PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CON ENFOQUE EN RIESGOS

Contenido

Introducción

La necesidad de contar con información clara y confiable que sea soporte para la toma de decisiones y permita reflejar el mejoramiento logrado a través de las medidas y planes de mejoramiento elaborados con respecto a los resultados no esperados.

En el marco de la política TIC se establecen en este documento los lineamientos de seguridad de la información para la ESE Hospital Marco Fidel Suárez, los cuales describen los comportamientos que deben asumirse por parte de los colaboradores del Hospital, sus contratistas y en general todas aquellas personas que hagan uso de su red de datos e infraestructura TIC.

La ESE Hospital Marco Fidel Suárez, a través de su Sistema de Gestión de Seguridad de la Información (SGSI), el Modelo de Seguridad y Privacidad de la Información (MSPI) de Gobierno en Línea (GEL) y teniendo en cuenta que la información es inherente a la misión de las instituciones y su correcta gestión debe apoyarse en tres atributos fundamentales:

- ✓ Confidencialidad: la información debe ser sólo accesible a sus destinatarios predeterminados.
- ✓ Integridad: la información debe ser correcta y completa.
- ✓ Disponibilidad: la información debe estar disponible en el momento y lugar que se requiera.

Dichos atributos serán aplicados a los procesos estratégicos, misionales, de apoyo y de evaluación de la ESE, por tal motivo, deberán ser conocidos y cumplidos por todo el recurso humano (servidores públicos, proveedores y terceros), que accedan a los sistemas de información e instalaciones físicas de la Institución.

El Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, de Gobierno en Línea, se encuentran basados, en el marco de lo establecido, en la norma internacional NTC-ISO-IEC 27001:2013 y las buenas prácticas contenidas en el componente Seguridad y Privacidad de la Información, de la estrategia GEL, este último desarrollado por el Ministerio de Tecnologías de la Información y las Comunicaciones en Colombia.

El plan general de seguridad de la información busca brindar seguridad, entendiéndola como la preservación de la confidencialidad, integridad y disponibilidad

de la información, así como de los sistemas que la soportan, incrementando los niveles de confianza en los servidores públicos, pacientes, clientes internos y externos, todo lo anterior, es fortalecido mediante el cumplimiento de todos los requisitos legales, reglamentarios y contractuales, que le sean de aplicación.

La norma ISO 27005:2011 es un estándar diseñado para la gestión de la seguridad de la información que contiene diferentes procedimientos y directrices, que permiten establecer los riesgos que enfrenta una organización y poder mitigarlos de la mejor manera.

Este plan de riesgos busca reducir las pérdidas de información y brindar protección de la misma, permitiendo conocer las debilidades que afectan, no solo en la prestación del servicio si no posterior a este durante la administración de la información recolectada.

Este plan enfocado en riesgos se ha desarrollado pensando en las diferentes etapas de la metodología PHVA donde inicialmente se realizará un diagnóstico en todas las áreas identificando todos los riesgos de la información y su medición de impacto en la institución. Luego se procederá a medir estos riesgos mediante los indicadores de los controles y dado el caso que se haya materializado algún riesgo se procederá a realizar el plan de mejoramiento para corregir el control sobre este riesgo.

La Alta Dirección de la ESE Hospital Marco Fidel Suárez se compromete a la implantación, mantenimiento y mejora del SGSI, y el MSPI de GEL(Gobierno en Linea), dotándolos de aquellos medios y recursos que sean necesarios e instando a todos los empleados, proveedores y partes interesadas, para que asuman este compromiso. Para ello, la ESE Hospital Marco Fidel Suaréz implantará las medidas requeridas para la formación y concientización de los servidores públicos, proveedores y partes interesadas, en temas de seguridad de la información.

A su vez, cuando exista una violación de las políticas de seguridad de la información, la gerencia se reserva el derecho de aplicar las medidas disciplinarias, acordes a los compromisos laborales de los empleados públicos, proveedores y partes interesadas, dentro del marco legal aplicable y dimensionadas al impacto que tengan sobre la ESE Hospital Marco Fidel Suaréz.

La responsabilidad general de la seguridad de la información en la ESE Hospital Marco Fidel Suárez recaerá sobre gerencia, subgerente administrativo, coordinador de sistemas de información y el Líder de Tecnología o Técnico del área de Sistemas. Por otro lado, todos los empleados públicos, proveedores y partes interesadas, tendrán la obligación de reportar los incidentes, en materia de seguridad, haciendo uso de las directrices establecidas por el manual de seguridad de la ESE Hospital Marco Fidel Suárez.

Todo lo definido en el Modelo General de Seguridad de la Información se concretará y desarrollará, mediante las buenas prácticas del mismo, normativas internacionales y procedimientos incluidos en el Sistema de Gestión de Calidad de la Institución, las cuales se integrarán, en la medida de lo posible, con otros sistemas de gestión, compartiendo aquellos recursos en pro de la optimización y buscando la mejora continua de la eficacia y eficiencia de la gestión de los procesos institucionales.

El área de TIC debe velar porque la información sea correcta y completa, esté siempre a disposición del cumplimiento de las metas de la institución y sea utilizada sólo por aquellos que tienen autorización para hacerlo, los lineamientos aquí definidos se establecen para garantizar el cumplimiento de los atributos de la información antes planteados.

Mediante este plan se busca identificar los riesgos presentes en la ESE Hospital Marco Fidel Suárez en cuanto a la información almacenada y administrada por sus funcionarios, para que de este modo se pueda evitar su materialización mediante la implementación de controles y dado el caso que estos controles fallen el daño causado no sea perjudicial para la continuidad del negocio y sobre todo incentivar al personal a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos.

Objetivo General:

El objetivo principal es desarrollar un plan de gestión de seguridad y privacidad de la información que permita minimizar los riesgos de pérdida de activos de la información y mantenerlos en un ambiente razonablemente seguro, alineado a la misión de la ESE. Hospital Marco Fidel Suárez y que permita proteger los activos de información de la misma, así como el uso adecuado de los recursos y gestión del riesgo, con el fin de preservar la disponibilidad, integridad y confidencialidad de la información y el aseguramiento de la continuidad de todos y cada uno de los procesos administrativo-asistenciales.

Objetivos Específicos:

- Proteger los activos de información de la ESE Hospital Marco Fidel Suárez, con base en los criterios de confidencialidad, integridad y disponibilidad.
- Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.
- Sensibilizar y capacitar a los servidores públicos, proveedores y partes interesadas acerca del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, de Gobierno en Línea, fortaleciendo el nivel de conciencia de estos, en cuanto a la necesidad de

salvaguardar los activos de información institucionales.

- Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico, revisiones por parte de la Alta gerencia y auditorías internas planificadas a intervalos regulares.
- Implementar acciones correctivas y de mejora para el Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, de Gobierno en Línea.
- Impartir lineamientos para la generación de información válida y confiable en todas las áreas de la institución.
- Garantizar la conservación y custodia de la información.
- Implantar normas claras de uso y manejo de las herramientas informáticas.
- Documentar las obligaciones de los funcionarios frente al manejo adecuado y administración de la información.
- Establecer horarios y requisitos en los archivos de la institución para garantizar la seguridad y conservación de la información de la institución.
- Proteger los activos de información de la ESE Hospital Marco Fidel Suaréz, con base en los criterios de confidencialidad, integridad y disponibilidad.
- Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables. Sensibilizar y capacitar a los servidores públicos, proveedores y partes interesadas acerca del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, de Gobierno en Línea, fortaleciendo el nivel de conciencia de estos, en cuanto a la necesidad de salvaguardar los activos de información institucionales.
- Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico, revisiones por parte de la Alta gerencia y auditorías internas planificadas a intervalos regulares.
- Implementar acciones correctivas y de mejora para el Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, de Gobierno en Línea.
- Establecer las guías con las cuales se realizará la identificación y categorización de los riesgos de la información.
- Establecer los controles y políticas de la seguridad de la información que garantice la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información.
- Proyectar el mapa de riesgos informáticos de la ESE Hospital Marco Fidel Suárez donde se establece el contexto.

SUBPROCESO CONTINGENCIA RECUPERACION Y RETORNO A LA NORMALIDAD

1. Objetivo

Definir las actividades que permiten implementar el plan de contingencia, recuperación y retorno a la normalidad de la plataforma de información de la ESE Hospital Marco Fidel Suárez, cuando se materialice algún tipo de desastre, que anule las operaciones de los recursos informáticos y/o servicios de la Institución.

2. Alcance

Inicia con la identificación del tipo de desastre materializado y finaliza con la elaboración de un informe final, donde se evidencien las afectaciones, acciones tomadas y resultados.

3. Responsabilidades

Área de Tecnología y Comunicaciones: Debe identificar el tipo de desastre materializado, debe informar inmediatamente a la Alta gerencia de la ESE Hospital Marco Fidel Suárez, sobre la materialización del desastre y los daños preliminares identificados. Deberá definir el tiempo de recuperación del servicio en condiciones de operación limitada y el tiempo máximo de recuperación en condiciones de operación plena. Debe elaborar un informe final, donde se evidencien las afectaciones, acciones tomadas y resultados.

El área de Tecnología debe poner en práctica, inmediatamente, el Plan de Contingencia, Recuperación y Retorno a la Normalidad.

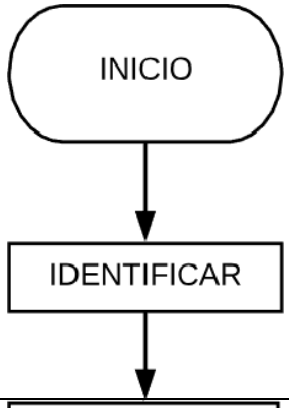
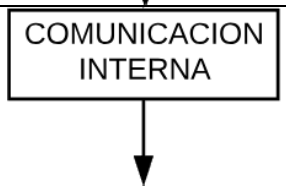
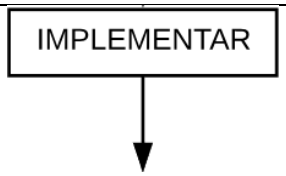
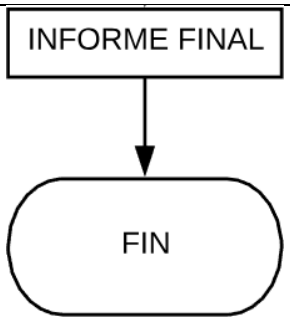
Las diferentes áreas de la ESE Hospital Marco Fidel Suárez se encargan de elaborar el plan de continuidad de cada proceso a su cargo en caso de presentarse alguna contingencia, es decir, cada una (y en conjunto) definen las acciones que deben ejecutar en sus procesos para garantizar que la ESE Hospital Marco Fidel Suárez sigue prestando sus servicios mientras el Área de TIC está ejecutando la recuperación o el restablecimiento de los servicios de TIC.

4. Definición de términos

Desastre Natural: Hace referencia a las enormes pérdidas materiales y vidas humanas ocasionadas por eventos o fenómenos naturales como los terremotos, inundaciones, tsunamis, deslizamientos de tierra, deforestación, contaminación

ambiental y otros.

Desastre ocasionado por el hombre: Es toda acción, consciente o inconsciente, llevada a cabo por el hombre, que pone en riesgo la continuidad de las operaciones de un negocio o servicio determinado. Ejemplo, ataque hacking, conato de incendio, entre otros.

