POLÍTICA DE SEGURIDAD Y GESTIÓN DE LA INFORMACIÓN

GESTIÓN INFORMÁTICA

CORPORACIÓN EDUCATIVA MINUTO DE DIOS

Tabla de contenido

1. INTRODUCCIÓN

Este documento tiene la finalidad de condensar la información referente a los procedimientos de la **Gestión Informática** de la CORPORACIÓN EDUCATIVA MINUTO DE DIOS, contiene las políticas de seguridad informática que deben observar los funcionarios, para proteger adecuadamente los activos tecnológicos y de la información.

Este documento estructura la política general de seguridad para funcionarios que usen recursos informáticos donde se consideran aspectos claves como la parte tecnológica, control de acceso, actualización y continuidad de los procesos de seguridad informática para la entidad.

El proponer esta política de seguridad requiere un alto compromiso con la institución, agudeza técnica para establecer fallas y deficiencias, mejoramiento continuo de dicha política en función un ambiente dinámico de la tecnología institucional.

La información, junto a los procesos que hacen uso de ella, son activos muy importantes en la **Gestión Informática**. La confidencialidad, integridad y disponibilidad de información sensible son esenciales para mantener los niveles de seguridad de conformidad legal y asegurar el cumplimiento de los objetivos misionales.

Las organizaciones y sus sistemas de información están expuestos a amenazas que, aprovechando cualquiera de las fallas existentes, pueden someter los activos críticos de información a diversas formas

de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos y el “hacking” son ejemplos comunes, es importante considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallas técnicas.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. En relación con lo anterior se describen tres términos centrales a destacar:

Confidencialidad: la información de los usuarios de los procesos y procedimientos informáticos y tecnológicos debe ser tratada conforme a la política de tratamiento de datos adoptada por la institución. No se dispone de esta información ni se le entrega a terceros sin cumplir los procedimientos autorizados.

Integridad: La información se debe procesar, archivar y comunicar (si se requiere) de manera exacta y sin alteraciones ni interpretaciones.

Disponibilidad: Se contará con el acceso y se podrá hacer uso de la información con el debido cumplimiento de los protocolos autorizados para tal fin.

En los últimos años, en la **CEMID**, ha ido en aumento su inventario tecnológico, tanto en infraestructura, hardware y software, por lo que se hace necesario crear una política que sirva como referencia de garantía en la seguridad de la información que cumpla con los tres valores anteriormente señalados.

2. OBJETIVO

Definir los lineamientos para proteger, preservar y administrar correctamente la información de la Corporación Educativa Minuto de Dios, con el fin de asegurar el cumplimiento de los protocolos para garantizar la confidencialidad, integridad, disponibilidad, de la información y su uso de conformidad legal, que sirva de referencia para todos los funcionarios directos, temporales, contratistas, practicantes, terceros o cualquier persona que tenga una relación contractual con la **CEMID**.

3. ALCANCE

Esta política aplica a todas las áreas que componen la institución, a sus recursos, a la totalidad de los procesos internos o externos vinculados a la **CEMID** a través de contratos o acuerdos con terceros y a todo el personal de la Corporación Educativa Minuto de Dios, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

4. DEFINICIONES

Para efectos de la aplicación de las políticas se adoptan las siguientes definiciones:

4.1. Activos de Información: cualquier componente (humano, tecnológico, software, manuales, documentación, entre otros) que tiene valor para la organización y signifique riesgo si llega a manos de personas no autorizadas.

4.2. Información: todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

4.3. Reportes básicos (RB): son aquellos informes generados por el sistema de información institucional que soportan o sirven de base para la toma de decisiones en cualquiera de las gestiones y sirven como base para aportar información a los organismos de inspección, control y vigilancia, tanto en el ámbito interno como externo.

4.4. Activos de Información críticos: activo de información cuya afectación o alteración puede generar un impacto negativo de carácter económico, legal o al buen nombre de la institución.

4.5. Archivo: colección de datos e información del mismo tipo, almacenada en forma organizada como una unidad, que puede emplearse y tratarse como soporte material de la información contenida en éstos.

4.6. Aplicación: programa informático diseñado para permitir a los usuarios la realización de tareas específicas en computadores, servidores y similares.

4.7. Base de Datos: conjunto de datos almacenados y organizados con el fin de facilitar su acceso y recuperación.

4.8. Backups o Copias de respaldo: copia que se realiza a la información institucional definida como sensible o vulnerable, con el fin de utilizarla posteriormente para restablecer el original ante una eventual pérdida de datos, para continuar con las actividades rutinarias y evitar pérdida generalizada de datos.

4.9. Clasificación de seguridad del documento: clasificación estratégica adoptada por el Sistema de Gestión de la Calidad, con el fin de llevar a cabo la gestión interna referente al mantenimiento de la seguridad de la información de acuerdo a su importancia para la organización, esta clasificación se define como:

- **Público**: información de dominio público, sean físicos o electrónicos, que la **CEMID** puede dar a conocer a terceras partes como estudiantes, proveedores, docentes y demás estamentos que tengan alguna relación directa o indirecta. Dicha información puede estar publicada en carteleras de la entidad o en las páginas web de la **CEMID**.
- **Controlado**: documentos de gestión físicos o electrónicos de las diversas unidades de la institución, que contienen los métodos de trabajo usados para su operación y/o para formación del personal. El

acceso a esta información está restringido a los miembros de cada área o disponibles para los ejercicios de auditoría interna o externa de la institución.

-**Reservado**: documentos estratégicos, o con información descriptiva de claves o datos técnicos de funcionamiento de las diversas unidades de la institución, que pueden ser físicos o electrónicos. Esta información solamente será accedida por personal autorizado para su uso y/o para atender solicitudes derivadas de los procesos de auditorías internas o externas y/o para atender requerimientos de orden legal o jurídico.

4.10. Código fuente: conjunto de instrucciones escritas en algún lenguaje de programación de computadoras, hechas para ser leídas y transformadas por alguna herramienta de software (compilador, intérprete, ensamblador) en lenguaje de máquina o instrucciones ejecutables en el computador.

4.11. Credenciales de acceso: privilegios de seguridad agrupados bajo un nombre y contraseña, que permiten acceso a los sistemas de información.

4.12. Custodio: es el encargado de gestionar y administrar la adecuada operación del activo y la información relacionada con éste. En ocasiones el responsable y el custodio son la misma persona.

4.13. Datacenter, centro de datos o sala de servidores: área dispuesta para el alojamiento seguro de los equipos de cómputo necesarios para el procesamiento y almacenamiento de la información de una organización (Servidores, SAN, equipos de comunicación, etc.).

4.14. Dispositivo biométrico: dispositivo de seguridad utilizado en sistemas computarizados que sirve para identificar atributos físicos como rasgos faciales, patrones oculares, huellas digitales, la voz y la escritura.

