POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

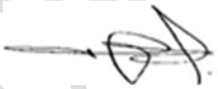
	ACTUALIZÓ	REVISÓ	APROBÓ
FIRMA:			
NOMBRE:	**FERNANDO CELIS CLAROS**	**María Elvira Yagüe Hurtado**	**Oriana Sofía Peña Mazabel**
CARGO:	Líder Gestión de las Tecnologías	Subdirectora Administrativa y Financiera	Gerente
FECHA:	16/01/2023	16/01/2023	16/01/2023

Tabla de contenido

1 OBJETIVO

Definir directrices y lineamientos necesarios que deben seguir los Funcionarios, Colaboradores y Terceros de la ESE Manuel Castro Tovar, con el fin de fortalecer la Seguridad de la Información y garantizar la disponibilidad, integridad y confidencialidad de la información.

2 ALCANCE

Aplica para todos los Funcionarios, Colaboradores y Terceros de la ESE Manuel Castro Tovar.

3 DEFINICIONES

- **Activo de Información:** Es todo aquello que en la ESE Manuel Castro Tovar es considerado importante o de alta validez para la misma ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.
- **Amenaza:** Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.
- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Copias de respaldo:** 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.
- **Dato:** Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Información:** Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Riesgo:** Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.
- **Servidor:** Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

4 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Con el fin de responder a la necesidad de asegurar un alto grado de cumplimiento en los pilares fundamentales de la seguridad y la privacidad de la información manejada en la ESE Manuel Castro Tovar, se elaboran una serie de políticas que se describen a continuación:

4.1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La ESE Manuel Castro Tovar se compromete a otorgar los recursos necesarios para contribuir de manera gradual en los tres (3) pilares fundamentales de la Seguridad como son la disponibilidad, integridad y confidencialidad de la información, con el fin de dar cumplimiento a los objetivos institucionales, la estrategia y misión de la ESE Manuel Castro Tovar.

La Dirección General se compromete a velar por la aplicación y cumplimiento adecuado de la presente política de seguridad de la información y todas las que se deriven de ella, por parte de todos los Funcionarios, Colaboradores y Terceros de la ESE Manuel Castro Tovar.

La Entidad se compromete a cumplir con los requisitos legales, reglamentarios y contractuales que haya a lugar, con el fin de gestionar y reducir los riesgos a un nivel aceptable.

Establecer la mejora continua del Sistema de Gestión de Seguridad de la Información, a través de un conjunto de reglas y directrices orientadas a garantizar la protección de los activos de información de la ESE Manuel Castro Tovar, de una manera contundente, eficiente y efectiva, de la misma forma velar por tomar las acciones necesarias para la evaluación, análisis y tratamiento de los riesgos de acuerdo a la metodología adoptada por la Entidad.

4.1.2 POLÍTICA DE PRIVACIDAD

La ESE Manuel Castro Tovar se compromete a otorgar los recursos necesarios para contribuir con los tres (3) pilares fundamentales de la privacidad de la información como son la finalidad, consentimiento y responsabilidad de información.

La Dirección General se compromete a velar por la aplicación y cumplimiento adecuado de la presente política de privacidad de la información y todas las que se deriven de ella, por parte de todos los Funcionarios, Colaboradores y Terceros de la ESE Manuel Castro Tovar.

La Entidad reconoce que el único medio autorizado para el tratamiento de datos personales es el dueño de la información, de acuerdo a la Ley de protección de datos personales 1581 de 2012 decreto 1377, o la que la adicione, modifique o derogue.

4.1.3 POLÍTICA DE ROLES Y RESPONSABILIDADES

Objetivo: Definir los Roles y Responsabilidades en Seguridad de la Información en la ESE Manuel Castro Tovar.

Todos los Funcionarios, Colaboradores y Terceros que ejercen funciones en la ESE Manuel Castro Tovar y previamente han sido autorizados para acceder a los recursos tecnológicos y de procesamiento de información de la Entidad, son responsables del cumplimiento de las políticas, procedimientos y normatividad vigente definida por la ESE Manuel Castro Tovar.

Es responsabilidad de todos los Funcionarios, Colaboradores y Terceros almacenar la información en la carpeta designada para ello, los documentos resultado de sus funciones laborales, ya que de esta forma se garantiza las copias de respaldo, lo que no se encuentre allí no queda dentro de la política.

