los Módulos	Software	NA	NA
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	Hardware / Componentes de Red	NA	NA
Switches	Componentes de red	NA	NA
Routers	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

4.1.4.Paso 5: Determinar la criticidad del activo

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

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

Criterios de Criticidad

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.

Niveles de Criticidad de los Activos

ACTIVO	TIPO DE ACTIVO	Criticidad / Confidencialidad	Criticidad / Integridad	Criticidad / Disponibilidad	NIVEL DE CRITICIDAD
Computador de escritorio	Hardware	NA	NA	NA	NA
Bases de datos en Excel	Información	ALTA	ALTA	ALTA	ALTA
Correo electrónico	Servicio	BAJA	BAJA	ALTA	MEDIA
Software COMPUCONTA	Software	ALTA	ALTA	ALTA	ALTA
Documentos en Word	Información	ALTA	MEDIA	MEDIA	MEDIA
Memorias USB y CD	Hardware	NA	NA	NA	NA
Software para controlar el acceso del personal	Software	ALTA	ALTA	ALTA	ALTA
Copias de seguridad	Información	ALTA	ALTA	ALTA	ALTA
Metadatos en archivos de Excel	Información	ALTA	ALTA	ALTA	ALTA
Carpeta compartida	Servicio	ALTA	ALTA	ALTA	ALTA
Lectores de código de barras	Hardware	NA	NA	NA	NA
Lector de temperatura	Hardware	NA	NA	NA	NA

ACTIVO	TIPO DE ACTIVO	Criticidad / Confidencialidad	Criticidad / Integridad	Criticidad / Disponibilidad	NIVEL DE CRITICIDAD
Partición de Disco Duro	Hardware / Información	ALTA	ALTA	ALTA	ALTA
Impresoras	Hardware	NA	NA	NA	NA
Red de Datos	Componentes de Red	NA	NA	NA	NA
Servidores	Hardware / Componentes de Red	NA	NA	NA	NA
Switches	Componentes de red	NA	NA	NA	NA
Routers	Componentes de red	NA	NA	NA	NA
Página WEB	Servicio	ALTA	ALTA	ALTA	ALTA
Redes Sociales	Servicio	ALTA	ALTA	ALTA	ALTA
Cableado estructurado	Componentes de red	NA	NA	NA	NA
CCTV	Componentes de red	NA	NA	NA	NA
Rack	Componentes de red	NA	NA	NA	NA
Centro de cableado	Componentes de red	NA	NA	NA	NA

4.1.5. Identificación de riesgos a la seguridad y privacidad de la información

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

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
	Radiación electromagnética	F, D, A

Perturbación debida a la radiación	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	MOTIVACION	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto Ego	Piratería Ingeniería social
Criminal de la computación	Destrucción 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.

Es de tenar 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

NIVEL	DESCRIPTOR	DESCRIPCION	FRECUENCIA	CONTROLES ACTUALES
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año	No existen controles
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año	Mal control: Existen, son manuales y han resultado ser poco eficientes en la mayoría de ocasiones
3	Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años	Regular control: Existen, son manuales y han resultado ser eficientes en la mayoría de ocasiones
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años	Buen control: Existen, son automáticos y manuales, están documentados, son evaluados frecuentemente y han resultado ser eficientes en la mayoría de ocasiones
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años	Excelente control: Existen, son automáticos, están documentados, son evaluados frecuentemente y han resultado ser eficientes.

Escala de Impacto

NIVEL	DECRIPTOR	DESCRIPCION
5	Catastrófico	Afectación ALTA de los siguientes tres criterios:1 Integridad, Disponibilidad y Confidencialidad
4	Muy grave	Afectación ALTA de dos de los siguientes tres criterios: Integridad, Disponibilidad y Confidencialidad
3	Grave	Afectación MEDIA de los siguientes tres criterios: Integridad, Disponibilidad y Confidencialidad

2	Moderado	Afectación MEDIA de uno de los siguientes tres criterios: Integridad, Disponibilidad y Confidencialidad
1	Leve	Sin afectación o afectación BAJA de los siguientes tres criterios: Integridad, Disponibilidad y Confidencialidad

Mapa de Calor

Impacto / Probabilidad	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Criterios de Evaluación del Riesgo

RANGO	NIVEL	TRATAMIENTO
1-4	Riesgo Bajo	Mantener los controles actuales
5-9	Riesgo Moderado	Tratar en el mediano plazo
10-14	Riesgo Alto	Tratar a corto plazo
15-25	Riesgo Extremo	Tratar de inmediato