	DIAGRAMA	ACTIVIDAD-DESCRIPCIÓN	RESPONSABLE	REGISTRO
1		IDENTIFICAR: El área de Tecnología y Comunicaciones debe identificar el tipo de desastre materializado. Tipos de Desastres: 1. Naturales 2. Provocados por el hombre	Área de Tecnología y comunicaciones	N/A
2		COMUNICACIÓN INTERNA: El área de Tecnología y Comunicaciones debe informar, inmediatamente a los coordinadores, administrador y Gerencia, sobre la materialización del desastre y los daños preliminares identificados.	Gerencia	
3		IMPLEMENTAR: El Líder de Tecnología debe poner en práctica, inmediatamente, el Plan de Contingencia, Recuperación y Retorno a la Normalidad.	Gerencia	Plan de contingencia
4		INFORME FINAL: El área de Tecnología y Comunicaciones debe elaborar un informe final, donde se evidencien las afectaciones, acciones tomadas y resultados.	Área de Tecnología y Comunicaciones	Informe Final

SUBPROCESO COPIA DE RESPALDO DE LA INFORMACION

1. Objetivo

Definir las actividades que permiten realizar las copias de respaldo, de los recursos informáticos y sistemas de información de la ESE HMFS, garantizando con esto la preservación de la disponibilidad de los datos generados, procesados y custodiados por la Institución.

2. Alcance

Inicia con la identificación de la información institucional que necesita ser respaldada con copias de seguridad y los respectivos tiempos de ejecución de la tarea y finaliza con la actividad de verificación del espacio de almacenamiento, definido para las copias de respaldo.

3. Responsabilidades

Profesional área de Tecnología y líderes de procesos administrativo asistencial:

- Definir con los Propietarios y/o Custodios de la información, qué documentos y/o sistemas de información deben estar incluidos en la tarea de copia de respaldo y los tiempos de realización de la actividad.
- Definir el lugar donde se almacenará la copia de respaldo (servidor), la partición, la estructura de los directorios, entre otras condiciones. Definir el método de realización de la actividad de copia de respaldo.

Propietarios y/o Custodios de la información:

Definir con el Profesional del área de Tecnología y Comunicaciones, qué documentos y/o sistemas de información deben estar incluidos en la tarea de copia de respaldo y los tiempos de realización de la actividad.

Profesional de Infraestructura TI:

- Programar la tarea de copia de respaldo, en la herramienta definida y aprobada para tal fin.
- Ejecutar la tarea de copia de respaldo manual, de acuerdo a los lineamientos definidos por el área.
- Verificar que la copia de respaldo realizada se almacenó en el servidor apropiado, en la partición adecuada y en la carpeta definida para tal fin.

4. Definición de términos

Copia de seguridad: También conocida como "copia de respaldo". En tecnologías de la información es una copia de los datos originales, que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Herramienta de Backup: Es un programa o software que se utiliza para garantizar la actividad de copia de respaldo de la información de manera automática. Permite

definir una serie de parámetros para automatizar la actividad, en un periodo definido por el administrador.

Información: Datos dotados de significado y propósito para la ESE HMFS.

Instructivo: Permite darle cumplimiento a una tarea o actividad determinada, mediante una secuencia paso a paso, que puede ser interpretada como una serie de instrucciones a seguir. Los instructivos también pueden hacer uso de imágenes que permiten ganar claridad en la secuencia a seguir.

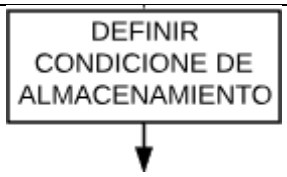
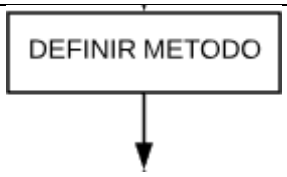
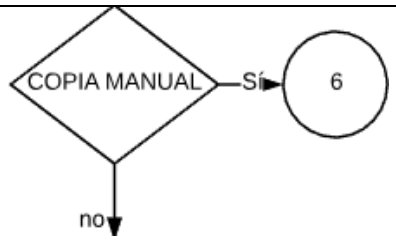
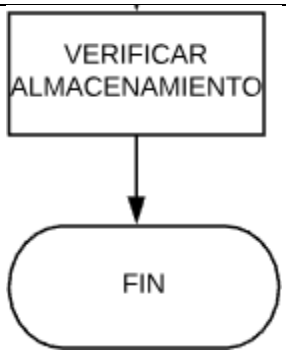
	DIAGRAMA	ACTIVIDAD DESCRIPCION	RESPONSABLE	REGISTRO
1		ACTUALIZAR PLATAFORMA DE INFORMACION: Los propietarios y/o custodios de la información deben almacenar la información en los archivos, rutas, o bases de datos definidas para tal fin, con el objetivo de Mantener actualizada la plataforma de información.	Profesional área de Tecnología. Líderes de los procesos Administrativos y/o asistenciales	Plataforma de información.
2		DEFINIR CONDICIONES DE ALMACENAMIENTO: El Profesional área de Tecnología, debe definir el lugar donde se almacenará la copia de respaldo (servidor), la partición, la estructura de los directorios, entre otras condiciones.	Profesional área de Tecnología.	N/A
3		DEFINIR METODO: El Profesional área de Tecnología, debe definir el método de la realización de la actividad del copia de respaldo. Este puede ser automático o manual.	Profesional área de Tecnología.	N/A

	DIAGRAMA	ACTIVIDAD DESCRIPCION	RESPONSABLE	REGISTRO
4		COPIA MANUAL: Si la copia es manual, el profesional del área de Tecnología debe ejecutar la tarea de copia de respaldo manual, de acuerdo a los lineamientos definidos por el área y continuar con el paso 6. De lo contrario debe programar la tarea.	Profesional área Tecnología.	Log de Transacción.
5		PROGRAMAR TAREA: El profesional del área de Tecnología debe programar la tarea de copia de respaldo en la herramienta definida y aprobada para tal fin.	Profesional área de Tecnología.	Log de Transacción.
6		VERIFICAR ALMACENAMIENTO: El profesional del área de Tecnología debe verificar que la copia de respaldo manual o automática realizada, se almaceno en el servidor apropiado, en la partición adecuada, y en la carpeta definida para tal fin.	Profesional área de Tecnología.	Log de Transacción.

SUBPROCESO RESTAURACION DE INFORMACION

1. Objetivo

Definir las actividades que permiten realizar una correcta restauración de la información recolectada, procesada y custodiada por el área de Informática, permitiendo identificar cualquier novedad, relacionada con la integridad de los datos institucionales, almacenados en las copias de respaldo existentes.

2. Alcance

Inicia con la definición de la frecuencia de ejecución de las actividades de restauración de la información institucional y finaliza con la actividad de informar los resultados obtenidos.

3. Responsabilidades

Profesional de área de Tecnología y Comunicaciones:
- Definir la frecuencia de ejecución de las actividades de restauración de la información.
- Seleccionar la(s) copia(s) de respaldo a restaurar.
- Seleccionar el personal del área, que será el responsable de ejecutar la tarea de restauración.

Personal seleccionado:
- Restaurar la información de las copias de respaldo almacenadas, de acuerdo a los lineamientos internos del área.
- Realizar una actividad de comprobación o verificación de la información restaurada.
- Informar al Profesional de Gestión de Informática y Comunicaciones, las novedades identificadas, al concluir la tarea.

4. Definición de términos

Información: Grupo de datos ya supervisados y ordenados, que sirven para construir uno o varios registros.

Instructivo: Permite darle cumplimiento a una tarea o actividad determinada, mediante una secuencia paso a paso, que puede ser interpretada como una serie de instrucciones a seguir. Los instructivos también pueden hacer uso de imágenes que permiten ganar claridad en la secuencia a seguir.

Integridad: Es el estado en que se encuentra algo. Una información es integra cuando, después de elaborada y/o alojada en algún sistema de información, no se experimenta ninguna modificación sobre ella, sin previa autorización de su propietario. También dentro del concepto de integridad, cabe destacar la veracidad de la información, puesto que una información es integra cuando es veraz también.

Restauración: Es la acción que permite devolver algo, al estado o circunstancia, en la que se encontraba antes.

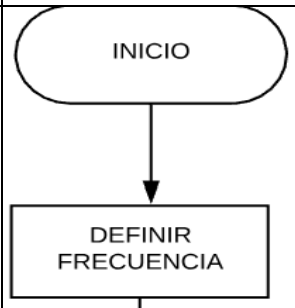
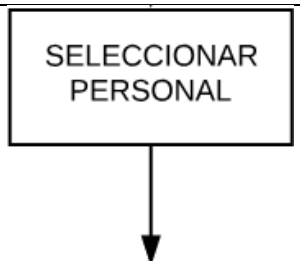
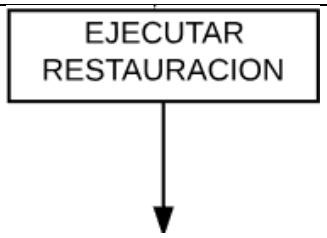
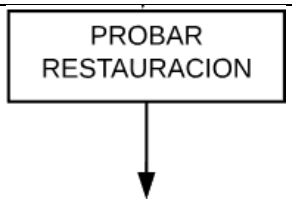
	DIAGRAMA	ACTIVIDAD-DESCRIPCIÓN	RESPONSABLE	REGISTRO
1		DEFINIR FRECUENCIA: El Profesional de Tecnología debe definir la frecuencia de ejecución de las actividades de restauración de la información, de acuerdo a los lineamientos internos del área.	Profesional área de Tecnología.	Documento con lineamientos internos del área.
2		SELECCION DE COPIA DE RESPALDO: El Profesional de Tecnología debe seleccionar la(s) copia(s) de respaldo a restaurar.	Profesional área de Tecnología.	N/A
3		SELECCIONAR PERSONAL: El Profesional área de Tecnología debe seleccionar al personal del área, que será el responsable de ejecutar la tarea e informarle por correo electrónico.	Profesional área de Tecnología.	Correo electrónico
4		EJECUTAR RESTAURACION: El personal seleccionado para ejecutar la tarea de restauración de la información de las copias de respaldo almacenadas, de acuerdo a los lineamientos internos del área y registra la información respectiva en el informe respectivo.	Profesional área de Tecnología.	Listade Chequeo de backup y restauración.
5		COMPROBAR RESTAURACION: El personal seleccionado para garantizar la actividad operativa de restauración de la información institucional debe realizar la comprobación o verificación de la información restaurada, con el objetivo de verificar si existe alguna afectación en la integridad de los datos.	Profesional área de Tecnología.	Lista de Chequeo de backup y restauración.

	DIAGRAMA	ACTIVIDAD-DESCRIPCIÓN	RESPONSABLE	REGISTRO
6		INFORMAR RESULTADOS: El personal seleccionado para garantizar las actividades operativas de restauración de la información institucional debe informar al personal de gestión informática y comunicaciones, las novedades identificadas, al construir la tarea.	Profesional área de Tecnología.	Correo electrónico

SUBPROCESO CREACION DE USUARIOS EN LAS PLATAFORMAS DE INFORMACION HMFS

1. Objetivo

Definir las actividades que permiten cumplir con la creación de las cuentas de acceso a los sistemas de información de la ESE HMFS, fortaleciendo con esto la preservación, confidencialidad, integridad y disponibilidad de la información de la institución.

2. Alcance

Inicia con el registro de los usuarios en el área de gestión humana y finaliza con la actividad de informar en el área solicitante de la cuenta sobre la creación y configuración en todas y cada una de las herramientas disponibles y que el usuario pueda y deba tener acceso mediante las credenciales de identificación de la cuenta asignada. Esta cuenta tendrá todos los detalles relacionados como nombre de usuario, contraseña, rol, permisos y privilegios otorgados con el fin de cumplir a cabalidad los procesos y procedimientos al interior de la ESE HMFS.

3. Responsabilidades

Profesional de Gestión Humana:

- Oficializar el ingreso de personal en el área de gestión Humana.
- El Personal de Gestión Humana debe comunicar al área de Informática el ingreso de los nuevos Empleados o Contratistas de la ESE HMFS.
- Solicitar la creación de cuentas del usuario en la red, correo electrónico, usuario en DGNET, SAIA, ETC. Donde debe especificar los permisos, privilegios, roles

y/o perfil del usuario, e informar a los líderes de las áreas la creación de los mismos.

Personal del área de Tecnología

- Crea usuario con los permisos requeridos por Gestión Humana.
- El área de Tecnología informa el área de gestión Humana Usuario y Clave.