4.15. Dispositivo móvil: aparato electrónico con capacidades de cómputo y conexión a redes inalámbricas cuyo tamaño y diseño permite ser fácilmente transportado para utilizarse en diversas ubicaciones con facilidad (portátiles, tablets, celulares inteligentes y demás dispositivos con características similares).

4.16. Información sensible o vulnerable: también llamado activo sensible, es el nombre que recibe la información personal o institucional (datos personales, información financiera, contraseñas de correo electrónico, datos personales, datos de investigaciones), la cual puede ser alterada, descompuesta, mal utilizada, divulgada y/o eliminada, causando graves daños a la organización propietaria.

4.17. Niveles de backup: se refiere a la cantidad de copias o respaldos que se tiene de datos determinados. Si se cuenta con una sola copia, se está hablando de un backup de 1er. Nivel; si se tienen dos copias, de un backup de 2do. Nivel. Cuanto mayor sea el número de niveles de backup, menor será el riesgo de perder los datos.

4.18. Propietario: en la estructura administrativa de la institución, se le otorga la propiedad del activo a cada una de las unidades estratégicas, divisiones organizacionales, gerencias, rectorías o vicerrectorías.

4.19. Responsable: el Jefe de área o gerente de cada una de dichas áreas, será el responsable ante la Institución, de los activos de información registrados como de su propiedad.

4.20. SAN (Storage Area Network) O Red de Área de Almacenamiento: recurso compartido, empleado como repositorio de información institucional tanto de funcionarios, docentes y/o contratistas como de grupos y unidades funcionales, donde se definen permisos de acceso de acuerdo a los roles al interior de la organización.

4.21. Seguridad de la Información: son todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información.

4.22. Servidor: equipo de computación físico o virtual, en el cual funciona un software, cuyo propósito es proveer servicios a otros dispositivos dentro de la red.

4.23. Servidor de Almacenamiento: equipo servidor dotado con varios discos duros destinados a respaldar y compartir datos.

4.24. Sistema Operativo (SO) u Operating System (OS): programa o conjunto de programas que en un sistema informático gestiona los recursos de hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto de los restantes.

5. POLÍTICA PARA DISPOSITIVOS MÓVILES

Se permite el uso de dispositivos móviles de conexión inalámbrica al interior de las instalaciones de todas las instituciones que hacen parte de la Corporación Educativa Minuto de Dios siempre y cuando se cumpla con los protocolos de seguridad de la información establecidos en este documento y/o se encuentre con la autorización requerida.

Los dispositivos móviles asignados a administrativos, contratistas y/o docentes, son de propiedad de la entidad, y los responsables de dichos equipos deberán velar por su adecuado uso, cuidado, mantenimiento y protección.

Los medios de almacenamiento de estos dispositivos pueden ser protegidos tecnológicamente con medios de cifrado de datos o mediante cualquier otro mecanismo definido por la Gestión Informática

6. POLÍTICA DE CONTROL DE ACCESO

El departamento de Gestión Humana, informará oportunamente al departamento de sistemas, las vinculaciones de personal nuevo, o desvinculaciones a las que hubiera lugar, esto con el fin de crear o cancelar perfiles, cuentas de correo y accesos a CEMIDWEB y demás plataformas de uso institucional.

La Gestión Informática es el encargado de crear cuentas de correo, asignar perfiles dentro de la plataforma, esto de acuerdo a las orientaciones del departamento de gestión humana y la dirección nacional de Educación, quienes lo definirán en concordancia con el rol asignado a cada funcionario.

Los usuarios son los únicos responsables por la seguridad de sus credenciales de acceso y sus perfiles, así como de los movimientos de información que se deriven en la interacción de las diferentes cuentas (usuario y contraseña), las cuales son de uso exclusivo, único e intransferible.

7. POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

La **CEMID** por medio de la **Gestión Informática** establecerá la implementación de los sistemas y técnicas criptográficas para la protección de la información, con base en los análisis de riesgos efectuados y con el fin de mantener la confidencialidad, integridad y autenticidad de la información.

La **Gestión Informática** deberá brindar el apoyo necesario a administrativos, contratistas y docentes, estudiantes y padres de familia en el uso de las herramientas tecnológicas para protección de la información sensible.

La **Gestión Informática**, deberá definir las herramientas necesarias para el cifrado de datos, cuando se estime conveniente, de tal forma que preserve la confidencialidad, la integridad en la transmisión y manejo de información al interior de la **CEMID**.

La **Gestión Informática**, debe definir un **procedimiento de gestión de claves**, en el que incluyan los métodos para la generación, longitud, eliminación y recuperación de claves en las cuentas administradas por dicho departamento.

El procedimiento de gestión de claves debe tener en cuenta la fecha de finalización de contratos o de retiro de cada responsable del activo de información; de esta manera podrán desactivar, bloquear o eliminar los accesos no autorizados durante el periodo no laboral para que la información no corra

ningún riesgo que afecte la continuidad de los procesos de la **CEMID**, lo cual deberá ser informado oportunamente por el departamento de gestión humana.

8. POLÍTICA DE TRANSFERENCIA E INTERCAMBIO DE INFORMACIÓN

La **Gestión Informática,** deberá realizar las acciones necesarias para el mejoramiento respecto a los protocolos de seguridad de la información, especialmente para realizar transferencia de información digital y/o física entre las instituciones que hacen parte de la **CEMID**, usuarios y terceras partes de la institución.

Los mensajes enviados a través de cualquier medio electrónico que contengan información pública, controlada o reservada, deben ir cifrados y se debe propender porque sólo sean conocidos por el emisor y por el receptor(es), del mensaje.

Dentro de la política de tratamiento de datos institucionalizada por la **CEMID**, se incluye el anexo de una cláusula de confidencialidad tanto en los contratos laborales como en los de servicios contratados a terceros, en las que se aplica la legislación vigente.

La descarga de reportes a herramientas ofimáticas tipo hoja de cálculo será permitida, pero el archivo de salida será plenamente identificable como un reporte de solo lectura, diferente a los que emite el propio sistema.

Se otorgará acceso a terceros a la información, y a las instalaciones de procesamiento u otras áreas de servicios críticos como servidores racks y data center, con previa autorización; con el fin de proteger la información, procesamiento, servicios, entre otros que afecten la integridad, confidencialidad y disponibilidad de la misma.

9. POLÍTICAS DE DESARROLLO SEGURO

Las solicitudes de desarrollos nuevos o modificación de las aplicaciones actualmente instaladas que se encuentran en producción, deben ser tramitadas ante la **Gestión Informática** previa autorización de la dirección a la que pertenece el solicitante y concertadas con el área de programación. De acuerdo al procedimiento, las solicitudes realizadas en el tiempo estipulado serán sometidas a un proceso de verificación y posterior aprobación o rechazo de la solicitud. La sola radicación no implica aceptación y

estará sujeta a un cronograma de desarrollo con prioridades según los objetivos misionales de la **CEMID**.