Todos los Funcionarios, Colaboradores y Terceros de la ESE Manuel Castro Tovar deben hacer buen uso de la información que se genera del desempeño de sus funciones laborales y bajo ninguna circunstancia podrán divulgar información con categoría CONFIDENCIAL o RESERVADA en espacios públicos o privados, mediante conversaciones o situaciones que puedan poner en riesgo la seguridad o el buen nombre de la ESE Manuel Castro Tovar. Esta restricción se debe cumplir inclusive después de la terminación del vínculo laboral y contractual y debe estar incluida en los Acuerdos de Confidencialidad establecidos por la Entidad.

Si después de revisar la solicitud, se identifica que los privilegios solicitados no están definidos en la Matriz de Roles y Responsabilidades de los activos de información, se debe solicitar aprobación por parte del dueño del activo y se ejecutan por el líder del área Gestión de las Tecnologías.

Se debe capacitar a todos los usuarios solicitantes de accesos a componentes tecnológicos sobre el uso y la responsabilidad que implica contar con esos privilegios.

Los roles y privilegios en el sistema de Información Institucional deben ser actualizados cada vez que surja un cambio, de acuerdo a un requerimiento formal por parte de la gerencia de la ESE Manuel Castro Tovar.

4.1.4 SEGURIDAD DE LOS RECURSOS HUMANOS

Objetivo: Garantizar la protección de la disponibilidad, integridad y confidencialidad de la información del personal que trabaja para la ESE Manuel Castro Tovar, a través de mecanismos de validación y concientización del recurso humano que hará uso de la misma.

Control y Política del Personal

Se deben definir controles de verificación del personal en el momento en que se postula al cargo. Estos controles incluirán todos los aspectos legales y de procedimiento que dicta el proceso de contratación de la ESE Manuel Castro Tovar.

Acuerdo de Confidencialidad

Todos los Funcionarios, Colaboradores y Terceros que ingresen a trabajar en la ESE Manuel Castro Tovar, deben firmar como parte de sus términos y condiciones iniciales de trabajo, un Acuerdo de Confidencialidad o no divulgación, en caso de que no estuviere incluido como una cláusula dentro del contrato de prestación de servicios o en el Acta de Posesión del funcionario. Este acuerdo debe incluir la aceptación de las políticas y lineamientos en Seguridad y Privacidad de la Información, el tratamiento de la información de la ESE Manuel Castro Tovar, en los términos de la Ley 1581 de 2012 y las demás normas que la adicionen, modifiquen, reglamenten o complementen, así como el Decreto 1377 de 2013. Este documento debe ser archivado de forma segura por el área de Talento Humano y Contractual, según sea el caso.

Dentro del mismo acuerdo el Funcionario, Colaborador o Tercero declaran conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad ni los derechos del Funcionario, Colaborador o Tercero.

Selección de personal

Dentro de los procesos de contratación de personal o de prestación de servicios, debe realizarse la verificación de antecedentes, de acuerdo a la reglamentación.

Se deben aplicar los controles establecidos por la Entidad para otorgar el acceso a la información CONFIDENCIAL o RESERVADA por parte del personal que resulte vinculado a la Entidad.

El área de Talento humano y Contratación son los responsables de realizar la verificación de antecedentes disciplinarios, fiscales y judiciales y que se anexe la documentación requerida para la contratación.

Términos y condiciones Laborales

Todos los Funcionarios, Colaboradores y Terceros de la ESE Manuel Castro Tovar deben dar cumplimiento a las políticas y normatividad establecida en seguridad y privacidad de la información y debe ser parte integral de los contratos o documentos de vinculación a que haya lugar.

Todos los Funcionarios, Colaboradores y Terceros, durante el proceso de vinculación a la ESE Manuel Castro Tovar, deberán recibir una inducción sobre las Políticas y Lineamientos de Seguridad y Privacidad de la Información.

Entrenamiento, concientización y capacitación

Todos los Funcionarios, Colaboradores y Terceros de la ESE Manuel Castro Tovar deben ser entrenados y capacitados para las funciones, actividades y cargos que van a desempeñar, esto con el fin de sensibilizar a los usuarios sobre la protección adecuada de los recursos y la información de la Entidad. Así mismo, se debe garantizar la comprensión del alcance y contenido de las políticas y lineamientos de Seguridad de la información y la necesidad de respaldarlas y aplicarlas de manera permanente e integral desde su función.