4. Definición de términos

Empleado Público: Persona vinculada a la entidad mediante cualquier modalidad: carrera, provisional, ocasional, libre nombramiento y remoción, supernumerario y contratista.

Sistema de Información: Es un conjunto de componentes relacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información, con el objetivo de apoyar la toma de decisiones y el control en una organización.

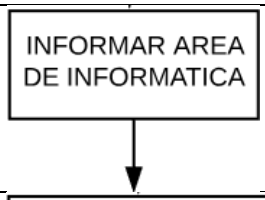
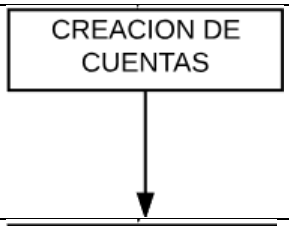
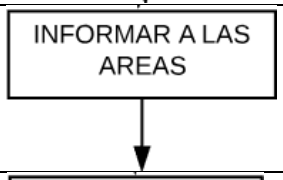
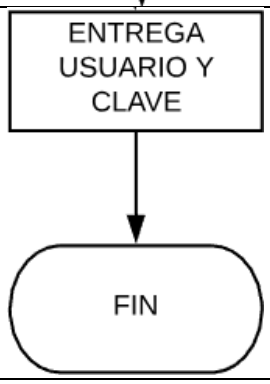
	DIAGRAMA	ACTIVIDAD-DESCRIPCIÓN	RESPONSABLE	REGISTRO
1		REGISTRO SISTEMA DE INFORMACION: Cumpliendo el proceso de selección y vinculación, y todos y cada uno de los requisitos en el área de gestión Humana.	Líder área Gestión Humana	Documentos de Ingreso a la ESE HMFS
2		El área de gestión humana informará al área de Tecnología el perfil y el rol del funcionario en la institución.	Profesional área de Tecnología.	Correo Electrónico
3		Personal del área de Tecnología verifica el rol con el fin de dar cumplimiento de las tareas y procesos.	Profesional área de Tecnología.	Log de registros

	DIAGRAMA	ACTIVIDAD-DESCRIPCIÓN	RESPONSABLE	REGISTRO
4		Luego de verificar el rol en la plataforma de información, se crea el usuario en la plataforma de información.	Profesional área de Tecnología.	Log de registros
5		El área de Tecnología informa al área de gestión humana el usuario y clave.	Profesional área de Tecnología.	Correo electrónico
6		El área de recursos humanos entrega usuario y clave al responsable del proceso en mención.	Líder área Gestión Humana	Correo electrónico

SUBPROCESO INTERCAMBIO DE INFORMACION DIGITAL

1. Objetivo

Definir las actividades que permiten cumplir con las solicitudes de intercambio de información institucional con terceros, garantizando niveles óptimos de preservación de la confidencialidad e integridad de la información durante la tarea.

2. Alcance

Inicia con la identificación del nivel de autorización de acceso, del tercero, a la información institucional y finaliza con el intercambio de información.

3. Responsabilidades

Del Propietario, Custodio de la Información, o Empleado Público:

- Identificar si el solicitante de la información tiene el nivel de autorización de acceso suficiente.
- Identificar la clasificación de la información, solicitada por el tercero.

- Identificar el método de intercambio de información.
- Informar al Profesional de Gestión de Informática y Comunicaciones, sobre la solicitud de intercambio de información institucional con un tercero (cuando la misma sea información Pública Clasificada o Reservada). Procede con el intercambio de información.

Del Profesional de sistemas de información:

- Verificar que el método de intercambio de información cumple con los requisitos de seguridad óptimos.
- Garantizar la preservación de la confidencialidad e integridad de la información a intercambiar con el tercero.
- Notificar al propietario de la información, custodio de la información, o servidor público, sobre el resultado de la verificación del método de intercambio y dar el visto bueno.

4. Definición de términos

Custodia de la información: Es un rol que cumplen todos los líderes· de áreas de la ESE HMFS.

Información Pública: Es toda información que su divulgación no pone en riesgo la integridad ni la imagen de la persona natural o jurídica.

Información Pública clasificada: Es aquella información semiprivada que es compartida entre un grupo de personas de la entidad, inclusive puede ser compartida con entes de control, pero no es de carácter público para personal ajeno a ESE HMFS.

Información Pública reservada: Es considerada información privada, teniendo en cuenta que su divulgación puede traer consigo daños de imagen e implicaciones jurídicas severas, tanto para la entidad, como para una persona natural. El acceso a la misma, lo efectúan un pequeño número de servidores públicos en la institución.

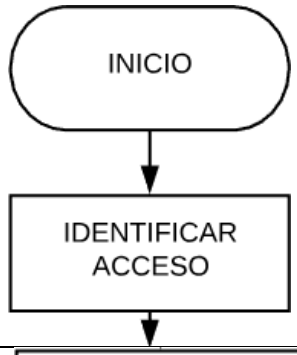
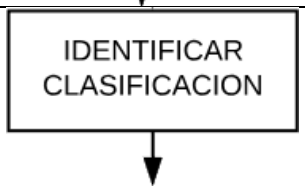
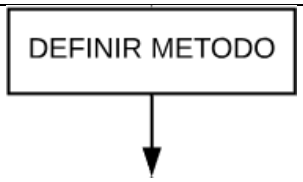
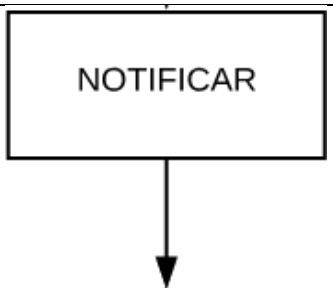
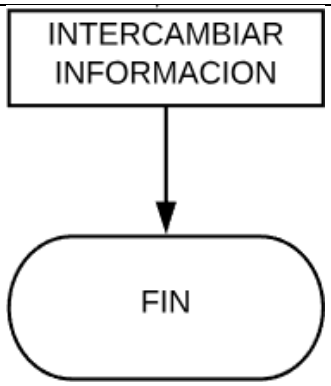
	DIAGRAMA	ACTIVIDAD DESCRIPCION	RESPONSABLE	REGISTRO
1		IDENTIFICAR ACCESO: El propietario de la información, custodio de la información o servidor público debe identificar si el solicitante de la información tiene el nivel de autorización de acceso suficiente.	Propietario de la información. Custodio de la información. Empleado público	N/A
2		IDENTIFICAR CLASIFICACION: El propietario de la información, custodio de la información o servidor público debe identificar la clasificación de la información solicitada porel tercero. Clasificación de Confidencialidad: 1. Información Publica 2. Información Publica Clasificada. 3. Información Publica Reservada.	Propietario de la información. Custodio de la información. Empleado público	N/A
3		IDENTIFICAR METODO: El propietario de la información, custodio de la información o servidor público debe identificar el método de intercambio de información: Método de Intercambio: 1. Mediante Sistemas de información. 2. Mediante mensaje de correo electrónico.	Propietario de la información. Custodio de la información. Empleado público	N/A
5		VERIFICAR METODO: El profesional del área de calidad (Profesional de Sistemas de Información) debe verificar que el método de intercambio de información cumple con los requisitos de seguridad óptimos; garantizando la preservación de la confidencialidad e integridad de la información a intercambiar con el tercero.	Profesional área de calidad. Profesional Sistemas de Información.	N/A

	DIAGRAMA	ACTIVIDAD DESCRIPCION	RESPONSABLE	REGISTRO
6		NOTIFICAR: El profesional del área de calidad (Profesional de Sistemas de información) debe notificar al propietario de la información, custodio de la información o servidor público, sobre el resultado de la verificación del método de intercambio y además dar el visto bueno.	Profesional Sistemas de Información.	Mensaje Correo Electrónico
7		INTERCAMBIAR INFORMACION: El propietario de la información, custodio de la información o servidor público, procede con el intercambio de información.	Propietario de la información. Custodio de la información. Empleado público	Mensaje Correo Electrónico

SUBPROCESO INTERCAMBIO INFORMACION FISICA

1. Objetivo

Definir las actividades que permiten cumplir con las solicitudes de intercambio de información institucional con terceros, garantizando niveles óptimos de preservación de la confidencialidad e integridad de la información durante la tarea.

2. Alcance

Inicia con la identificación del nivel de acceso a la información que posee el solicitante y finaliza con el envío de la documentación, a su respectivo destinatario.

3. Responsabilidades

Del Propietario, Custodio de la información, o empleado público:

- Identificar si el solicitante de la información tiene el nivel de autorización de acceso adecuado.
- Identificar la clasificación de la información, solicitada por el tercero.
- Implementar controles de seguridad para el transporte y entrega de la documentación clasificada como Pública Clasificada o Reservada.

- Consultar el procedimiento "Recepción y Radicación de Comunicaciones Oficiales Externas Recibidas, y Enviadas", para llevar esta actividad.

Del Profesional o Técnico de Correspondencia:

- Implementar controles de seguridad para el transporte y entrega de la documentación clasificada como Pública Clasificada o Reservada.
- Radicar la información en el archivo administrativo con el visto bueno de la gerencia. Requerido Para llevar a cabo esta actividad.
- Gestionar la actividad de envío de la documentación, a su respectivo destinatario.

4. Definición de términos

Custodia de la información: Es un rol que cumplen todos los líderes de áreas de la ESE HMFS.

Información Pública: Es toda información que su divulgación no pone en riesgo la integridad ni la imagen de la persona natural o jurídica.

Información Pública clasificada: Es aquella información semiprivada que es compartida entre un grupo de personas.

Información Pública reservada (Concepto mejorado): Es considerada información privada, teniendo en cuenta que su divulgación puede traer consigo daños de imagen e implicaciones jurídicas severas, tanto para la entidad, como para una persona natural. El acceso a la misma, lo efectúan un pequeño número de servidores públicos en la institución.

Empleado Público: Persona vinculada a la entidad mediante cualquier modalidad: carrera, provisional, ocasional, libre nombramiento y remoción, supernumerario y contratista.

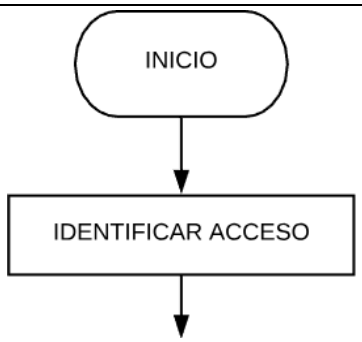
	DIAGRAMA	ACTIVIDAD DESCRIPCION	RESPONSABLE	REGISTRO
1		IDENTIFICAR ACCESO: El solicitante se debe presentar en el área de calidad donde el Profesional de sistemas de información debe identificar si el solicitante de la información tiene el nivel de autorización de acceso a la	Profesional Sistemas de Información	Plantilla de solicitud de información

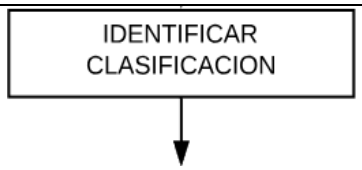
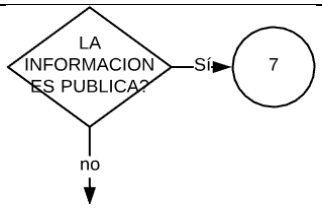
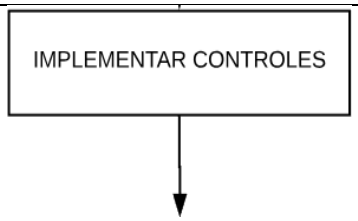
	DIAGRAMA	ACTIVIDAD DESCRIPCION	RESPONSABLE	REGISTRO
		información requerida.		
2		IDENTIFICAR CLADIFICACION: El Profesional de sistemas de información debe identificar la clasificación de la información requerida por el tercero. 1. Información Pública 2. Información Pública Clasificada 3. Información Pública Reservada	Profesional Sistemas de Información	Plantilla de solicitud de información
3		ESTABLECER CONTROLES: Si la información es publica, para el ítem 7 de lo contrario se debe implementar controles para trasporte y entrega.	Profesional Sistemas de Información	N/A
4		ESTABLECER CONTROLES: Si la información es publica Clasificada: 1. La información debe introducirse en un sobre. En la portada del sobre debe aparecer a quien va dirigido la información (Nombre de la persona y nombre de la entidad). El sobre debe estar cerrado. 2. El sobre anterior debe introducirse en otro sobre mas grande. En la portada del sobre debe aparecer a quien va dirigido el documento (Nombre de la persona, dirección, entidad, etc.) El sobre debe estar cerrado también.	Profesional Sistemas de Información	