La **Gestión Informática** es la única unidad encargada de la realización y/o contratación de desarrollos dentro de la **CEMID** y dará cumplimiento a los lineamientos de construcción de aplicaciones seguras adoptados por este departamento.

Todos los desarrollos serán puestos en producción según las presentes políticas, los términos y condiciones de privacidad y la **POLÍTICA DE USO ACEPTABLE (INTERNET, COMPUTADORES Y CORREO CORPORATIVOS) Y BACKUPS – PUAB**; y antes de pasar a producción deberán haber cumplido las fases de testeo en un ambiente de pruebas.

Con el fin de garantizar la seguridad, estabilidad y uso de las soluciones, todos los desarrollos nuevos o modificaciones a desarrollos existentes, se deben realizar de conformidad con el **Procedimiento de desarrollo de sistemas de información** aprobado y vigente para tal fin.

10. POLÍTICA DE GESTIÓN DE CAMBIOS

Los recursos que se encuentran administrados por la **Gestión Informática** que son cobijados por control de cambios son: las Aplicaciones de Software que han sido desarrolladas internamente o desarrolladas externamente y entregadas formalmente para su administración, los equipos de cómputo (servidores), las redes de telecomunicaciones locales, extendidas y externas, los gestores de bases de datos corporativos y la información documentada de los servicios gestionados por este departamento.

Cualquier modificación a las condiciones actuales de funcionamiento de los recursos administrados por la **Gestión Informática** serán considerados como Cambios Tecnológicos y por tanto, deben cumplir con los protocolos emitidos por la **Gestión Informática**.

En casos de alguna emergencia, que estén afectando directamente la normal prestación de los servicios de la Corporación Educativa Minuto de Dios en cualquiera de sus instituciones, se podrán realizar cambios en la configuración de recursos y servicios de infraestructura tecnológica. La emergencia manifiesta será reportada por rectoría, coordinación y/o administrativo de la sede a la **Gestión Informática**.

11. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS

El escritorio de trabajo de todos los administrativos, contratistas, docentes o proveedores de la institución debe permanecer completamente despejado y libre de documentos controlados y/o reservados a la vista del público.

El escritorio o la pantalla de inicio del computador, tableta, escritorio virtual o cualquier dispositivo que permita el acceso a información institucional, debe permanecer libre de documentos, carpetas e íconos

de acceso directo a archivos y/o carpetas que contengan documentos. En lo posible, sólo deben permanecer en la pantalla los íconos por defecto del sistema operativo instalado en el equipo.
Todos los administrativos, contratistas, docentes y/o proveedor son responsables de velar por la adecuada protección de la información física y lógica al ausentarse de su puesto de trabajo.
Los usuarios deberán bloquear su estación cada vez que se retiren de su puesto de trabajo y solo se podrá desbloquear con la contraseña del mismo usuario que la bloqueo.

Todas las estaciones de trabajo deberán usar únicamente el papel tapiz y el protector de pantalla establecido por la **CEMID**.

Todos los documentos controlados y/o reservados y en general, toda la documentación clasificada como "Información confidencial" debe permanecer guardados en un lugar seguro (archivadores con llaves o cajas fuertes), ya sea en un espacio físico o virtual, siempre que mantenga las debidas condiciones de almacenamiento y claves de acceso.

12. POLÍTICAS DE BACKUPS O COPIAS DE SEGURIDAD

12.1. En el caso de los **Backups de Usuario** la responsabilidad por el cumplimiento del procedimiento recae sobre los funcionarios que utilicen o manipulen información confidencial o de importancia para la **CEMID**, en el desempeño de sus funciones y en segunda medida sobre el Departamento de **Gestión Informática** quien deberá implementar las políticas para salvaguardar esta información y facilitará a los usuarios las herramientas para ejecución de copias de seguridad.
12.2. Los Backups de servidores son responsabilidad de la **Gestión Informática**.
12.3. La gestión de las copias de respaldo y la administración de los equipos de respaldo masivo de datos estará a cargo de la persona designada desde la **Gestión Informática**, quien además velará por los respectivos medios de respaldo y los datos contenidos en éstos.
12.4. El delegado como administrador de equipos de respaldo masivo de datos, integrante de la **Gestión Informática**, velará por los backups y por el resguardo de los datos contenidos en ellos; así como por su integridad, disponibilidad y confidencialidad.
12.5. Los medios de respaldo empleados para efectuar las copias de seguridad en la Corporación Educativa Minuto de Dios serán los definidos por el dueño del proceso de la **Gestión Informática** o por el delegado como administrador de plataforma tecnológica en el procedimiento de Copias de Respaldo.
12.6. El detalle del procedimiento de respaldo de la información, así como las responsabilidades, periodicidad, pruebas de restauración y documentación de eventos, está descrito en el documento

"**POLÍTICA DE USO ACEPTABLE (INTERNET, COMPUTADORES Y CORREO CORPORATIVOS) Y BACKUPS - PUAB**" a partir del numeral 2.

12.7. Se hará Respaldo a los archivos, aplicaciones, bases de datos y configuración de los sistemas operativos de los servidores calificados como críticos para la Corporación Educativa Minuto de Dios, casos en los que será obligatorio contar con mínimo dos niveles de respaldo.

12.8. El equipo de **Gestión informática** será responsable de definir los mecanismos adecuados para la ejecución de los respaldos de información, así como la periodicidad, etiquetado, lugar de archivo y el tiempo de retención de las copias, de acuerdo con el perfilamiento de usuarios.

12.9. La ejecución de las copias de seguridad debe llevarse a cabo en horas de poca o ninguna actividad laboral; por lo tanto, la **Gestión informática** será responsable de definir el horario de ejecución de estas tareas.

12.10. La necesidad de ejecutar un respaldo por demanda de los servidores críticos será determinada por la **Gestión Informática**, en base a los requerimientos de los usuarios.

12.11. La ejecución de las copias se revisará con la periodicidad definida en el **PROCEDIMIENTO PARA EL RESPALDO DE LA INFORMACIÓN** y se evidenciará en la **bitácora de Backups**.

12.12. La Comprobación periódica del estado de las copias se llevará a cabo con el fin de garantizar la disponibilidad e integridad de los datos almacenados. Los responsables de la administración de equipos de respaldo masivo de datos evidenciarán la comprobación periódica del estado de las copias de seguridad en la **bitácora de Backups.**

12.13. Los equipos para el respaldo de información de la Corporación Educativa Minuto de Dios deben estar ubicados en centros de datos (Datacenters) con las medidas de seguridad pertinentes, y tener acciones de mantenimiento regulares vigentes que deben registrarse en el **inventario de Gestión Informática**.