Matriz de riesgos de seguridad y privacidad de la información

PROCESO	RIESGO	CLASIFICACIÓN	CAUSAS	CONSECUENCIAS	CONTROLES ACTUALES	P	I	NR	NUEVOS CONTROLES PROPUESTOS	RESPONSABLE	PLAZO
Gestión de sistemas de información - GSI	Colapso de la estructura por movimiento sísmico	Seguridad y privacidad de la información	Cercanía al volcán galeras Acentamiento en falla geológica	Pérdida de información Perdidas económicas	No existen	1	5	5	1. Elaborar el plan de contingencia y recuperacion ante eventos catastróficos	Líder GSI	1. Primer semestre de 2019
	Ausencia de políticas de seguridad de la información o estas estan icompletas		Desconocimiento del deber de tenerlas No ver la información como un activo importante Restarle importancia al proceso de GSI	Abuso de derechos Libertad de accesos Acceso sin restricciones	Existen algunas polícias de seguridad de la información definidas pero están incompletas	4	5	20	1. Elaborar el documento que contenga las políticas de seguridad de la información 2. Hacer revisión periódica de las políticas 3. Divulgar las políticas entre todos los usuarios	Líder GSI	1. Primer trimestre de 2019 2. Revisión una vez por año 3. Primer trimestre 2019 y cada que haya actualización
	Desconocimiento de aspectos mínimos de seguridad y privacidad de la información		Entrenamiento insuficiente del personal Falta de conciencia en seguridad y privacidad de la información Ausencia de políticas	Hurto de información Pérdidas ecnonómicas	Existen algunas polícias de seguridad de la información definidas pero están incompletas	3	4	12	1. Capacitación al personal en seguridad informática e ingeniería social	Líder GSI	1. Primer trimestre de 2019
	Control de acceso insuficiente a cuarto de servidores y centro de datos		Barreras de seguridad y acceso debiles	Hurto de información Hurto de equipos Pérdidas económicas	1. Chapa de seguridad para acceso 2. Llaves en un solo lugar 3. Manejo de llaves por una sola persona	4	5	20	1. Bitácora de ingreso al cuarto de servidores 2. Acceso solo a personal autorizado 3. Control de acceso con dispositivo biométrico	1 y 2. Líder GSI 3. Líder GSI, Subgerencia Administrativa y financiera y Gestión financiera	1 y 2. Primer trimestre de 2019 3. Cuarto trimestre de 2019
	Líneas de comunicación e interconección y tráfico sencible sin protección		Falta de equipos de seguridad perimetral de la red	Hurto de información Pérdidas económicas Afectacion del buen nombre Espionaje remoto	1. Se cuenta con firewall 2. Se cuenta con antivirus	3	4	12	1. Equipos hardware de seguridad perimetral administrables	1. Líder GSI, Subgerencia Administrativa y financiera y Gestión financiera	1. Segundo semestre de 2019
	Copias de seguridad no controladas		No se cuenta con almacenamiento externo de back up de información	Sanciones Demandas Pérdida de credibilidad Pérdidas económicas Afectación del buen nombre	1. Existe cronograma de copias de seguridad y se le da cumplimiento 2. Se almacena las copias de seguridad internamente	3	3	9	1. Contratar el servicio de custodia externa de copias de seguridad 2. Establecer el protocolo para realizar las copias externas	1 y 2. Líder GSI, Subgerencia Administrativa y financiera, Gestión financiera	2020
	Mal funcionamiento de los equipos		Demora en el mantenimiento correctivo	Inoportunidad en la prestación del servicio Insatisfacción del usuario	1. Existe cronograma de mantenimiento preventivo y se le da cumplimiento	2	2	4	1. Contar con stock de repuestos de acuerdo a los modelos de los equipos	1. Líder GSI	
	Mal funcionamiento del software COMPUCONTA		No realizar pruebas del software antes de liberar una actualización Interfaz de usuario compleja Software en módulos asistenciales poco maduro Falta de mantenimiento del sistema Bajo nivel de contraseñas de seguridad No existe control de las solicitudes de soporte	Inoportunidad en la prestación del servicio Insatisfacción del usuario Afectación del buen nombre	1. Existe contrato de mantenimiento del software	5	5	25	1. Establecer control de soportes solicitados 2. Política para establecer contraseñas seguras 3. Ejecutar el plan de mejora para software	1, 2 y 3. Líder GSI	1,2 y 3. Primer trimestre 2019

4.1.6. Indicadores para la gestión de los riesgos

Se establece un indicador de eficacia relacionado con el cumplimiento de actividades el cual se lo calcula de la siguiente manera:
Índice de Cumplimiento de Actividades = (No. De Riesgos materializados / No. Riesgos Gestionados) * 100 siendo la meta establecida cero (0).
Si la entidad lo prefiere puede establecer un indicador por cada riesgo para ejercer un mejor control sobre la ejecución de lo programado.

4.2. 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 y Mediana 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.

4.3. 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 seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.
- Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.
- 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.

Es importante tener presente que una vez que el plan de tratamiento se haya ejecutado en las fechas y con las disposiciones de recursos previstas, la entidad debe valorar nuevamente el riesgo y verificar si el nivel disminuyó o no (es decir, si se desplazó de una zona mayor a una menor en el mapa de calor) y luego, compararlo con el último nivel de riesgo residual.

4.4. FASE 4: Mejoramiento Continuo

La Entidad debe garantizar la mejora continua de la gestión de los riesgos de seguridad y privacidad de la información, por lo tanto, debe establecer que cuando existan hallazgos, falencias o incidentes de seguridad y privacidad de la información se debe mitigar el impacto de su existencia y tomar acciones para controlarlos y prevenirlos. Adicionalmente, se debe establecer y hacer frente a las consecuencias propias de la no conformidad que llegó a materializarse.
Deben definirse las acciones para mejorar continuamente la gestión de riesgos de seguridad y privacidad de la información de la siguiente manera:

- Revisar y evaluar los hallazgos encontrados en los informes de los entes de control.
- Establecer las posibles causas y consecuencias del hallazgo.
- Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.
- Emprender acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la entidad o de los servicios que presta al ciudadano.
- Adicionalmente, se sugiere llevar un registro documentado del tratamiento realizado al hallazgo, así como las acciones realizadas para mitigar el impacto y ver el resultado para futuros hallazgos.

	Actualizado por:	Revisado por:	Aprobado por:
Firma			
Nombre	JHON JAIRO FIGUEROA	ISABEL CABRERA	RIGOBERTO MELO ZAMBRANO
Cargo / Rol	Profesional Universitario Líder GSI	Subgerente Administrativa y Financiera	Gerente

	Visto Bueno.
Firma	
Nombre	
Cargo	Líder GDC