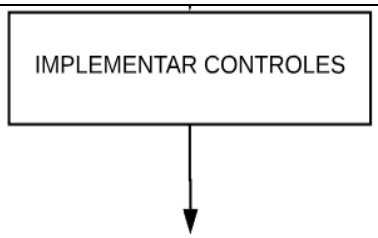
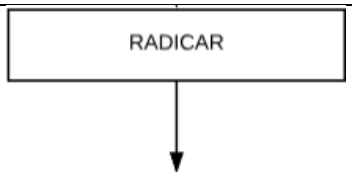
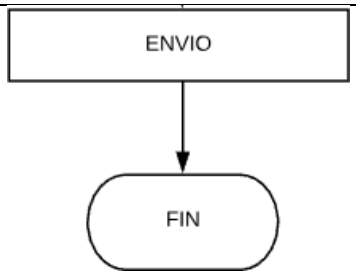
	DIAGRAMA	ACTIVIDAD DESCRIPCION	RESPONSABLE	REGISTRO
		3. La entrega del sobre a su destinatario no requiere que se realice a la mano del solicitante, ni tampoco se requiere que el solicitante firme algún otro recibo. Si la información es pública y reservada: 1. El propietario de la información debe tener conocimiento sobre la solicitud y además debe de dar su aprobación. 2. El documento se debe introducir en un sobre, en la portada del sobre debe aparecer a quien va dirigido el documento (nombre de la persona, dirección, entidad). El sobre debes estar sellado.		
5		3. El sobre anterior debe introducirse en otro sobre mas grande. En la portada del sobre debe aparecer a quien va dirigido el documento (Nombre de la persona, dirección, entidad, etc.) El sobre debe estar sellado también. Nota: En ninguno de los dos sobres debe aparecer la clasificación de la información contenida, ni tampoco su etiqueta correspondiente. 4. La entrega del sobre a su destinatario requiere que se realice a la	Profesional Sistemas de Información	

	DIAGRAMA	ACTIVIDAD DESCRIPCION	RESPONSABLE	REGISTRO
		mano del solicitante, y también se requiere que el solicitante firme registro de recibido.		
6		RADICAR: Para llevar a cabo esta actividad, el propietario de la información, custodio de la información, o funcionario público debe consultar el procedimiento de recepción y radicación de las comunicaciones externas recibidas y/o enviadas.	Coordinador Archivo	Registro software gestión Documental
7		Coordinador archivo administrativo gestiona la actividad de envió de la documentación a su respectivo destinatario, dejando evidencia de la radicación en el software de Gestión Documental.	Coordinador Archivo	Registro software gestión Documental

SUBPROCESO CONTROL DE DOCUMENTOS

1. Objetivo

Establecer mecanismos para el control de los documentos en la ESE Hospital Marco Fidel Suárez

2. Alcance

Inicia con el requerimiento de elaboración, modificación o eliminación de la documentación de los Sistemas de Gestión y termina con el ingreso del documento al listado de información documental respectivo y la publicación en el sitio web institucional.

3. Responsabilidades

Del Administrador de la Documentación:

Revisar, editar, registrar, distribuir, divulgar, controlar y en general administrar la documentación original que conforman los Sistemas de Gestión, así como el control de los cambios de dicha documentación. Los Sistemas de Gestión de la ESE HMFS son:

- Sistema de Gestión de Calidad
- Sistema de Seguridad de la Información.
- Sistema de Seguridad y Salud en el Trabajo.
- Sistema de Gestión Ambiental.
- Sistema de Gestión Documental.
- Modelo de Seguridad y Privacidad de la Información (Gobierno en Línea).

De los Líderes de los Procesos: Generar y solicitar creación o cambios a documentos actuales, implementar los documentos del proceso a cargo, controlar los documentos externos o de otros procesos que interactúen con su gestión y socializar con su personal a cargo la documentación vigente. Recoger copias obsoletas, si se trata de documentos a modificar o eliminar

Del Representante de la Dirección: Aprobar los documentos de los sistemas de gestión y controlar los documentos externos o de otros procesos que interactúen con su gestión.

4. Definición de términos

En este capítulo se definen términos que son de conocimiento común y que son necesarios para la comprensión y aplicación del procedimiento control de documentos. En caso de ser necesario se pueden utilizar términos técnicos contenidos en la norma NTCGP1000:2009 y algunos específicos como los siguientes:

- **Alcance**: Establece dónde inicia, dónde finaliza y dónde aplica el procedimiento en mención.

- **Aprobar un documento**: Acción de verificar que los resultados obtenidos al aplicarlo descrito en el documento son apropiados para cumplir los requisitos y la política de calidad de la Institución. Cuando sea aprobado el documento, se entiende que éste puede iniciar su distribución y divulgación.

- **Control**: Mecanismo para garantizar la disponibilidad de los documentos vigentes que conforman el sistema de calidad.

- **Custodia de la información**: Este rol lo cumplen todos los líderes de áreas.

- **Difusión**: Utilización de cualquier medio de comunicación para hacer conocer la información de los procesos documentados.

- **Distribuir**: Hacer entrega física de un documento aprobado o facilitar el acceso a éste para que sea utilizado por el personal involucrado en la actividad para el cumplimiento de los objetivos institucionales y para que permita asegurarse de la eficaz planeación, operación y control de los procesos.

- **Disposición final**: Manejo que se le debe dar a un documento una vez alcanza su periodo útil para la institución.

- **Divulgación**: Dar a conocer el contenido de un documento para que sea cumplido por el personal de la institución involucrado en la actividad descrita.

- **Documento**: Información y su medio de soporte.

- **Documento controlado**: Involucra los documentos de los procesos cuya distribución es restringida o controlada, los cuales deben ser actualizados permanentemente.

- **Documentos de origen interno**: Todos aquellos documentos generados por la ESE Hospital Marco Fidel Suárez tales como: propuestas, planes de calidad, instructivos, formatos, diagramas, procedimientos, manuales, tablas, compendios, etc.

- **Documento de origen externo**: Todos aquellos documentos suministrados por entes reguladores o de control, por el cliente, los proveedores y otros; tales como: diseños, especificaciones, manuales de productos o servicios, certificaciones de productos, fichas técnicas, leyes, normas, decretos, reglamentos, resoluciones, planes de manejo ambiental, contratos, garantías, etc.

- **Documento no controlado**: Son los documentos que se entregan solamente para consulta o que están en fase de elaboración y revisión para aprobación antes de su emisión, incluyen la entrega de copias físicas de documentos en donde no se requiere controlar su disponibilidad en los puestos de uso.

- **Documento obsoleto**: Documento cuya vigencia ha caducado.

- **Documento original**: Aquel que presenta la evidencia de la aprobación de su contenido (firmas) y sirve para tomar las copias para la distribución al proceso (es el documento controlado).

- **Documento Público**: Es el elaborado por funcionario público en ejercicio de su cargo o con su intervención.

- **Eliminación**: Retiro de un documento del sistema de gestión de calidad de circulación ya sea porque el proceso cambió radicalmente y obligó a que se elaborara un nuevo documento, o porque el proceso dejó de ejecutarse o sé fusionó con otro proceso o sistema de gestión.

- **Especificación**: Documento que establece requisitos.

- **Formato**: Documento empleado para el registro de información necesaria en un proceso o actividad específica, convirtiéndose así en un registro.

- **Listado maestro**: Es el inventario actualizado de documentos tanto internos como externos o datos que permite verificar y controlar la vigencia del documento y establecer su ubicación (en manos de quién se encuentra).

- **Manual del sistema integrado de Gestión**: Documento que articula de forma armónica e interdependiente los componentes de los Sistemas de Gestión de la Seguridad de la Información.

- **Objetivo**: Describe el propósito o el para qué del procedimiento control de documentos.

- **Procedimiento**: Forma específica de efectuar una actividad. Documento que especifica los pasos que debe seguir un proceso o actividad.

- **Propietario de la información**: Este rol lo cumplen todos los líderes de procesos.

- **Registro**: Es un documento debidamente diligenciado en el cual reposa una evidencia de una actividad realizada y la obtención de unos resultados planificados, para asegurar el cumplimiento y eficacia del Sistema de Gestión de la Calidad.

- **Revisar un documento**: Acción de asegurar la conveniencia, la adecuación, eficacia, eficiencia y efectividad del documento revisado para alcanzar unos objetivos. Corresponde a la forma como se hace en la institución. Actualizar las versiones.

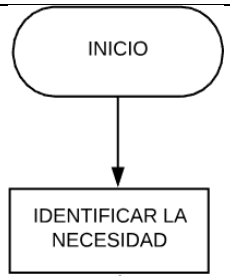
- **Tabla de retención documental**: Listado de series con sus correspondientes tipos documentales, a las cuales se asigna el tiempo de permanencia en cada etapa del ciclo vital de los documentos.

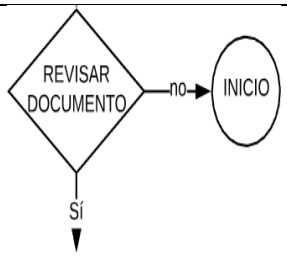
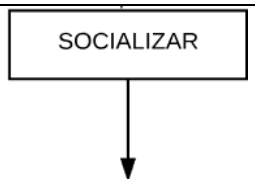
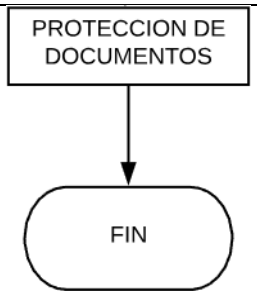
5. DESCRIPCIÓN DEL PROCEDIMIENTO

5.1. CRITERIOS PARA IDENTIFICAR CUÁNDO ES NECESARIO DOCUMENTAR Y CÓMO DOCUMENTAR

- Cuando la norma lo requiera o cuando exista una necesidad a nivel de gobierno.
- Cuando la institución requiera documentos para el cumplimiento de sus objetivos y que le permitan asegurarse de la eficaz planificación, operación y control de sus procesos. Todos los documentos del sistema de gestión de calidad deberán redactarse en idioma español, tendrán un encabezado similar al de este documento, el logo en la parte superior izquierda. En la sección central el nombre del documento y en la sección derecha código, versión, vigencia (fecha en la que entra en uso el documento), número de páginas y si es documento controlado, esta información se elaborará en mayúscula fija, en negrilla y en Verdana 11.
- Todos los documentos del Sistema de Gestión de la Calidad se elaborarán en letra Verdana 11, excepto los diagramas de flujo y formatos donde el tamaño de la letra podrá disminuir según la necesidad.
- En los documentos se deben conservar de ser posible los siguientes márgenes: Izquierdo: 3 cm, Derecho: 2 cm, Superior: 2 cm, Inferior: 2 cm.