12.14. Los medios de almacenamiento de datos deben tener un manejo adecuado para mitigar la perdida de información a causa de un daño o fallo físico.

a. Se debe asegurar que la información considerada de nivel de clasificación alta, en las plataformas tecnológicas de la **CEMID**, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, se resguarde periódicamente a través de mecanismos adecuados que garanticen su identificación, protección, integridad y disponibilidad, según lo definido por el Grupo de **Gestión Informática** realizando seguimiento, registro y control de Backups.

b. Los medios de las copias de respaldo se almacenarán tanto en cada oficina o grupo como también en un sitio de custodia físico o almacenamiento en la nube a cargo de la **Gestión Informática** de la **CEMID**, procurando la protección ambiental y de control de acceso físico.

c. Se establecerá un plan de restauración o duplicación de copias de seguridad de servidores críticos que serán probados periódicamente según las necesidades y capacidades de la **CEMID** por el

Grupo de **Gestión Informática**, con el fin de asegurar su confiabilidad en caso de emergencia. Las copias serán conservadas por un periodo de tiempo acorde a las tablas de retención documental definidas por la entidad.

d. La **Gestión Informática** de la **CEMID**, establecerá las instrucciones de resguardo y recuperación de la información que incluyan especificaciones acerca de su traslado, duplicación, identificación; así mismo, comunicará a los usuarios los periodos de retención de la información que les atañe.

e. Se debe disponer de los recursos necesarios para identificar y adquirir los medios de almacenamiento, mantener la información contenida en ellos, garantizar periodos de realización de copias y la ubicación física de los mismos, de manera que se garantice un acceso rápido y eficiente a ellos y a la información crítica resguardada de la **CEMID**.

13. Responsabilidades Gestión Informática

a. Promover el cumplimiento de las políticas de seguridad de la información por parte del personal bajo su cargo.

b. Gestionar los recursos financieros que se requieren para la una protección apropiada de los activos tecnológicos de la información.

c. Implementar, administrar y mejorar constantemente los medios y herramientas tecnológicas para cumplir con las políticas de seguridad de la información.

d. Implementar controles específicos de seguridad de la información y garantizar que estos son auditables.

e. Implementar, actualizar y administrar los controles de seguridad de la información, así como las conexiones de la estructura de red de datos bajo la administración propia o de terceros.

f. Definir e implementar un plan de capacitación y concientización en seguridad de la información, para los colaboradores directos, contratistas, practicantes o cualquier persona que deba tener acceso a los activos tecnológicos de la información de la **CEMID**.

g. Custodiar los medios de almacenamiento y la información contenida en ella, que estén bajo cargo de la **Gestión Informática**.

h. Acatar las recomendaciones derivadas en los análisis de vulnerabilidad o de riesgos, que se generen en la actividad propia o por consultorías contratadas para ello; o por sugerencia de las casas de software cuyos servicios fueran contratados para apoyar las actividades diarias de la empresa.

i. Definir, mantener y controlar la lista actualizada de software, aplicaciones autorizadas y el licenciamiento.

j. Monitorear y evaluar los procesos o actividades de las plataformas tecnológicas contratadas a terceros.

k. Establecer procedimientos de contingencia que garanticen la continuidad del negocio, para cada una de las plataformas tecnológicas críticas bajo la responsabilidad de la **Gestión Informática**, esos procedimientos deben ser susceptibles de verificación, monitoreo y validación.

l. Establecer, documentar y actualizar los procedimientos de seguridad de la información que apliquen para las plataformas tecnológicas administradas por la Gestión Informática.

m. Gestionar y documentar los incidentes que se presenten en seguridad de la información.

n. Realizar análisis de vulnerabilidad en las plataformas tecnológicas que produzcan recomendaciones y mejoras.

o. Monitorear el uso de los activos de información de la entidad, para prevenir el impacto de los riesgos derivados por pérdida de integridad, disponibilidad y confidencialidad de la información.

p. Determinar en común acuerdo con las direcciones, los privilegios de acceso a los activos de información. Realizar actividades de mantenimiento y administración de esos privilegios.

14. Responsabilidades de Colaboradores, Oficinas y Grupos que hacen parte de la CEMID

a. Gestionar en los programas de inducción y/o re-inducción, la inclusión del tema de seguridad de la información asegurando que los colaboradores conozcan sus responsabilidades, así como las implicaciones por el uso inadecuado de los activos de información u otros recursos informáticos, enfatizando en las consecuencias jurídicas que pueden derivar de esta mala práctica.

b. Hacer conocer que la información almacenada en los activos tecnológicos de la **CEMID** es responsabilidad del colaborador, quien determina la criticidad de esta y la clasifica basándose en su valor, sensibilidad, riesgo de pérdida o compromiso y/o requerimientos legales de retención, para todo esto se apoya con el grupo de **Gestión Informática**.

c. Acordar con la **Gestión Informática**, la definición de los requerimientos de continuidad y de recuperación en caso de desastre de la información si llegara a ser necesario, teniendo en cuenta la periodicidad vigente de los Backups.

d. Hacer conocer al grupo de **Gestión Informática** sus requerimientos de seguridad de información.

e. Los colaboradores de la **CEMID** deben contar con los medios necesarios para cumplir con sus responsabilidades de Seguridad Informática desde su ingreso hasta su retiro, siendo conscientes que la información almacenada en ellos es responsabilidad del funcionario. Deberá gestionar ante la dirección a la que está adscrito, los elementos que considere le ayuden a garantizar esta actividad y que sean diferentes al estándar que ofrece la **Gestión Informática**.

15. Política de Uso Adecuado de los Activos de Información

Conforme a lo establecido en la política de seguridad informática y la legislación vigente, la **CEMID** podrá monitorear y supervisar la información, los sistemas, los servicios y los equipos que sean de su propiedad.

Conforme a lo establecido en la política de seguridad informática y la legislación vigente, la **CEMID** podrá monitorear y supervisar la información, los sistemas, los servicios y los equipos que sean de su propiedad.