Formación y Capacitación en Materia de Seguridad de la Información

Todos los Funcionarios, Colaboradores y Terceros cuando sea el caso, que trabajan para la ESE Manuel Castro Tovar deben recibir una adecuada capacitación y actualización periódica en materia de las políticas, normas y procedimientos de Seguridad y privacidad de la Información. Dentro del contenido se deben contemplar los requerimientos de seguridad y las responsabilidades legales, así como la capacitación sobre el uso adecuado de las instalaciones de procesamientos de información y los recursos tecnológicos informáticos que les provee la Entidad para el desempeño de sus funciones laborales y contractuales.

Procesos disciplinarios

Todos los incidentes de seguridad de la información presentados en la ESE Manuel Castro Tovar deben tener el tratamiento adecuado, con el fin de determinar sus causas y responsables.

Del resultado de los procesos derivados de los reportes y del análisis de los Incidentes de Seguridad y teniendo en cuenta el impacto y las responsabilidades identificadas, se tomarán acciones y se realizará el respectivo traslado ante las instancias correspondientes.

4.1.5 POLÍTICA DE USO DE CORREO ELECTRÓNICO

Objetivo: Definir las directrices generales del buen uso del correo electrónico en la ESE Manuel Castro Tovar.

Usos aceptables del servicio

Se debe utilizar exclusivamente para las actividades propias del desempeño de las funciones o actividades laborales a desempeñar en la ESE Manuel Castro Tovar y no se debe utilizar para otros fines.

Se debe utilizar de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos o sistemas de información e imagen de la ESE Manuel Castro Tovar.

Todos los Funcionarios, Colaboradores y Terceros que son autorizados para acceder a la red de datos y los componentes de Tecnologías de Información son responsables de todas las actividades que se ejecuten con sus credenciales de acceso a los buzones de correo.

Todos los Funcionarios, Colaboradores y Terceros deben dar cumplimiento a la reglamentación y leyes, en especial la Ley 1273 de 2009 de Delitos Informáticos, así mismo evitar prácticas o usos que puedan comprometer la seguridad de la información de la ESE Manuel Castro Tovar.

El servicio de correo electrónico debe ser empleado para servir a una finalidad operativa y administrativa en relación con la ESE Manuel Castro Tovar. Todas las comunicaciones establecidas mediante este servicio, sus buzones y copias de seguridad se consideran de propiedad de la ESE Manuel Castro Tovar y pueden ser revisadas por el administrador del servicio o cualquier instancia de vigilancia y control, en caso de una investigación o incidentes de seguridad de la información.

Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por la ESE Manuel Castro Tovar.

El único servicio de correo electrónico controlado en la ESE Manuel Castro Tovar es el asignado directamente por la Oficina de comunicaciones, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques informáticos, virus, spyware y otro tipo de software o código malicioso.

Los demás servicios de correo electrónico son utilizados bajo responsabilidad directa y riesgo de los usuarios, siendo necesaria la aprobación y firma por parte del Director, Jefe de Oficina, Subdirector, Coordinador de Grupo de Trabajo o Supervisor de contrato; de un documento de análisis de riesgos para la autorización de sistemas de correo electrónico diferentes al institucional.

El usuario debe reportar cuando reciba correos de tipo SPAM, es decir correo no deseado o no solicitado, correos de dudosa procedencia o con virus a la Oficina de Gestión de las Tecnologías, con el fin de tomar las acciones necesarias que impidan el ingreso de ese tipo de correos. De la misma forma el usuario debe reportar cuando no reciba correos y este seguro que este no es de tipo SPAM, así la Oficina de Gestión de las Tecnologías hacen el análisis para evaluar el origen y así tomar las medidas pertinentes.

Cuando un usuario se retire de la ESE Manuel Castro Tovar, y se le haya autorizado el uso de una cuenta con acceso a la red y al servicio de correo corporativo, debe abstenerse de continuar empleándolas y debe verificar que su cuenta y acceso a los servicios sean cancelados.

Los mensajes y la información contenida en los buzones de correo son de propiedad de la ESE Manuel Castro Tovar.

Cada usuario se debe asegurar que en el reenvío de correos electrónicos, la dirección de destino es correcta, de manera que esté siendo enviado a los destinatarios que son. Si tiene listas de distribución también se deben depurar. El envío de información a personas no autorizadas es responsabilidad de quien envía el mensaje de correo electrónico.