5.2. ELABORACIÓN DE UN DOCUMENTO

		ACTIVIDAD DESCRIPCION	RESPONSABLE	REGISTRO
1		IDENTIFICAR NECESIDAD: Identificar La necesidad generar, revisar, actualizar o eliminar un documento y diligenciar solicitud mediante oficio al área de calidad. Remitirlo al correo electrónico del administrador de la documentación, junto con el documento generado o modificado.	Líder del proceso	Formato de Solicitud y envió al Correo Electrónico

		ACTIVIDAD DESCRIPCION	RESPONSABLE	REGISTRO
2		REVIZAR DOCUMENTO: Revisar el documento (procedimiento, instructivo, manual, Formato, otro), si requiere explicación pasa al numeral 1, en caso contrario pasa el numeral 3 con el respectivo visto bueno del administrador de la información.	Administrador de la documentación	Correo Electrónico
3		Aprobar el documento y devolverlo al administrador de la información para su respectiva divulgación y distribución.	Líder área de calidad	Documento Firmado
4		Actualizar listados maestros de documentación. Si el documento fue clasificado con información pública se realiza la respectiva solicitud al administrador del sitio web para su publicación. Si se trata de documentos a modificar o eliminar recoger copias obsoletas.	Administrador de la información. Administrador sitio WEB. Líderes del proceso	Publicación en el Sitio WEB institucional.
5		SOCIALIZACION El líder del proceso socializará con su equipo de trabajo los cambios realizados y remitirá por Correo electrónico a los procesos que requieran conocer la respectiva información. Se publicará la información en la intranet de la institución y/o página web.	Líder del proceso	Correo electrónico
6		PROTECCION DE DOCUMENTOS: Los controles de seguridad para la documentación se definirían con base al criterio de clasificación de confidencialidad definido por su propietario y/o custodios, de conjunto con el personal del archivo administrativo.	Propietario y/o custodio Profesional Sistemas de Información	Matriz de inventario de activos de información tipo documental

5.3. REVISIÓN O ACTUALIZACIÓN DE UN DOCUMENTO

Cada líder de proceso será responsable de asegurarse que todos los procedimientos que aplican a sus procesos se encuentran establecidos, documentados, implementados y mantenidos, en caso de que se identifique la necesidad de

modificación de alguno de los documentos se deben seguir los parámetros establecidos en las actividades 1 a 6 del procedimiento.

Los documentos de los Sistemas de Gestión tales como manuales, procedimientos e instructivos, deben revisarse por el líder del proceso una vez cada dos años, o antes si es necesario, esto con el fin de asegurar su continua adecuación.

5.3.1. Identificación y control de cambios y estado de revisión actual de los documentos de origen interno:

El líder de cada proceso es responsable de controlar los documentos de origen interno que afecten directamente el proceso bajo su responsabilidad.

La identificación de los documentos de los Sistemas de Gestión se realizará por medio del código y nombre de cada documento relacionado en la lista maestra de documentos, adicionalmente el estado de revisión actual se identificará con el número de versión de cada documento, el control de cambio de versión se relacionará en cada documento en "Estado de Revisión y Aprobación". Así mismo, se descubrirá la clasificación de confidencialidad, integridad y disponibilidad de la documentación.

Debe asegurarse de que las versiones aplicables se encuentren en los puntos de uso: Para ello, el administrador de la documentación debe mantener actualizado las Tablas de Retención documental.

5.3.2. Identificación y control de los documentos de origen externo:

El líder de cada proceso es responsable de controlar los documentos de origen externo que afecten directamente el proceso bajo su responsabilidad.

Los documentos de consulta (leyes, resoluciones, decretos, manuales, procedimientos, instructivos) que apliquen a cada proceso deben registrarse en el Normograma.

5.4. ELIMINACIÓN DE UN DOCUMENTO

Identificación y control de documentos obsoletos: Cuando un documento sea modificado o eliminado según el presente procedimiento, la versión obsoleta o anterior debe identificarse con un sello de "DOCUMENTO OBSOLETO". El administrador .de la documentación debe solicitar al líder del proceso que recoja o elimine las copias obsoletas (en caso de existir) para destruirlas y las debe cambiar por las versiones actualizadas.

El original de los documentos obsoletos debe archivarse por el administrador de la documentación.

5.5. TIPOS DE DOCUMENTOS

Tipos de documentos que soportan la planeación, operación y control de los procesos:

5.6. CODIFICACIÓN DE DOCUMENTOS DEL SISTEMA INTEGRADO DE GESTIÓN

Se establece el criterio para codificar los documentos, el cual obedece a una estructura alfanumérica. En este documento se indica el significado de cada uno de los caracteres.

El responsable de la asignación del código de cada uno de los documentos del sistema de gestión de calidad es el administrador de la documentación y él mismo lo formaliza en el Listado Maestro de Documentos.

Archivo clínico

La dependencia de archivo clínico se regirá por las normas contenidas en el código de ética de la ESE Hospital Marco Fidel Suárez y teniendo presente en todo momento la práctica de los DEBERES Y DERECHOS del usuario, quien es nuestra razón de ser.

Horario de Servicios

De lunes a viernes, en el horario de 7:00 a.m. a 17:00 p.m., se prestará el servicio por parte del personal adscrito al archivo clínico y/o archivo

administrativo, quien es el único personal autorizado para ingresar al archivo clínico de la institución.

Acceso al archivo:

Solamente tendrán acceso al archivo clínico los miembros del Equipo de salud (Médico, enfermera, auxiliar de enfermería, técnicos de rayos x) o personal no asistencial con funciones de vigilancia y control: Auditor médico, Control interno.

El archivo deberá permanecer con llave, cuando no esté atendido por personal autorizado.

Parágrafo: el personal de servicios generales solo ingresa para realizar las actividades propias de su labor, en presencia del personal adscrito al archivo clínico.

Seguridad y custodia de la historia clínica:

a. Las historias clínicas de pacientes egresados de hospitalización se recogerán diariamente a las 7:00 a.m. por el personal de archivo clínico quien está a cargo de la realización del censo diario de pacientes.
b. Cada vez que entre o salga una historia clínica se debe registrar en el aplicativo de entradas y salida para garantizar un control sobre la historia clínica
c. Las historias clínicas que salgan para consulta externa deben ser entregadas al archivo clínico el mismo día, cuya responsabilidad estará a cargo del personal del archivo clínico.
d. Las historias clínicas de los servicios de hospitalización, urgencias y cirugía deben ser recogidas por el personal de archivo clínico todos los días de la semana (lunes a viernes) a las 7:00 a.m.
e. Las Historias clínicas que sean prestadas para asuntos administrativos deberán ser devueltas al archivo clínico por la persona responsable en máximo 24 horas.
f. Las historias clínicas que lleguen al archivo se organizarán el mismo día.
g. Las historias clínicas sólo podrán ser retiradas de su lugar en el archivo y distribuidas por las personas del equipo de salud.
h. Toda salida de historias clínicas debe dejar registro en el tarjetón de reemplazo y en la base de datos de entradas y salidas.
i. Solo manejarán llaves las auxiliares administrativas del archivo clínico.

j. Está prohibido el ingreso y consumo de alimentos sólidos y líquidos dentro del archivo; así mismo por motivos de seguridad y salubridad se prohíbe fumar.
k. La Empresa garantizará la integridad física y técnica, sin adulteración o alteración de la información contenida en las historias clínicas, bajo condiciones locativas, ambientales y materiales.

Solicitud de copia de la historia clínica.

Solamente se entregará copia del contenido de la historia clínica, en los siguientes casos:

a. Al titular de la historia clínica, previa identificación.
b. A los padres, en representación de menores de edad, previa demostración del parentesco.
c. A terceros con autorización firmada y autenticada del titular.
d. A las autoridades competentes, específicamente reglamentadas en la resolución 1995 de 1999.

Parágrafo: El costo de las copias estará a cargo del solicitante, excepto por requerimientos legales.

Ingreso y salida de las historias clínicas.

Toda historia clínica que sea solicitada por un servicio, profesionales de la salud, encargados de facturación o personal administrativo debe estar acorde con el procedimiento establecido en la institución.

Transporte de la Historia Clínica:

a. El transporte de la historia clínica a hospitalización, cirugía y urgencias lo hará el camillero, la auxiliar de archivo clínico, la auxiliar de enfermería, enfermera ó médico.
b. Los traslados de las historias clínicas entre las diferentes sedes o anexos de la institución se harán previo registro CONTROL DE DOCUMENTOS ENVIADOS Y RECIBIDOS (Archivo Administrativo).

Búsqueda de las historias clínicas.

El personal del archivo propenderá por la búsqueda y suministro oportuno de las historias solicitadas previamente por los diferentes servicios, según lo estipulado en el procedimiento.

Será prioritaria la búsqueda de las Historias Clínicas requeridas para los procedimientos de auditoría, entes de control y atención oportuna al paciente.

Parágrafo: Cuando no se encuentre una historia clínica, debe atenderse al usuario diligenciando los registros clínicos requeridos y debe reportarse como historia clínica perdida en el registro según manual de procedimientos, y posteriormente debe realizarse la consolidación de la historia clínica si esta se encuentra y de encontrarse se debe colocar la fecha de aparición de la misma en el registro de historias clínicas perdidas.

Informes.

El funcionario de archivo clínico es el responsable de mantener actualizado el formato de historias clínicas perdidas y entradas y salidas de las historias clínicas.

Disposiciones varias.

a. El uso de la extensión telefónica es exclusivo para el personal de la dependencia y a lo máximo debe ser utilizada únicamente en las labores inherentes a su oficio.
b. El personal de archivo clínico en su horario de trabajo debe portar siempre su escarapela.

Archivo administrativo

a. El acceso al archivo administrativo es restringido, el ingreso es solo para la persona encargada de esta área y auxiliares o practicantes autorizados por la administración para desempeñar labores de apoyo con previa inducción.
b. Toda la documentación que se entregue en el archivo administrativo será almacenada en una base de datos con la fecha y nombre del documento que se entrega para asegurar continuidad y oportunidad en el acceso a dicha información.
c. Para solicitar un documento conservado en el archivo administrativo, se debe contar con la autorización de la administración o de la gerencia en caso tal de que lo amerite, si es un funcionario de la institución debe hacer el requerimiento al archivo administrativo para que le sea entregado el documento.

Hardware y software

a. El mantenimiento de los activos informáticos debe ser permanente, tanto componentes como soporte técnico, migración a nuevas necesidades y tecnologías.

b. Las interfaces deben facilitar el acceso a los servicios, de modo que se puedan utilizar de una forma rutinaria sin esfuerzo y deben prevenir los errores del usuario.
c. Todos los equipos de la institución estarán asegurados.
d. Se harán auditorias semestrales para verificar que el sistema y los equipos no tenga copias ilegales o piratas.
e. Se restringirá el acceso de disco externos y/o memorias USB
f. Se restringirán los permisos a los equipos para evitar descargas de virus o programas ilegales.
g. Se implementarán barreras protectoras en los equipos como el Firewall, el Proxy, los dominios, entre otros softwares expertos en brindar seguridad a la información.
h. Se harán capacitaciones al personal sobre el manejo y uso de las herramientas informáticas.
i. Los aplicativos que se instalen en la institución deben sincronizarse con la fecha y hora correcta.
j. El uso de los equipos es para uso exclusivo de los funcionarios de la institución.
k. No exponer los equipos al sol o al agua para evitar su deterioro o daño permanente.
l. Los equipos son para uso únicamente de cumplimiento de las funciones de cada funcionario.
m. Para trasladar un equipo de un lugar a otro se debe contar con la autorización del personal de sistemas.
n. No se deberán instalar programas sin la debida autorización.
o. Los Software utilizados por la ESE Hospital Marco Fidel Suárez son de uso interno y sólo para ser utilizado en los procesos administrativo-asistenciales de nuestra institución.
p. No se debe entregar datos o reproducir total o parcialmente la información a personas ajenas de la ESE Hospital Marco Fidel Suárez o que no sean parte del proceso administrativo correspondiente.
q. El correo electrónico, internet e intranet son de uso exclusivo labores relacionadas con nuestras tareas o funciones de nuestra área, queda prohibido el uso para otros fines.
r. Se prohíbe la descarga de archivos, transmisión o almacenamiento que pudiera ser considerado pornográfico, difamatoria, racista, videos, música o que atente contra las buenas costumbres o principios, excepto que el trabajo lo amerite.