15.1. **Internet**:

a. La navegación en internet se controlará conforme a las reglas de navegación generales definidas para los perfiles de usuario; sin embargo, los siguientes usos no son aceptables por parte de la **CEMID**:

1. Visitas a sitios de contenido sexualmente explicito, de contenido discriminatorio, de contenido que implique un delito informático o cualquier otro contenido que se considere fuera de los límites permitidos.
2. Comercio, adquisición o publicación de contenido sexualmente explicito, contenido discriminatorio o cualquier otro contenido que se considere fuera de los límites permitidos.
3. Comercio, publicación o envió de información confidencial de la **CEMID**, sin aplicar controles para salvaguardar la información o sin contar con la autorización de los propietarios respectivos.
4. Utilizar servicios disponibles a través de la red que permitan intercambios de información no autorizados.
5. Descargar, copiar o piratear software y archivos electrónicos sujetos a derechos de autor, así mismo descargar programas en los equipos informáticos de la **CEMID** sin el consentimiento del grupo de **Gestión Informática**.
6. Descargar, instalar y utilizar programas de aplicación o software no relacionados con la actividad laboral de la **CEMID** y que afecte el procesamiento de la estación de trabajo o de la red.
7. Publicación de anuncios comerciales o material publicitario, salvo los corporativos que dentro de sus funciones así lo requieran. Lo anterior deberá contemplar una solitud previa, avalada por la dirección a la cual el funcionario esté adscrito.
8. Promover o mantener asuntos o negocios personales, usando las conexiones de la **CEMID**.
9. Emplear cuentas de correo externas no corporativas para él envió o recepción de información institucional.
10. Utilización de las cuentas de correo personales, no corporativas, o navegación en redes sociales, sin una justificación por parte de la entidad.
11. Uso de herramientas de mensajería instantánea diferentes a las corporativas ofrecidas por la **CEMID**.

b. La **Gestión Informática** tendrá la facultad de monitorear o controlar las videoconferencias o videollamadas que se generan con los medios corporativos entre las diferentes áreas de la **CEMID**, en cualquiera de sus sedes, con el fin de garantizar que estas se realicen sin intervenciones, verificando la navegación responsable y no abusiva.

c. Se realizará un registro permanente de tiempos de navegación y páginas visitadas por los colaboradores y terceros autorizados, para un posterior monitoreo; de igual manera, se podrá inspeccionar, registrar e informar las actividades realizadas durante la sesión de navegación.

d. El uso de Internet por los colaboradores de la **CEMID** está permitido y alentado cuando su uso apoya los objetivos de la corporación y mientras no infrinja ninguna de las restricciones anteriores.

e. Está prohibido el uso de internet con el propósito de navegar sitios como YouTube, Facebook, Instagram, otras redes sociales o servicios de descarga en línea de material protegido por derechos de autor; excepto con autorización explícita del jefe inmediato previamente avalado por el grupo de **Gestión Informática**.

15.2. Correo electrónico Institucional o Corporativo

a. La cuenta de correo electrónico institucional debe ser usada para el desempeño de las funciones asignadas dentro de la **CEMID**.

b. Los mensajes y la información contenida en los buzones institucionales son de propiedad de la **CEMID**. Cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones. Por este motivo la información, y el tráfico de la misma, se consideran de interés de la entidad.

c. La capacidad de almacenamiento de los buzones y mensajes de correo serán determinados para la **CEMID**, por parte del proveedor del servicio, las cuentas serán administradas por el grupo de **Gestión Informática**, y sus características se ajustarán a las necesidades de cada usuario, acordadas con el jefe inmediato.

d. La **CEMID** suministrará una cuenta de correo electrónico corporativa para el envío de correos institucionales, a cada oficina que lo requiera, previa autorización de la dirección a la que está adscrita.

e. El uso del correo electrónico corporativo se considera inadecuado para los siguientes fines:

1. Enviar o retransmitir cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.
2. Él envió de cualquier tipo de archivo adjunto que vulnere la seguridad de la información.

f. Toda la información que requiera ser enviada fuera de la **CEMID**, debe estar en formatos no editables y protegida con mecanismos de seguridad. Solo puede ser enviada en el formato original y sin restricción de bloqueo, bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a esa información.

g. Todo mensaje de correo electrónico deberá acogerse al estándar de formato e imagen corporativa definidos para la **CEMID** y deberá contener al final un texto en el que se incluya:

1. El mensaje (incluso cualquier Anexo) contiene información confidencial y se encuentra protegido por la ley.
2. El mensaje solo puede ser utilizado por la persona o empresa a la cual está dirigido.
3. Solicitud de eliminación inmediata del mensaje en caso de que este sea recibido por alguna persona o empresa no autorizada.
4. Prohibir la retención, difusión, distribución, copia o toma de cualquier acción basada en el mensaje.

15.3. Redes Inalámbricas:

Para las sedes en las que la **CEMID** ha implementado el uso de redes inalámbricas dentro de las instalaciones, se deben tener en cuenta las siguientes directrices:

a. Se procurará la implementación de ambientes de trabajo independientes para la red operativa y la red con servicio de internet a fin de minimizar los riesgos de intrusión a las redes institucionales.

b. Los usuarios de las redes inalámbricas se deben someter a las mismas condiciones de seguridad de las redes cableadas en lo que tiene que ver con identificación, autenticación, control de contenido de internet y cifrado, en algunos casos las condiciones para el servicio Wi Fi deberán ser incluso más estrictas.

c. Se deben implementar soluciones de red inalámbrica que permitan configuraciones de seguridad. En ningún caso se podrá dejar las configuraciones y contraseñas que vienen de fábrica.

15.4. Segmentación de Redes

a. La infraestructura y/o plataforma tecnológica de la **CEMID** que soporta los sistemas de información deberá considerar escenarios de segmentos de red físicos y lógicos independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet.

b. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos, de enrutamiento y de seguridad, si así se requiere. El Grupo de **Gestión Informática**, estará a cargo de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

15.5. Computación en la Nube (Cloud Computing)

La **CEMID** implementara el uso de Computación en la Nube, según los requerimientos, tanto para el almacenamiento de información dinámica o de Backups de la entidad, se deben tener en cuenta las siguientes directrices:

a. La **CEMID**, implementará servicios de nube privada, a fin de hacer uso de las facilidades y bondades tecnológicas, garantizando la implementación de los controles adecuados.

b. La **CEMID** en la actualidad cuenta con servidores web que archivan parte de la información de la entidad, en donde se tendrán en cuenta las directrices para la Computación en la Nube.

c. Se deberán capacitar a los funcionarios en el manejo del almacenamiento en la nube.

15.6. Sistemas de Información con Acceso Público

a. La información ofrecida al pública y producida al interior de la **CEMID** se deberá resguardar de posibles modificaciones que afecten la imagen corporativa.

b. En la página de la **CEMID**, se deber publicar la política de protección de datos personales la cual incluirá en uno de sus apartados la política de privacidad y uso.

c. La **CEMID**, garantizará el derecho Habeas Data a todos los públicos que utilizan los diferentes módulos de consulta y servicios ofrecidos en los portales corporativos además de ello garantizará la seguridad de la información ingresada a través de estos medios, con la salvedad de que no se es responsable de la veracidad de esa información.

d. Toda la información publicada en los portales institucionales, o en cualquier otro medio, debe contar con la revisión y aprobación de la gestión o departamento a la que conciernen dichos datos.