La información almacenada en los archivos de tipo .PST es responsabilidad de cada uno de los usuarios y cada usuario debe realizar la depuración periódica del buzón para evitar que alcance su límite.

Todo usuario es responsable de reportar los mensajes cuyo origen sean desconocidos, y asume la responsabilidad de las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En los casos en que el Funcionario, Colaborador o Tercero desconfíe del remitente de un correo electrónico debe remitir la consulta a la mesa de servicios.

Si una cuenta de correo es interceptada por personas malintencionadas o delincuentes informáticos (crackers) o se reciba cantidad excesiva de correos no deseado (SPAM), la Oficina de Gestión de las Tecnologías actuará según sea el caso.

La Oficina de Gestión de las Tecnologías se reserva el derecho de filtrar los tipos de archivo que vengan anexos al correo electrónico para evitar amenazas de virus y otros programas destructivos. Todos los mensajes electrónicos serán revisados para evitar que tengan virus u otro programa destructivo. Si el virus u otro programa destructivo no pueden ser eliminados, el mensaje será borrado.

Ningún Funcionario, Colaborador o Tercero debe suscribirse en boletines en líneas, publicidad o que no tenga que ver con sus actividades laborales, con el correo institucional.

El Funcionario, Colaborar o Tercero no debe responder mensajes donde les solicitan información personal o financiera que indican que son sorteos, ofertas laborales, ofertas comerciales o peticiones de ayuda humanitaria. Por el contrario debe notificar a la Oficina de Gestión de las Tecnologías, con el fin de ejecutar las actividades pertinentes como bloquear por remitente y evitar que esos mensajes lleguen a más buzones de correo de la ESE Manuel Castro Tovar.

Usos no aceptables del servicio

Envío de correos masivos que no hayan sido previamente autorizados a través del procedimiento formal de Solicitud de Cuentas de Usuario, establecido en la ESE Manuel Castro Tovar.

Envío, reenvío o intercambio de mensajes no deseados o considerados como SPAM, cadena de mensajes o publicidad.

Envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que represente riesgo de virus.

Envío o intercambio de mensajes que promuevan la discriminación sobre la raza, nacionalidad, género, edad, estado marital, orientación sexual, religión o discapacidad, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de activos.

Envío de mensajes que contengan amenazas o mensajes violentos.

Crear, almacenar o intercambiar mensajes que atenten contra las leyes de derechos de autor.

Divulgación no autorizada de información propiedad de la ESE Manuel Castro Tovar.

Enviar, crear, modificar o eliminar mensajes de otro usuario sin su autorización.

Abrir o hacer uso y revisión no autorizada de la cuenta de correo electrónico de otro usuario sin su autorización.

Adulterar o intentar adulterar mensajes de correo electrónico.

Enviar correos masivos, con excepción de funcionarios con nivel de Director o superior, quienes sean previamente autorizados por estos para ello, o de funcionarios que en calidad de sus funciones amerite la excepción.

Cualquier otro propósito inmoral, ilegal o diferente a los considerados en el apartado “Usos aceptable del servicio” de la presente política.

4.1.6 POLÍTICA DE USO DE INTERNET

Objetivo: Definir los lineamientos generales para el buen uso del internet y asegurar una adecuada protección de la información de la ESE Manuel Castro Tovar.

Usos aceptables del servicio

Este servicio debe utilizarse exclusivamente para el desempeño de las funciones y actividades desarrolladas durante la contratación en la ESE Manuel Castro Tovar y no debe utilizarse para ningún otro fin.

Los usuarios autorizados para hacer uso del servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer los recursos tecnológicos de la Entidad o que afecte la seguridad de la información de la ESE Manuel Castro Tovar.

Todas las comunicaciones establecidas mediante este servicio pueden ser revisadas y/o monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control.

El navegador autorizado para el uso de Internet en la red de la ESE Manuel Castro Tovar es el instalado por la Oficina de Gestión de las Tecnologías.

No se permite la conexión de módems externos o internos en la red de la ESE Manuel Castro Tovar, previa solicitud autorizada por la Oficina de Gestión de las Tecnologías.

El acceso a internet por cada usuario, depende del rol que desempeñe en la ESE Manuel Castro Tovar y para los cuales este formal y expresamente autorizado.

Todo usuario es responsable de informar el acceso a contenidos o servicios no autorizados o que no correspondan al desempeño de sus funciones o actividades dentro de la ESE Manuel Castro Tovar.