Manejo apropiado de las impresiones

a. Las impresoras solo podrán ser utilizadas para imprimir documentos requeridos por la institución.

b. Retirar los documentos que se envían a imprimir.
c. Todo documento que quede en la impresora al final del día debe ser eliminado.
d. En caso del mal funcionamiento en una impresora, o que está siendo mal utilizada, deberá informar al área de Tecnología de la ESE HMFS.
e. Cada área será la responsable de mantener los suministros correspondientes.
f. El material impreso que contenga información sensible no debe ser descuidado en áreas abiertas, debe ser removido de las impresoras sin demora.

Manejo apropiado de contraseña

a. Nunca guarde sus contraseñas, en ningún tipo de papel, agenda, etc.
b. Las contraseñas se deben mantener confidenciales en todo momento.
c. No compartir las contraseñas con otros usuarios.
d. Cambiar la contraseña si piensa que alguien más la conoce y si ha tratado de dar mal uso de ella.
e. Selecciona contraseñas que no sean fáciles de predecir.
f. Nunca grabe su contraseña en una tecla de función o en un comando de caracteres pre- definido.
g. Cambie sus contraseñas regularmente.
h. No utilizar la opción de almacenar contraseñas en Internet.
i. No utilizar contraseña con números telefónicos, nombre de familia etc.

Manejo apropiado de control de Virus

a. El sistema de actualizaciones y detección diaria es automatizado en la consola de antivirus.
b. Se debe comunicar de cualquier infección por virus que no fue eliminada por el antivirus al área de Tecnología.
c. Los usuarios no podrán bajo ninguna circunstancia desinstalar el producto de antivirus existente en su equipo.
d. Los dispositivos extraíbles antes de ser usados deben realizar scanner con el antivirus.

Manejo de cuentas de sistemas

a. Toda cuenta de acceso que se requiera modificar deberá ser solicitada a través de los administradores de los sistemas de información o en la opción de cambio de contraseña.
b. El procedimiento de creación de cuentas debe ser canalizado por el coordinador del área.
c. La cuenta de red es la que utilizará cada usuario para conectarse a su equipo PC, esta debe ser solicitada por el coordinador del área.
d. La cuenta de usuario software SAIA debe ser solicita por el líder del área.

e. La eliminación de cuentas se realizará de forma formal, por el área de recurso humano cuando el funcionario no tenga vínculo laboral con la institución o cuando este lo requieran, pero en situaciones especiales como suspensiones del personal, podrá ser enviado un correo por parte del jefe solicitando el bloqueo temporal de las cuentas del funcionario en cuestión formalizando a la brevedad.

Manejo de acceso a internet

a. El acceso a internet se encuentra protegido por filtros para disminuir sitios peligros que contenga código malicioso o que se encuentren ajenos al servicio, permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus.
b. No navegar por sitios no confiables.
c. Queda prohibido el uso de sitios de radios online.
d. Queda prohibido el uso de intercambio de archivos (Ares, emule, Torrents, Limewire, etc.).
e. Queda prohibido el uso de sitios de chat (Messenger, chat, etc.).
f. Queda prohibido el uso de internet para actividades ilícitas.
g. Queda prohibido la descarga que no cumpla con la normativa vigente de copyright y similar.
h. Se prohíbe el acceso a los sitios o páginas Web que contengan materiales amenazadores, pornográficos, racistas, sexistas o cualquier otro que degrade la calidad del ser humano, salvo aquellas requeridas por la naturaleza de las funciones institucionales del usuario.
i. No compartir sus claves para ingresar a sitios que lo requiera como Bancos, Correo, etc.
j. No permitir que el navegador de internet recuerde la contraseña automáticamente.
k. Está Prohibido participar en juegos de entretenimiento en línea.
l. Si no está navegando por internet, cierre todas las ventanas abiertas.
m. Cualquier archivo que se reciba o descargue de internet deberá revisarse con el antivirus para asegurar que no tenga virus.
n. El área de Informática tiene la facultad de suspender el servicio de navegación en internet bajo circunstancias que así lo requiera (Virus, mal uso de internet, trafico sospechoso, etc.).
a. Si requiere navegar en algún sitio bloqueado enviar correo a **jllano@hmfs.gov.co**, para su evaluación.

Manejo de correo electrónico

a. El área de informática cuenta con filtros para identificar y bloquear correos no deseados (Spam o Virus), archivos infectados o maliciosos.
b. El Correo electrónico es de uso exclusivo para las labores de nuestras funciones de la ESE Hospital Marco Fidel Suárez y queda restringido el uso para otros fines.
c. Se prohíbe expresamente el envío de archivos, transmisión o almacenamiento de cualquier información que pudiera ser considerada pornográfica, difamatoria, racista, música, videos, etc., o que atente contra las buenas costumbres o principios.
d. Todo correo ajeno que no pertenezca al dominio HMFS, no se entrega soporte o algún tipo de estabilidad.
e. La contraseña del correo debe ser cambiada periódicamente.
f. No dar click en link sospechosos llegados por correos electrónicos (bancos, tiendas, etc.).
g. No completar datos personales en correos electrónicos sospechosos.
h. Eliminar correo no deseado (spam o sospechoso).
i. No enviar correo que su tamaño se ha superior a 10MB.

Manejo de redes sociales

El área de Tecnología bloquea todo tipo de sitio relacionado con redes sociales, permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus, si algún funcionario por motivos de trabajo requiera acceder a ello, el coordinador o líder de área debe enviar la solicitud formal a informática, especificando los siguientes datos:

1. Nombre del funcionario
2. IP del equipo
3. Motivo

Cabe destacar que cualquier foto subida o comentario en acebook, twitter o en alguna red social es responsabilidad exclusiva del que la emite.

Manejo de software

b. Queda prohibida la instalación que no cumpla con las instrucciones del Área de Sistemas de Información.
c. Los usuarios no deben instalar ni descargar aplicaciones que podrían provocar alguna vulnerabilidad o inestabilidad en los servicios.
d. Toda solicitud debe ser canalizada al correo **jllano@hmfs.gov.co**

Manejo de dispositivos móviles

Para garantizar la seguridad y estabilidad de la red y los dispositivos móviles, se describen algunos concejos y manejo adecuado, de los dispositivos móviles.net:

a. Los teléfonos móviles de la ESE Hospital Marco Fidel Suárez se han adquirido específicamente para facilitar el desarrollo de actividades laborales relacionadas con la entidad y el uso para propósitos personales debe ser ocasional, racional y no debe obstaculizar las actividades laborales.
b. En caso de licencia o vacaciones del funcionario, el teléfono móvil debe quedar a disposición del área a la cual fue asignado.
c. La instalación, configuración, modificación o eliminación de software aplicativo sobre los dispositivos móviles es responsabilidad exclusiva del área de Informática.
d. No descargar ningún software que no se encuentre licenciado o que indique claramente que es de licencia libre.
e. Las actualizaciones de sistemas operativos de los dispositivos móviles, debe ser coordinado con el área de Tecnología, que es la responsable de realizar las actualizaciones.
f. Se debe mantener desactivada la red Wifi, Bluetooth, Infrarrojos, etc., en caso de que no esté siendo utilizada.
g. Es responsabilidad de cada funcionario hacer copias de seguridad de la información almacenada en el teléfono móvil, si no está seguro del proceso debe comunicarse con el Área de Tecnología.
h. Es responsabilidad del funcionario reportar inmediatamente al Área de Activos fijos, cualquier daño o pérdida del dispositivo móvil que le ha sido asignado.
i. Se debe solicitar al área de Tecnología la configuración y acceso a los correos de la ESE Hospital Marco Fidel Suárez, a los teléfonos móviles donde exista servicio disponible y que pertenezcan a la institución.
j. No insertar tarjetas de memoria sin haber comprobado previamente que están libres de virus o de algún tipo de código malicioso.
k. No acceder a los enlaces no solicitados a través de SMS/MMS/Email podría ser código malicioso.

Manejo computadores portátiles

Para garantizar la seguridad y estabilidad de la red de la ESE Hospital Marco Fidel Suárez, se describen algunos concejos y manejo adecuado.

a. Todo computador portátil debe ser incorporado al dominio de la red de la ESE Hospital Marco Fidel Suárez.
b. Los computadores portátiles de la ESE Hospital Marco Fidel Suárez se han adquirido específicamente para facilitar el desarrollo de actividades laborales, su uso debe estar relacionado con las actividades del área a la cual ha sido asignado y el uso para propósitos personales debe ser ocasional, racional y no debe obstaculizar las actividades laborales.
c. Los equipos portátiles deben permanecer en las instalaciones de la ESE Hospital Marco Fidel Suárez, durante los días y horarios hábiles de trabajo, pueden salir de las instalaciones, solo en el caso de utilizarlo en labores de la entidad.
d. En caso de licencia o vacaciones del funcionario, el equipo portátil debe quedar a disposición del área a la cual fue asignado, si el coordinador del área autoriza puede ser utilizado en el periodo de licencia o vacaciones.
e. La instalación, configuración, modificación o eliminación de software aplicativo sobre los equipos portátiles es responsabilidad exclusiva del área de Tecnología.
f. El área de Tecnología tiene la potestad para remover, sin notificar al funcionario, cualquier software que no esté autorizado
g. La configuración, eliminación, modificación o cambio de sistema operativo es de responsabilidad del área de Tecnología.
h. La configuración e instalación de hardware de los equipos portátiles, es responsabilidad exclusiva del área de Tecnología de la ESE o el área de soporte, según corresponda.
i. Se debe mantener desactivada la red inalámbrica en caso de que no esté siendo utilizada.
j. Es responsabilidad de cada funcionario hacer copias de seguridad de la información almacenada en el equipo portátil, si no está seguro del proceso debe comunicarse con el Área de Soporte.
k. Es responsabilidad del funcionario reportar inmediatamente al Área activos fijos, cualquier daño o pérdida del dispositivo móvil que le ha sido asignado.
l. No insertar tarjetas de memoria sin haber comprobado previamente que están libres de virus o de algún tipo de código malicioso.

Software Administrativo Hospitalario DGNET

Es un sistema de información está compuesto por módulos que integran todas las áreas de la ESE Hospital Marco Fidel Suárez, públicas y privadas y de todos los niveles de atención, es decir, que a partir del acto médico afecta las demás unidades funcionales y su correspondiente resultado en el área administrativa.

DGNET garantiza la seguridad de la información y seguridad por usuario con su correspondiente clave de acceso donde autoriza o restringe las actividades dentro de la plataforma de información. DGNET cuenta con un registro de transacciones que permite identificar a los usuarios que utilizaron el sistema de información, el día, la hora y la transacción realizada, para efectuar actividades de seguimiento y auditoría, dicho software está certificado en las normas internacionales de calidad de la información ISO 27001.

Responsabilidades del personal de Tecnología

a. Se harán investigaciones exhaustivas a las variaciones significativas en los resultados de los indicadores.
b. Se harán auditorias trimestrales para identificar la vulnerabilidad del sistema de información y el grado de capacitación operativa y técnica de los funcionarios.
c. Se harán evaluaciones al fluido eléctrico, las conexiones y los cables para evitar eventos adversos en el sistema de información.
d. Todos los equipos entrarán en el inventario de la institución.
e. Todos los funcionarios de la institución contarán con herramientas informáticas de trabajo en buen estado si así lo requiere su labor.
f. A cada usuario de la institución se le deben conceder los accesos necesarios para el cumplimiento de sus funciones.
g. Es responsabilidad del personal de Tecnología instalar todo el software de la institución.
h. Realizar Copias de respaldo todos los días a las 02:00 am de todos y cada uno de los servidores (Servidor de Correo, servidor de base de datos DGNET -ETNA, servidor de archivos (FENIX), servidores plantas telefónicas – Niquía y Autopista, servidores de acceso remoto – GANIMEDES), donde se garantice fiel copia de la información que repose sobre estos equipos del área de Tecnología.