15.7. Recursos Tecnológicos:

a. Los integrantes de la **Gestión Informática** son los únicos autorizados para la instalación de todo tipo de software en los equipos de cómputo de la **CEMID**.

b. Los colaboradores de la **CEMID** deberán utilizar los recursos informáticos y medios tecnológicos que se le asignen para realizar las funciones específicas de su cargo, por ende, todo software instalado en sus equipos debe contar con su respectiva licencia.

c. Como política de seguridad ningún activo de información debe ser instalado con la configuración establecida por defecto por el fabricante o por el proveedor, en esta regla se incluyen las cuentas y claves de administrador.

d. Los usuarios en general deben abstenerse de realizar cambios físicos en las estaciones de trabajo referentes a cableado, cambio de ubicación, mantenimientos, repotenciación, modificaciones en su configuración física, conexiones de red, o equipos periféricos y/o modificaciones lógicas como configuraciones del equipo, manipulación de usuarios locales de la máquina, cambios en tapiz y protector de pantalla. Estos cambios son responsabilidad únicamente del Grupo de **Gestión Informática** de la **CEMID**.

e. Los equipos de cómputo de la **CEMID** asignados a cada colaborador, deberán ser reintegrados a la dependencia responsable con la información que se genere durante el desempeño de su cargo, cada vez que se presente un cambio de dispositivo por actualización o deterioro, o cuando el responsable de dicho elemento finalice su vinculación con la entidad. En consecuencia, los departamentos que componen la **CEMID** no deben almacenar equipos de cómputo en sus oficinas una vez haya finalizado el uso de los mismos.

f. El colaborador que maneje recursos informáticos y/o tecnológicos, es responsable por el cuidado y buen uso del elemento que se le asigne, por ende, su uso estará limitado única y exclusivamente a trabajos relacionados con su labor en la **CEMID**.

g. Los funcionarios de la **CEMID** tienen la obligación de dejar los recursos tecnológicos bajo llave o vigilancia, cuando no los esté utilizando o al culminar la jornada laboral, para garantizar la seguridad de la información.

16. Política de Concientización y Capacitación de Seguridad de la Información

a. La **CEMID**, programará capacitaciones anuales con el fin de dar a conocer las políticas de seguridad de la información y adelantará campañas informativas a través de los medios electrónicos existentes.

b. Se debe informar y capacitar a todos los colaboradores y contratistas de la **CEMID**, acerca del cumplimiento de las Políticas de Seguridad de la Información y de los aspectos necesarios para desempeñar sus funciones, durante su proceso de vinculación. Se realizarán actividades de reinducción cuando dichas políticas sean actualizadas.

c. Los colaboradores de la **CEMID** deberán ser capacitados en seguridad de la información, incluyendo aspectos como:

- Seguridad en claves de acceso.
- Acuerdos de confidencialidad y no divulgación de la información.

- Ataques de ingeniería social.
- Uso y edición de la página web de la entidad.
- Normatividad tecnológica.
- Uso de la plataforma para videoconferencias.
- Seguridad informática.

d. Se establecerá al interior de la **CEMID**, un programa permanente que propenda la creación de una cultura en seguridad de la información que incluya a todos los usuarios y terceros, cumpliendo un cronograma de capacitaciones anual ejecutado por el Grupo de **Gestión Informática**, de igual manera, se generará documentación de acceso público en la intranet de la entidad, donde se desarrollen temas de seguridad informática dirigidos a las acciones cotidianas de los colaboradores.

17. Política de Finalización de la Relación Laboral

Al momento de la desvinculación o traslado, todo funcionario y/o tercero debe hacer devolución formal de todos los activos de información y activos tecnológicos asignados a su cargo, en el momento de su vinculación, relacionados en el **ACTA DE ENTREGA Y REGLAMENTO DE USO DE EQUIPOS**, estos serán entregados conforme al proceso de manejo de activos implementado por la dirección administrativa. Esta entrega hace parte del proceso de emisión de paz y salvo ante la entidad.

Por su parte, el Grupo de **Gestión Informática** cuenta con dos módulos uno llamado **SOLICITUD DE SERVICIOS INFORMATICOS**, y otro **INVENTARIO GESTIÓN INFORMÁTICA** con los que lleva control y seguimiento de los activos de la información de la entidad.

18. Política de Trabajo de Áreas Protegidas

a. Todas las áreas que se hayan definido como protegidas y activos de información que le componen, mediante el procedimiento de control de acceso a área protegida, son considerados áreas seguras por lo tanto deben ser protegidas de acceso no autorizado mediante controles.

b. Todo acceso físico a las áreas protegidas deberá ser manejado según los lineamientos definidos por la gestión o grupo a quien competa el área protegida.

c. Se debe acatar las siguientes indicaciones en las áreas protegidas, en las que se encuentren activos informáticos:

1. Prohibido el consumo de alimentos y bebidas.
2. Prohibido ingresar elementos inflamables.
3. El ingreso de personal ajeno a la entidad está estrictamente restringido, salvo que este acompañado por un funcionario durante la vista y previa autorización del dueño del proceso de la gestión.
4. Se debe implementar un formato en el que se registre cada ingreso al área protegida, el cual debe incluir la relación de la persona o personas que ingresan, fecha y hora del evento, motivo de la visita y firma.
5. Está expresamente prohibido el almacenaje de elementos ajenos a la funcionalidad de la respectiva zona protegida.
6. Tomar fotos o grabaciones de las áreas protegidas está prohibido, salvo previa autorización de la gestión o departamento responsable de la misma.

7. No está permitido el ingreso de equipos electrónicos, maletas o contenedores a las zonas protegidas, a menos que exista una justificación válida y autorización previa para ello. En estos casos, estos elementos ingresados deberán ser registrados tanto al ingreso como a la salida con el ánimo de minimizar la posibilidad de intrusión de dispositivos no autorizados o la extracción de elementos propios del área protegida.

19. Política de mantenimiento y seguridad de los dispositivos informáticos

a. Todos los equipos que hacen parte de la infraestructura tecnológica de la **CEMID** deberán ser ubicados y protegidos adecuadamente para preservarlos de acceso no autorizado, perdida, daño o robo.

b. La **CEMID** adoptara los controles necesarios para mantener los dispositivos alejados de sitios en donde existan riesgos potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo entre otros.

c. Los colaboradores directos, temporales, contratistas, practicantes, terceros o cualquier persona que se relacione contractualmente con la entidad, deberán propender el adecuado uso de los dispositivos informáticos que se les haya asignado, por ende, está prohibido el préstamo de dichos equipos a personas ajenas a la institución o a su gestión sin una autorización previa. De igual manera ningún elemento deberá salir de las instalaciones sin haber tramitado los permisos previstos en el proceso que para tal fin ha estipulado la dirección administrativa.

d. Se deben realizar y registrar mantenimientos periódicos de la infraestructura utilizada para el procesamiento de datos, para las comunicaciones y para la seguridad informática, con el fin de que se garantice la no intermitencia de estos procesos y que no se vean afectadas por obsolescencia. Es indispensable revisar rutinaria miente la vida útil de cada recurso que compone dicha infraestructura de acuerdo con las recomendaciones de los fabricantes.