Para realizar intercambio de información de propiedad de la ESE Manuel Castro Tovar con otras entidades, se debe seguir un proceso formal de requisición de la información, el cual debe contar con la previa autorización del dueño de la información o de acuerdo a lo establecido por la Ley.

La ESE Manuel Castro Tovar se reserva el derecho de realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los usuarios. Así mismo, revisar, registrar y evaluar las actividades realizadas durante la navegación.

Todos los usuarios que se encuentren autorizados son responsables de dar un uso adecuado de este recurso y por ninguna razón pueden hacer uso para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información, la seguridad de la información, entre otros.

Los Funcionarios y Colaboradores y Terceros de la ESE Manuel Castro Tovar no deben asumir en nombre de la ESE Manuel Castro Tovar, posiciones personales en encuestas de opinión, foros u otros medios similares.

Este recurso puede ser utilizado para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de la ESE Manuel Castro Tovar.

Usos no aceptables del servicio

Envío o descarga de información masiva de un tamaño grande o pesado que pueda congestionar la red a menos que el desempeño de las funciones lo amerite.

Envío, descarga o visualización de información con contenidos restringidos y que atenten contra la integridad moral de las personas o instituciones.

Cualquier otro propósito diferente al considerado en el apartado de Usos aceptables del servicio de la presente política.

Todos los usuarios invitados que tengan acceso al servicio de internet, deben cumplir estrictamente con las políticas de seguridad de la información, de lo contrario asumirán las acciones pertinentes.

No se permite el acceso a páginas con contenido restringido como pornografía, anonimizadores, actividades criminales y/o terrorismo, crímenes computacionales, hacking, discriminación, contenido malicioso, suplantación de identidad, spyware, adware, redes peer to peer (p2p) o páginas catalogadas como de alto riesgo dictaminado desde la herramienta de administración de contenidos de la ESE Manuel Castro Tovar y las emitidas por los entes de control.

No se permite la descarga, uso, intercambio o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información o productos que atenten contra la propiedad intelectual, archivos ejecutables que comprometan la seguridad de la información, herramientas de hacking, entre otros.

4.1.7 POLÍTICA DE USO DE REDES SOCIALES

Objetivo: Definir los lineamientos generales para el uso del servicio de Redes sociales por parte de los usuarios autorizados en la ESE Manuel Castro Tovar.

Usos aceptables del servicio

El personal autorizado para hacer uso de las Redes Sociales en La ESE Manuel Castro Tovar es el personal de comunicaciones.

Los usuarios autorizados para hacer uso de los servicios de Redes Sociales son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información de la ESE Manuel Castro Tovar.

El servicio autorizado debe ser utilizado exclusivamente para el desarrollo de las actividades relacionadas con la ESE Manuel Castro Tovar.

Es permitido el uso de redes sociales utilizando video conferencia y streaming (descarga de audio y video), siempre y cuando no interfiera o altere la operación normal de los sistemas de información de la Entidad.

La ESE Manuel Castro Tovar facilita el acceso a estas herramientas, teniendo en cuenta que constituyen un complemento de varias actividades que se realizan por estos medio y para el desempeño de las funciones y actividades a desempeñar por parte de Funcionarios, Colaboradores y Terceros, sin embargo es necesario hacer buen uso de estas herramientas de forma correcta y moderada.

No se deben descargar programas ejecutables o archivos que puedan contener software o código malicioso.

No se permiten descargas, distribución de material obsceno y no autorizado, degradante, terrorista, abusivo o calumniante a través del servicio de Redes Sociales.

No se debe practicar e intentar acceder de forma no autorizada a los sistemas de seguridad del servicio de Internet de la ESE Manuel Castro Tovar, o aprovechar el acceso a Redes Sociales para fines ilegales.

Es claro que no se puede difundir cualquier tipo de virus o software de propósito destructivo o malintencionado.

Todos los Funcionarios, Colaboradores y Terceros de la ESE Manuel Castro Tovar, deben seguir los procedimientos y planes de comunicaciones interna y externa.

4.1.8 POLÍTICA DE USO DE RECURSOS TECNOLÓGICOS

Objetivo: Definir los lineamientos generales para el uso aceptable de los recursos tecnológicos de la ESE Manuel Castro Tovar

Usos aceptables del servicio

La ESE Manuel Castro Tovar asigna los recursos tecnológicos necesarios como herramientas de trabajo para el desempeño de las funciones y actividades laborales de los Funcionarios, Colaboradores y terceros de ser necesario.