Dicha información se guarda en discos duros externos.
Actualmente también se guarda una copia de seguridad diaria en la NUBE de los servidores antes mencionados y de la información que en ellos reposa.

ARTÍCULO OCTAVO: DERECHOS Y RESPONSABILIDADES DE LA INSTITUCIÓN

a. La institución se reserva todos los derechos sobre sus activos, incluido el mensaje de cualquier información o mensaje residentes en sus sistemas y medios de almacenamiento de información. Los usuarios de sistemas de información no deben esperar más privacidad que la protegida por la ley para actividades sindicales.
b. Está terminantemente prohibido el manejo de la información en sistemas ajenos a ella, excepto la estrictamente necesaria para el cumplimiento de sus obligaciones legales y contractuales.
c. La institución retiene sus derechos de propiedad intelectual de cualquier material, aunque este material sea publicado en un foro público.
d. Para el uso y divulgación de cualquier material bajo una licencia no propietaria deberá ser expresamente autorizado por el departamento legal.
e. Es prohibido el consumo de alimentos en el lugar de trabajo.
f. Es prohibido fumar en el lugar de trabajo.
g. Se deberán vacunar todos los equipos archivos y medios extraíbles que introduzcan en cada equipo.
h. La información que se reportada para el sistema de información debe ser completa, veraz y confiable.
i. En caso de sospechas o evidencia sobre fugas de información se comunicará inmediatamente al Subgerente administrativo.
j. Está prohibido iniciar o reenviar correos encadenados.
k. Se prohíbe el uso de correo no deseado.
l. Está prohibido el abandono de documentos impresos con información confidencial en cualquier impresora, fax, fotocopiadora, o dispositivo similar.

Confidencialidad de la información

a. Toda la información generada en la institución será considerada como confidencial y se tomarán las medidas correspondientes a garantizar la privacidad de esta.
b. Es responsabilidad de cada usuario velar por la custodia de la información albergada en sus puestos y/o equipos de trabajo.
c. Sólo los usuarios autorizados pueden acceder a la información sean internos o externos, las autorizaciones son asignadas por la gerencia o la subgerencia administrativa.
d. La información estará centralizada en el área de sistemas de información y desde allí será gerenciado este bien.

e. Se harán copias de seguridad (Backups) diariamente a la información del software y de la información almacenada en respaldo en servidor.
f. Se actualizará el antivirus periódicamente en cada uno de los equipos del hospital.
g. La información privada y confidencial estará protegida mediante control de accesos.
h. El acceso físico a la zona donde se maneja información confidencial estará limitado a personal controlado.
i. Debe evitarse el envío de información confidencial fuera de los sistemas de la institución. De realizarse, el receptor debe garantizar su secreto.
j. Todo miembro de la institución debe firmar a su entrada en la institución un Acuerdo de Confidencialidad.
k. Todo miembro de la institución que deje la institución debe firmar una Declaración de Confidencialidad, como parte de la cual se hará una declaración de accesos conocido, los cuales tendrán su medio de autenticación cambiado.

Sanciones

Esta norma obliga a todos los miembros de la institución, y a todos los particulares y miembros de la institución que usen el sistema de información.

a. Todo miembro de la institución tiene la responsabilidad de conocer esta norma y cumplir con ella, esta condición es imprescindible para ingresar en la institución.
b. Los miembros de la institución están obligados al cumplimiento de esta norma.
c. El incumplimiento de esta norma implica la apertura de un proceso disciplinario que puede conducir a sanciones, al despido justificado o a demandas civiles o penales.

Disposiciones finales.

El presente reglamento se complementa y no es excluyente de las normas establecidas en el reglamento interno de trabajo, el reglamento de prestación de servicios y el reglamento de uso y manejo de la información. Así también la normatividad específica como la resolución 1995/99, ley 594/2000 (general de archivo), y resolución 1715/2005.

IDENTIFICACIÓN DEL RIESGO

Identificación de activos

El principal activo de una organización es la información, la cual puede estar en forma física como documentos (Archivo de gestión) o escritos a mano (libros de cirugía, libros de vigilancia, libros de defunción o nacimiento), en medios electrónicos almacenados en Discos Duros Externos (Back up), Memorias USB (firmas digitales o informes) o en forma digital (bases de datos), en los equipos de cómputo o en la Nube. Toda esta información requiere ser analizada para su protección. (Un activo es todo aquello que genera valor para una empresa u organización.)
Para este proceso se llevará a cabo un inventario de activos mediante una encuesta en la que se identificará su tipología si es software o hardware, si esta información se encuentra de manera digital o física, y si se encuentra en digital que tipo de archivo es. Aparte de conocer toda la información al interior de la institución también se realizará una valoración de esta información mediante los siguientes criterios:

Confidencialidad

Nivel	Descripción Criterio de Confidencialidad	Denominación
0	Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado o no	Publico
1	Información que puede ser conocida y utilizada por todos los empleados y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la institución, el Sector Público Nacional o terceros.	Reservada –Uso Interno
2	Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la institución o a terceros.	Reservada – Confidencial
3	Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de la institución, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo o a terceros.	Reservada Secreta

Integridad

Nivel	Descripción Criterio de Integridad
0	Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operación.
1	Información cuya modificación no autorizada puede repararse, aunque podría ocasionar pérdidas leves.
2	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas.
3	Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves.

Disponibilidad

Nivel	Descripción Criterio de Disponibilidad
0	Información cuya inaccesibilidad no afecta la operación.
1	Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas.
2	Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas.
3	Información cuya inaccesibilidad permanente durante una hora podría ocasionar pérdidas significativas.

Después de este proceso se procederá a identificar también su ubicación ya sea al interior de la institución o por fuera en algún servicio en la nube y en cualquier caso las credenciales de ingreso si se necesitase.

Identificación Del Riesgo

Los riesgos numerados a continuación son identificados en la guía metodológica del ministerio de las TICS:

1. Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
2. Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
3. Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.
4. Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
5. Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con

los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, de acuerdo con su misión.

6. Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras, y el cumplimiento de la misión.

En cuanto a los riesgos que afectan directamente a la información se ha evidenciado en la literatura en los siguientes.

Riesgos Informáticos	Causas	Efecto
Perdida Robo o Fuga de Información	- Fallas en el proceso de copia de respaldo o de restauración de la información, o pérdida de la misma. - Fallas en los análisis y socialización de las vulnerabilidades de la infraestructura de IT - No contar con acuerdos de confidencialidad con los empleados y terceros. - Falta de autorización para la extracción de información generadas por requerimientos. - Ingreso a la red y acceso a los activos de TI por parte de máquinas ajenas a la entidad. - Habilitación de puertos USB en modo lectura y escritura para medios de almacenamiento - Ataques cibernéticos internos o externos - Empleados no capacitados en los temas de riesgos informáticos. - Desconocimiento del riesgo. - Prestar los equipos informáticos a personal no autorizado. - No cerrar sesión cuando se desplaza del puesto. - Acceso no autorizado a las dependencias. - Conectar dispositivos	- Afectación parcial o total de la continuidad de las operaciones de los servicios del Incumplimiento normativo. - Vulneración de los sistemas de seguridad operando actualmente. - Mala imagen, multas, sanciones y pérdidas económicas. - Generación de consultas, funcionalidades o reportes con información sensible de los clientes. - Pérdida o fuga de información.

Riesgos Informáticos	Causas	Efecto
	externos a los equipos.	
Correos electrónicos de extraña procedencia	- Empleados no capacitados en los temas de riesgos informáticos. - Desconocimiento del riesgo. - No generar una Cultura de Seguridad de la Información. - Falta de Filtros en el Servidor de Correo. - Programas de DLP (Data Lost Prevention). - Falta de instalación de EndPoint (programa seguridad punto final) en las estaciones de trabajo.	- Cifrado o secuestro de la información. - Monitoreo de las actividades realizadas en el equipo. - Ataque remoto mediante un troyano o gusano. - Robo de contraseñas. - Equipo usado como Zombie. - Robo de documentos y/o archivos. - Sistema con mal Funcionamiento.
Daño en los equipos tecnológicos	- Manejo inadecuado de los equipos. - Falta de mantenimiento o mala conexión de los mismos en las instalaciones eléctricas. - Falta de equipos de potenciación. - Fallas por defectos de fábrica. - Derrame de líquido. - Falta de ambiente adecuado para los equipos. - Falta Educación a los usuarios en el manejo de los equipos de computo	- Perdida de información. - Perdidas de los quipos informáticos. - Indisponibilidad del Servicio. - Traumatismos en los procesos.

Riesgos Informáticos	Causas	Efecto
Perdida de conectividad	- Daño externo del proveedor de internet. - Ataque DDoS o DOS (denegación de servicios distribuidos o Denegación de servicios).	
Ataques Informáticos	- Estimulo o Reto personal. - Rebelión. - Ánimo de lucro. - Espionaje.	- Daño en los equipos tecnológicos. - Incidente en la confidencialidad, integridad y disponibilidad de la información. - Denegación de servicios. - Secuestro de la información. - Divulgación ilegal de la información. - Suplantación de identidad. - Destrucción de la información. - Soborno de la información.

Identificación de amenazas

Una amenaza se identifica como un evento, persona, situación o fenómeno que pueda causar daño no solo a un activo sino también a varios activos de la organización por ende hay que identificarlos de la mejor manera. Las amenazas pueden ser de origen Humano o Ambientales.

Tipo	Amenaza
Daño físico	Fuego
	Agua
	Contaminación
	Accidente Importante
	Destrucción del equipo o medios
	Polvo, corrosión, congelamiento
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
	Fenómenos volcánicos
	Fenómenos meteorológico
	Inundación
Perdida de los servicios	Fallas en el sistema de suministro de agua o aire

Tipo	Amenaza
esenciales	acondicionado
	Perdida de suministro de energía
	Falla en equipo de telecomunicaciones
Perturbación debida a la radiación	Radiación electromagnética
	Radiación térmica
	Impulsos electromagnéticos
Compromiso de la información	Interceptación de señales de interferencia comprometida
	Espionaje remoto
	Escucha encubierta
	Hurto de medios o documentos
	Hurto de equipo
	Recuperación de medios reciclados o desechados
	Divulgación
	Datos provenientes de fuentes no confiables
	Manipulación con hardware
	Manipulación con software
	Detección de la posición
Fallas técnicas	Fallas del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información.
Acciones no autorizadas	Uso no autorizado del equipo
	Copia fraudulenta del software
	Uso de software falso o copiado
	Corrupción de los datos
	Procesamiento ilegal de datos
Compromiso de las funciones	Error en el uso
	Abuso de derechos
	Falsificación de derechos
	Negación de acciones
	Incumplimiento en la disponibilidad del personal

Identificación de las vulnerabilidades

Las vulnerabilidades son las Fallas o debilidades en un sistema, que puede ser explotada por quien la conozca. Cuando la amenaza encuentra la vulnerabilidad es cuando se crea el riesgo. Por eso es necesario conocer la lista de amenazas y el inventario de activos de información.

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o medios.
	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión y congelamiento.
	Sensibilidad a la radiación electromagnética.	Radiación electromagnética.
	Ausencia de un eficiente control de cambios en la configuración.	Error en el uso.
	Susceptibilidad a las variaciones de voltaje.	Pérdida del suministro de energía.
	Susceptibilidad a las variaciones de temperatura.	Fenómenos meteorológicos.
	Almacenamiento sin protección.	Hurtos medios o documentos.
	Falta de cuidado en la disposición final.	Hurtos medios o documentos.
	Copia no controlada.	Hurtos medios o documentos.
SOFTWARE	Ausencia o insuficiencia de pruebas de software.	Abuso de los derechos.
	Defectos bien conocidos en el software.	Abuso de los derechos.
	Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo.	Abuso de los derechos.
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado.	Abuso de los derechos.
	Ausencias de pistas de auditoría.	Abuso de los derechos.
	Asignación errada de los derechos de acceso.	Abuso de los derechos.