e. Los elementos como impresoras, copiadoras, multifuncionales y escáneres deberán estar ubicados en zonas protegidas, y deberán contar con un control de acceso, de manera que se garantice un uso adecuado y solo por personal autorizado.

f. Todos los dispositivos informáticos deberán protegerse con un cierre de sesión temporal cuando no vayan a estar utilizándose por el responsable encargado, esta política aplica dentro y fuera de las instalaciones de la **CEMID**.

g. La **CEMID** propenderá por la existencia de pólizas o seguros para la reposición de los activos informáticos que respalden los planes de contingencia y la continuidad de las actividades de los departamentos.

h. Los equipos de cómputo de la **CEMID** deben tener un mantenimiento anual mínimo, como se menciona en el documento "**POLÍTICA DE USO ACEPTABLE (INTERNET, COMPUTADORES Y CORREO CORPORATIVOS) Y BACKUPS - PUAB**"

20. Política de Seguridad de dispositivos asignados para uso fuera de las instalaciones

a. Los usuarios que requieran manipular los dispositivos por fuera de las instalaciones de la **CEMID** deberán tramitar el requerimiento bajo el protocolo establecido por la dirección administrativa, y tendrán

la responsabilidad de velar por la protección de los elementos a su cargo sin dejarlos desatendidos, comprometiendo la imagen o información de la entidad.

b. El responsable del activo, con el apoyo del equipo de **Gestión Informática**, identificará mediante una metodología que la **CEMID** establezca, los riesgos potenciales que se originen a raíz del uso de los dispositivos por fuera de la entidad, de igual manera, deberá adoptar los controles necesarios para la mitigación de esos riesgos.

c. En caso de pérdida o robo de cualquier dispositivo informático que contenga información relacionada con la **CEMID**, se deberá realizar inmediatamente el respectivo reporte siguiendo los parámetros establecidos por la dirección administrativa, los cuales incluyen entre otros informar inmediatamente al área encargada y realizar las respectivas denuncias ante las autoridades legales competentes, cuando sea necesario.

d. Todos los dispositivos informáticos que por razones que atañen al cargo, se autoricen para uso por fuera de las instalaciones de la **CEMID**, deberán contener únicamente la información estrictamente necesaria para el cumplimiento de su actividad y se deshabilitaran los recursos que no se requieran o que puedan poner riesgo a la información, todo ello concertado con jefes directos o dueños de proceso del área responsable.

21. Política de Documentación de Procedimientos Operativos

a. Las actividades relacionadas con la infraestructura tecnológica para el procesamiento de información, comunicaciones y seguridad informática deben estar documentadas por instrucciones o procedimientos operativos que deben estar a disposición de los usuarios que en su actividad lo requieran, y que cumplan con los estándares exigidos en el documento "**PROCEDIMIENTO PARA EL CONTROL DE LA DOCUMENTACIÓN (PGGC-01)**" del sistema de gestión de calidad.

b. La mesa de ayuda o el equipo de soporte de la **Gestión Informática** debe contar con la documentación de los procedimientos operativos, así como el procesamiento y manejo de información, manejo de errores, contactos de soporte o escalamiento, de igual forma instrucciones para el manejo de medios y exposición de resultados especiales y de carácter de confidencial.

c. Los procedimientos operativos deben contener instrucciones para el manejo de los errores, contactos de soporte o escalamiento, procedimientos de reinicio y recuperación de sistemas y aplicaciones, forma de procesamiento y manejo de la información, copia de respaldo de la información y los demás a los que hubiere lugar, los cuales están contenidos en el **plan de continuidad del negocio** , la directiva de copias de seguridad, manuales y demás documentos que soportan tales procedimientos de la **CEMID**.

22. Política de Control de Cambios Operativos

a. La **Gestión Informática** deberá controlar, gestionar y autorizar todo cambio que se realice sobre los sistemas de información e infraestructura tecnológica, cumpliendo con una planificación y ejecución de pruebas en ambientes controlados que permitan la identificación de riesgos e impactos potenciales asociados. En la medida de lo posible, todos los cambios que se realicen sobre los sistemas de información e infraestructura tecnológica deben contar con un plan de contingencia, respaldo y reversión.

b. Todos los cambios que se realicen sobre los sistemas de información y la infraestructura tecnológica deberán estar debidamente justificados y autorizados por las directivas o jefaturas pertinentes en base a la definición de requerimientos, especificaciones y controles definidos en la **Gestión Informática** siempre velando por mantener la confidencialidad, integridad y disponibilidad de la información.

23. Política de Segregación de Funciones

a. Todas las personas que tengan acceso a la infraestructura tecnológica o a los sistemas de información, deben contar con roles y funciones claramente definidos para mitigar, controlar y evitar el uso no autorizado o modificación de los activos de información de forma intencional o no. Estos se registrarán en el **Documento de roles y funciones**.

b. La segregación de funciones sobre la infraestructura tecnológica y los sistemas de información deberá ser revisada anualmente por la **Gestión Informática** y dependencias que consideren necesarias, con el fin de mantenerlas documentadas y actualizadas acorde con la realidad de la corporación.

24. Política de Separación de Ambientes

a. Se contarán con espacios físicos y/o lógicos para los ambientes de pruebas y producción en la infraestructura tecnológica y los sistemas de información de la corporación con el propósito de reducir el acceso no autorizado y cambios que repercutan en la operación de la entidad.

b. Quedan prohibidas las pruebas y desarrollos físicos o lógicos en los ambientes productivos.

25. Política de Protección contra Software Malicioso

a. Se debe contar con hardware y software de detección, prevención, protección, aislamiento y recuperación para todos los recursos tecnológicos y de comunicación con los que cuente la organización, con el fin de prevenir y/o eliminar código malicioso en la red y los dispositivos finales.

b. Las herramientas de protección y los dispositivos brindados por la entidad a sus colaboradores deben permanecer actualizados para prevenir software malicioso de última generación.

c. Los mecanismos de seguridad implementados ya sean hardware o software no debe ser desactivados sin la autorización de la **Gestión Informática**.

d. Queda prohibido el uso de cualquier tipo de software diseñado para autorreplicarse, dañar, espiar, capturar datos, afectar el desempeño, o cualquier otro tipo de actividad que se considere puede atentar o vulnerar la red, los equipos o a sus usuarios.

e. Los medios de almacenamiento deben ser analizados en busca de software malicioso que atente contra la seguridad de la infraestructura y sus usuarios; así mismo, se programarán análisis periódicos en busca de éstos.

f. La instalación y ejecución de programas de tipo instalador o portables que no hagan parte del listado de software permitido en la **CEMID** debe ser validado por la **Gestión Informática** con previa justificación y autorización.

g. La **CEMID** mantendrá informados a los usuarios sobre los riesgos y amenazas a la seguridad de la información, medios de transmisión, metodologías y demás información necesaria, con el fin de minimizar y controlar rápidamente toda acción sospechosa sobre la infraestructura y su información.