El uso adecuado de estos recursos se establece bajo los siguientes criterios:

La instalación de software se encuentra bajo la responsabilidad la Oficina de Gestión de las Tecnologías y por tanto son los únicos autorizados para realizar esta actividad.

Ningún usuario debe realizar cambios relacionados con la configuración de los equipos, como conexiones de red, usuarios locales de la máquina, fondo de escritorio y protector de pantalla corporativo. Estos cambios únicamente deben ser realizados por la Oficina de Gestión de las Tecnologías previa actualización de la carpeta ISO realizada por el proceso de Mejora Continua.

La Oficina de Gestión de las Tecnologías es el responsable de instalar las aplicaciones autorizadas que se encuentran permitidas en la ESE Manuel Castro Tovar para ser instaladas en las estaciones de trabajo de los usuarios.

Sólo el personal autorizado por la Oficina de Gestión de las Tecnologías podrá realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de la ESE Manuel Castro Tovar.

Los Funcionarios, Colaboradores y Terceros de la Entidad son responsables de hacer buen uso de los recursos tecnológicos de la ESE Manuel Castro Tovar y en ningún momento pueden ser usados para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra otros

Funcionarios, Colaboradores y Terceros, legislación vigente y políticas y lineamientos de seguridad de la información establecidas por la ESE Manuel Castro Tovar.

Todo activo de propiedad de la ESE Manuel Castro Tovar, asignado a Funcionarios, Colaboradores y Terceros de la ESE Manuel Castro Tovar, debe ser entregado al finalizar el vínculo laboral o contractual o por cambio de cargo si es necesario. Esto incluye los documentos corporativos, equipos de cómputo (Hardware y Software), dispositivos móviles, manuales y la información que tenga almacenada en dispositivos móviles o removibles.

Borrado seguro

Todo medio de almacenamiento que tenga información de la ESE Manuel Castro Tovar, que salga de la entidad y que no vaya a tener más uso en la institución, deberá ser formateado por el personal de Gestión de las Tecnologías, previo respaldo de ser necesario.

Trasferencia de medios físicos

El transporte de los medios físicos, se debe hacer mediante un medio de transporte confiable y seguro, tomando las medidas y precauciones necesarias para garantizar que los medios de almacenamiento sean transportados adecuadamente, de esta forma se evitar una afectación a la integridad y disponibilidad.

Se debe llevar un registro o cadena de custodia de los medios de almacenamiento físico que son transportados.

4.1.9 POLÍTICA DE CONTROL DE ACCESO

Objetivo: Definir las directrices generales para un acceso controlado a la información de la ESE Manuel Castro Tovar.

Control de Acceso a Redes y Servicios en Red

El proceso Gestión de las Tecnologías otorgará a los usuarios una contraseña de acceso al Sistema de Información institucional (Dinámica Gerencial Hospitalaria) y al Chat institucional (Spark), el usuario podrá posteriormente y de forma opcional cambiar esta contraseña.

Las claves son de uso personal e intransferible y es responsabilidad del usuario el uso de las credenciales asignadas.

Sólo el personal designado por la Oficina de Gestión de las Tecnologías está autorizado para instalar software o hardware en los equipos, servidores e infraestructura de tecnología de la ESE Manuel Castro Tovar.

Todo actividad que requiera acceder a los servidores, equipos o a las redes de la ESE Manuel Castro Tovar, se debe realizar en las instalaciones. No se debe realizar ninguna actividad de tipo remoto sin la debida autorización la Oficina de Gestión de las Tecnologías.

La creación y retiro de usuarios en los sistemas de información en producción debe seguir un procedimiento de Creación, Edición y Eliminación de Usuarios.

Gestión de Acceso a Usuarios

Se establece el uso de contraseñas individuales para determinar las responsabilidades de su administración.

Los usuarios pueden elegir y cambiar sus claves de acceso periódicamente, inclusive antes de que la cuenta expire.

Todos los usuarios deben dar buen uso a las claves de acceso suministradas y no deben escribirlas o dejarlas a la vista.

No prestar, divulgar o difundir la contraseña de acceso asignadas a compañeros, Jefes u otras personas que lo soliciten.

Las contraseñas no deben ser reveladas por vía telefónica, correo electrónico o por ningún otro medio.