	Software ampliamente distribuido.	Corrupción de datos.
	En términos de tiempo utilización de datos errados en los programas de aplicación.	Corrupción de datos.

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Interfaz de usuario compleja.	Error en el uso.
	Ausencia de documentación.	Error en el uso.
	Configuración incorrecta de parámetros.	Error en el uso.
	Fechas incorrectas.	Error en el uso.
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario.	Falsificación de derechos.
	Tablas de contraseñas sin protección.	Falsificación de derechos.
	Gestión deficiente de las contraseñas.	Falsificación de derechos.
	Habilitación de servicios innecesarios.	Procesamiento ilegal de datos.
	Software nuevo o inmaduro.	Mal funcionamiento del software.
	Especificaciones incompletas o no claras para los desarrolladores.	Mal funcionamiento del software.
	Ausencia de control de cambios eficaz.	Mal funcionamiento del software.
	Descarga y uso no controlado de software.	Manipulación con software.
	Ausencia de copias de respaldo.	Manipulación con software.
	Ausencia de protección física de la edificación, puertas y ventanas.	Hurto de medios o documentos.
	Fallas en la producción de informes de gestión.	Uso no autorizado del equipo.
	Ausencia de pruebas de envío o recepción de mensajes.	Negación de acciones.
	Líneas de comunicación sin protección.	Escucha encubierta.
	Tráfico sensible sin protección.	Escucha encubierta.

RED	Conexión deficiente de los cables.	Fallas del equipo de telecomunicaciones.
	Punto único de fallas.	Fallas del equipo de telecomunicaciones.
	Ausencia de identificación y autentificación de emisor y receptor.	Falsificación de derechos.

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Arquitectura insegura de la red.	Espionaje remoto.
	Transferencia de contraseñas en claro.	Espionaje remoto.
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento).	Saturación del sistema de información.
	Conexiones de red pública sin protección.	Uso no autorizado del equipo.
PERSONAL	Ausencia del personal.	Incumplimiento en la disponibilidad del personal.
	Procedimientos inadecuados de contratación.	Destrucción de equipos y medios.
	Entrenamiento insuficiente en seguridad.	Error en el uso.
	Uso incorrecto de software y hardware.	Error en el uso.
	Falta de conciencia acerca de la seguridad.	Error en el uso.
	Ausencia de mecanismos de monitoreo.	Procesamiento ilegal de los datos.
	Trabajo no supervisado del personal externo o de limpieza.	Hurto de medios o documentos.
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería.	Uso no autorizado del equipo.
	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.	Daño en la infraestructura física y tecnológica.
	Ubicación en área susceptible	Daño en la infraestructura física y tecnológica.

LUGAR	de inundación.	
	Red energética inestable.	Daño en la infraestructura física y tecnológica.
	Ausencia de protección física de la edificación (Puertas y ventanas)	Daño en la infraestructura física y tecnológica.
ORGANIZACIÓN	Ausencia de procedimiento formal para el registro y retiro de usuarios.	Abuso de los derechos.
	Ausencia de proceso formal para la revisión de los derechos de acceso.	Abuso de los derechos.

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad).	Abuso de los derechos.
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información.	Abuso de los derechos.
	Ausencia de auditorías.	Abuso de los derechos.
	Ausencia de procedimientos de identificación y valoración de riesgos.	Abuso de los derechos.
	Ausencia de reportes de fallas en los registros de administradores y operadores.	Abuso de los derechos.
	Respuesta inadecuada de mantenimiento del servicio.	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos.	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de procedimientos de control de cambios.	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de procedimiento formal para la documentación del MSPI.	Corrupción de datos.

	Ausencia de procedimiento formal para la supervisión del registro del MSPI.	Corrupción de datos.
	Ausencia de procedimiento formal para la autorización de la información disponible al público.	Datos provenientes de fuentes no confiables.
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información.	Negación de acciones.
	Ausencia de planes de continuidad.	Falla del equipo.
	Ausencia de políticas sobre el uso de correo electrónico.	Error en el uso.
	Ausencia de procedimientos para introducción del	Error en el uso.

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	software en los sistemas operativos.	
	Ausencia de registros en bitácoras.	Error en el uso.
	Ausencia de procedimientos para el manejo de información clasificada.	Error en el uso.
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos.	Error en el uso.
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información.	Hurto de equipo.
	Ausencia de política formal sobre la utilización de computadores portátiles.	Hurto de equipo.
	Ausencia de control de los activos que se encuentran fuera de las instalaciones.	Hurto de equipo.
	Ausencia de política sobre limpieza de escritorio y pantalla.	Hurto de medios o documentos.

	Ausencia de autorización de los recursos de procesamiento de información.	Hurto de medios o documentos.
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad.	Hurto de medios o documentos.
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad.	Uso no autorizado de equipo.
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	Uso de software falsificado o copiado.

Identificación De Controles Existentes

La identificación de los controles existentes permite realizar la evaluación de riesgos. Es necesario realizar esta identificación para poder conocer si existen controles similares o incluso repetidos que se pueden unificar y posterior a esto evaluarlos para calificar como ineficaz, insuficiente o injustificado, si es injustificado o insuficiente, se debería revisar el control para determinar si se debe eliminar o reemplazar por otro más adecuado.

EVALUACIÓN DE RIESGO

La evaluación de riesgo se realiza con enfrentamiento entre la probabilidad de ocurrencia y el impacto que genera el riesgo en los activos de información, dado por la matriz de calificación, evaluación y respuestas a los riesgos.

Tabla De Probabilidad			
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años
2	improbable	El evento puede ocurrir en algún momento	Al menos una vez en los últimos 5 años
3	posible	El evento podría ocurrir en algún momento	Al menos una vez en los últimos 2 años
4	probable	El evento probablemente ocurra en la mayoría de las circunstancias	Al menos una vez en el último año
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año

Tabla De Impacto

1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efecto mínimos sobre la entidad
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto mínimos sobre la entidad
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efecto sobre la entidad
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad

Probabilidad	**Impacto**				
	Insignificante (1)	**Menor (2)**	**Moderado (3)**	**Mayor (4)**	**Catastrófico (5)**
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de Riesgo Baja: Asumir el riesgo
M: Zona de Riesgo Moderada: Asumir el riesgo, Reducir el riesgo
A: Zona de Riesgo Alta: Reducir, Evitar, Compartir o Transferir
E: Zona de Riesgo extrema: Reducir el riesgo, evitar compartir o transferir

Ejemplo de análisis de riesgo.

Análisis De Riesgos					
Riesgo	**Calificación**		**Tipo de impacto**	**Evaluación**	**Medidas de respuestas**
	Probabilidad	**Impacto**		**Zona de riesgo**	
Perdida, Robo o fuga de información	3	5	Disponibilidad integridad Y confidencialidad de la información	Extrema	Reducir el riesgo, Evitar o Transferir

Indicadores

CUMPLIMIENTO DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA ENTIDAD		
DEFINICION		
Cumplimiento de políticas de seguridad de la información en la entidad		
OBJETIVO		
Busca identificar el nivel de estructuración de los procesos de la entidad orientados a la seguridad de la información.		
TIPO INDICADOR		
Indicador de Cumplimiento		
DESCRIPCION DE VARIABLES	**FORMULA**	**FUENTE DE INFORMACIÓN**
VSI09: ¿La entidad ha definido una política general de seguridad de la información?	VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Guía del Modelo de Operación / Usuarios Internos
VSI10: ¿La entidad ha definido una organización interna en términos de personas y responsabilidades con el fin de cumplir las políticas de seguridad de la información y documenta estas actividades?		Guía del Modelo de Operación / Usuarios Internos
VSI11: ¿La entidad cumple con los requisitos legales, reglamentarios y contractuales con respecto al manejo de la información?		Guía del Modelo de Operación / Usuarios Internos
METAS		
CUMPLE 1	**NO CUMPLE**	0
OBSERVACIONES		

DENTIFICACION DE LINEAMIENTOS DE SEGURIDAD DE LA ENTIDAD		
DEFINICION		
Grado de la seguridad de la información y los equipos de cómputo.		
OBJETIVO		
Busca medir el nivel de preparación del recurso humano y su apropiación en cuanto a la seguridad de la información y los equipos de cómputo.		
TIPO INDICADOR		
Indicador de Cumplimiento		
DESCRIPCION DE VARIABLES	**FORMULA**	**FUENTE DE INFORMACION**
VSI12: ¿La entidad ha definido lineamientos de trabajo a través del comité o responsable de seguridad para que sus funcionarios cumplan las políticas de seguridad y evalúa periódicamente su pertinencia?	VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Usuarios Internos.
VSI13: ¿La entidad ha definido lineamientos en cuanto a la protección de las instalaciones físicas, equipos de cómputo y su entorno paraevitar accesos no autorizados y minimizar riesgos de la información de la entidad?		Usuarios Internos.
METAS		
CUMPLE 1	**NO CUMPLE**	0

OBSERVACIONES

INDICADOR – VERIFICACIÓN DEL CONTROL DE ACCESO			
DEFINICIÓN			
Grado control de acceso en la entidad.			
OBJETIVO			
Busca identificar la existencia de lineamientos, normas o estándares en cuanto al control deacceso en la entidad.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
VSI14: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el acceso de los usuarios a sus servicios de Gobierno en línea y a sus redes de comunicaciones?		VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Usuarios Internos.
VSI15: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el uso y el acceso a los sistemas de información, las aplicaciones y los depósitos de información con las que cuenta la entidad? VSI16: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar las terminales móviles y accesos remotos a los recursos de la entidad?			Usuarios Internos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

Estrategias por ejecutar para cumplir con la presente iniciativa:

ACTIVIDADES PROGRAMADAS	META O PRODUCTO	RESPONSABLE	FECHA PROGRAMADA
Socialización del Plan de Seguridad y Privacidad de la Información	100% del personal institucional informado sobre el plan	Asesor de TIC's y Oficial de Protección de Datos	Febrero 2024
Capacitación sobre Normativas de Seguridad y Privacidad de la Información	100% del personal instruido en normativas aplicables	Asesor de TIC's y Oficial de Protección de Datos	Abril 2024
Replicación de Información a través de Medios de Comunicación	100% de difusión de información en correo, redes sociales y otros medios	Asesor de TIC's y Oficial de Protección de Datos	Junio 2024
Evaluación del Nivel de Conocimiento del Personal sobre Seguridad y Privacidad	70% de conocimiento mínimo requerido	Asesor de TIC's y Oficial de Protección de Datos	Agosto 2024
Verificación de copias respaldo de la información	100% copias de bases de datos del Sistema de Información	Área de Tecnología	Diario 2024
Revisión Usuarios creados en las plataformas de la entidad	100% Usuarios activos y retirados en las plataformas	Área de Tecnología	Semanal y a demanda 2024
Realizar seguimiento bimestral a los riesgos y controles de Seguridad Digital definidos en el Mapa de Riesgos Institucional	Realizar seguimiento bimestral en un 100%	Asesor tecnología Oficial protección de datos Asesora y apoyo técnico planeación	Bimestral 2024

REVISIÓN Y APROBACIÓN		
ELABORACIÓN	**REVISIÓN**	**APROBACIÓN**
Nombre: Carolina Jiménez - Fernando Camejo	**Nombre:** María Fanny Jaramillo Tabares	**Nombre:** Isauro Barbosa
Cargo: GESIS - Asesor TICS	**Cargo:** Planeación	**Cargo:** Gerente ESE.

CONTROL DE CAMBIOS			
VERSIÓN	**FECHA**	**CAMBIO**	**RESPONSABLE**
07	Enero de 2023	Creación del documento	Técnico de Sistemas
08	Enero de 2024	Se actualiza actividades, acciones a desarrollar y estrategias por ejecutar	Asesor TICS