26. Política de Gestión de Registros

a. Los sistemas de información y de comunicaciones críticos deberán generar registros de eventos que puedan ser estudiados para prevenir, analizar y rastrear las actividades, comportamientos, accesos, riesgos o fallos en los sistemas.

b. La retención de los registros de eventos estará dada por las condiciones específicas de cada sistema de información o dispositivo que componga la infraestructura tecnológica, y deberá regirse por las leyes, normativas o regulaciones vigentes.

c. Los eventos que se identifiquen proactivamente o por requerimiento a través de los sistemas de monitoreo y revisión serán reportados al jefe de la **Gestión Informática**.

27. Política de Control de Acceso

a. La **CEMID** contará con los mecanismos para crear, modificar, actualizar y eliminar usuarios, así como gestionar los roles y permisos y accesos a los diferentes sistemas de información y equipos informáticos.

b. El acceso remoto o local a los activos de la información de la **CEMID** estará permitido únicamente a los usuarios autorizados por la **Gestión Informática**.

c. Todas las conexiones remotas deberán ser autenticadas y seguras antes de conceder acceso.

d. Los usuarios de uso temporal o de terceros deben tener una fecha de vencimiento limitado a la fecha contractual establecida.

e. La asignación de roles, permisos y funciones de los usuarios estarán definidos según el cargo. Todo cambio debe ser autorizado por la dirección o jefatura pertinente. Esta tipificación debe revisarse periódicamente. Toda solicitud que exija cambio en el perfilamiento de usuario o función ya sea por promociones, ascensos, traslados, cambios de cargo o terminación de la relación laboral, debe ser reportado a la **Gestión Informática**.

f. Los accesos a la red inalámbrica deberán ser autorizados por la **Gestión Informática** de la **CEMID**, previa verificación de que cuenten con las condiciones de seguridad, estableciendo mecanismos de control necesarios para proteger la infraestructura.

28. Política de Administración de Contraseñas

a. La administración, asignación y entrega de las contraseñas de los usuarios estará a cargo de la **Gestión Informática**.

b. Los usuarios deberán establecer contraseñas seguras que deberán cambiar al menos una vez al año.

c. El colaborador interno y/o externo se responsabilizará de cualquier acceso o acción que se realice utilizando su nombre de usuario y contraseña tanto en los activos de información, el usuario local y el directorio activo.

d. Las contraseñas son de uso personal e intransferible, excepto para los casos en que sean entregadas para la custodia a la **Gestión Informática**.

e. Las contraseñas no deberán ser reveladas.

f. Toda sospecha de uso indebido o no autorizado del usuario y contraseña debe ser reportada a la **Gestión Informática**.

29. Política de Gestión de Incidentes de Seguridad de la Información

a. Todo usuario interno o externo debe informar cualquier evento sospechoso que ponga en riesgo los activos de información y que comprometa la confidencialidad, integridad y disponibilidad de la información.

b. Todos los incidentes que se consideren graves deben ser registrados, de igual forma deberán reportarse a los entes de control interno y a las entidades judiciales encargadas.

c. Se registrarán los incidentes de forma detallada, los activos de información involucrados y afectados, la respuesta, y demás información que se considere relevante para el caso, seguimiento, evaluación, solución y acción de mejora.

d. Los resultados de las investigaciones que involucren a los funcionarios de la **CEMID** deberán ser informados a las áreas competentes y al jefe directo.

30. Política de Seguridad de la Información en la Continuidad del Negocio

a. La seguridad de la información es una prioridad y debe ser tratada como activo vital para la continuidad del negocio, debe incluirse como parte esencial de toda gestión en la organización y hacer parte de compromiso de la alta gerencia.

b. Debe existir un **Plan de Continuidad de Negocio** para la operación de los procesos críticos ante cualquier incidente intencional, no planeado o natural y debe articularse con los planes de contingencia de los proveedores de servicios o de plataformas tecnológicas.

c. Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades relacionadas con el plan, estarán incorporados y definidos en el **Plan de Continuidad del Negocio**.

d. La **Gestión Informática** tendrá la responsabilidad de mantener documentados y actualizados los procesos internos de resolución de incidentes de seguridad informática e informar cualquier cambio al responsable del **Plan de Continuidad de Negocio**.

31. Política de Derechos de Propiedad Intelectual

a. La **CEMID** cumplirá con la reglamentación vigente sobre la propiedad intelectual, para lo cual implementará los controles necesarios que garanticen el cumplimiento de las normas.

b. No se permitirá el almacenamiento, descarga, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal.

c. Se permitirá el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite el autor de los mismos, con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.

d. Los procesos de adquisición de aplicaciones, plataformas y paquetes de software cumplirán con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor.

e. El software a la medida, adquirido a terceras partes para la **CEMID**, será de uso exclusivo de la entidad y la propiedad intelectual será de quien lo desarrolle.

f. El material elaborado, desarrollado y almacenado en los dispositivos otorgados por la corporación están cubiertos bajo los derechos de la propiedad intelectual de la entidad.

32. Política de asignación, renovación y obsolescencia de equipos

a. La solicitud de equipos para usuarios nuevos debe ser tramitada por el jefe inmediato o dirección encargada a la Dirección Administrativa quienes gestionarán la solicitud de cotización y compra con las áreas encargadas. La **Gestión Informática** supervisará, alistará y asignará el activo o activos al responsable que dispondrá del elemento.

b. Los dispositivos serán configurados y asignados según el **protocolo de alistamiento de equipos** teniendo en cuenta el perfil del usuario y las necesidades para un correcto desempeño de su labor.

c. La actualización o renovación de los equipos debe ser tramitada por el jefe inmediato o dirección encargada a la Dirección administrativa con el aval de la **Gestión Informática**.

d. En general la vida útil de los equipos de IT es de 3 años, pero su uso posterior a la depreciación total no debe exceder en más de 2 años los límites de las normas vigentes para los activos de la organización.

Los dispositivos de almacenamiento deben tener un tratamiento especial para su disposición final con el objetivo de mantener la confidencialidad.

33. APLICABILIDAD

33.1. El contenido de este documento aplica a todos los procesos y procedimientos que conforman el Sistema Integrado de Gestión de la calidad de la CEMID, de igual manera a todas las actuaciones administrativas que se ejecuten desde las distintas unidades, por intermedio de sus administrativos, contratistas, docentes y colaboradores en general**.**

33.2. La violación a las disposiciones del contenido de este documento dará lugar a sanciones disciplinarias, administrativas, civiles y/o penales de conformidad con lo establecido en las leyes colombianas vigentes.