Reportar a la Oficina de Gestión de las Tecnologías sobre cualquier incidente o sospecha de que otra persona esté utilizando su contraseña o usuario asignado.

Reportar a la Oficina de Gestión de las Tecnologías sobre cualquier sospecha o evidencia de que una persona esté utilizando una contraseña y usuario que no le pertenece.

El acceso a Bases de Datos, Servidores y demás componentes tecnológicos de administración de la Plataforma y Sistemas de Información, debe estar autorizado por la Oficina de Gestión de las Tecnologías.

Retiro de los derechos de acceso

Cada uno de los procesos de la Entidad es responsable de comunicar a la Oficina de Talento Humano y Contratación, el cambio de cargo, funciones o actividades o la terminación contractual de los Colaboradores pertenecientes al proceso. La Oficina de Talento Humano y Contratación son las encargadas de comunicar a la Oficina de Gestión de las Tecnologías sobre estas novedades, con el fin de retirar los derechos de acceso a los servicios informáticos y de procesamiento de información.

4.1.10 POLÍTICA SEGURIDAD FÍSICA Y DEL ENTORNO

Objetivo: Evitar accesos físicos no autorizados a las instalaciones de procesamiento de información, que atenten contra la confidencialidad, integridad o disponibilidad de la información de la ESE Manuel Castro Tovar.

Perímetro de Seguridad Física

En la oficina de Gestión de las Tecnologías, deberá permanecer al menos un funcionario del área, de lo contrario, permanecerá a puerta cerrada.

Los visitantes deben permanecer acompañados de un Funcionarios o Colaborador de la ESE Manuel Castro Tovar, cuando se encuentren en las oficinas o áreas donde se maneje información.

Es responsabilidad de todos los Funcionarios, Colaboradores y Terceros de la ESE Manuel Castro Tovar borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo. Igualmente, no se debe dejar documentos o notas escritas sobre las mesas al finalizar las reuniones.

Los visitantes que requieran permanecer en las oficinas de la ESE Manuel Castro Tovar por periodos superiores a dos (2) días deben ser presentados al personal de oficina donde permanecerán.

El horario autorizado para recibir visitantes en las instalaciones de la ESE Manuel Castro Tovar es de 7:00 AM a 12:00 PM. Y de 2:00 PM A 6:00PM. En horarios distintos se requerirá de la autorización del Gerencia y/o subdirección Administrativa y Técnico-Científica.

Los dispositivos removibles, así como toda información CONFIDENCIAL de la ESE Manuel Castro Tovar, independientemente del medio en que se encuentre, deben permanecer guardados bajo seguridad durante horario no hábil o en horarios en los cuales el Funcionarios, Colaboradores o Terceros responsable no se encuentre en su sitio de trabajo.

Las instalaciones de la ESE Manuel Castro Tovar deben estar dotadas de un circuito cerrado de TV con el fin de monitorear y registrar las actividades de Funcionarios, Colaboradores y Terceros y visitantes.

Controles de Acceso Físico

Las áreas seguras, dentro de las cuales se encuentran el Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, deben contar con mecanismos de protección física, y controles de acceso adecuados para la protección de la información.

En las áreas seguras, bajo ninguna circunstancia se puede fumar, comer o beber.

Las actividades de limpieza en las áreas seguras deben ser controladas y supervisadas por un Funcionarios o Colaboradores del proceso.

Ubicación y Protección de los equipos.

La plataforma tecnológica (Hardware, software y comunicaciones) debe contar con las medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.

Se debe instalar sistemas de protección eléctrica en el centro de cómputo de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Así mismo, se debe proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.

Seguridad de los equipos fuera de las instalaciones

No se debe cargar información CONFIDENCIAL o RESERVADA en los equipos portátiles de la institución a menos que sea por orden expresa de la gerencia o alguna de las subdirecciones.

Los equipos portátiles no deben estar a la vista en el interior de los vehículos. En casos de viaje siempre se debe llevar como equipaje de mano.

En caso de pérdida o robo de un equipo portátil se debe informar inmediatamente a la Subdirección Administrativa y la Oficina de Gestión de las Tecnologías y debe poner la denuncia ante las autoridades competentes y debe hacer llegar copia de la misma.

Para el caso de los equipos que cuentan con puertos de transmisión y recepción de infrarrojo y Bluetooth estos deben estar deshabilitados.

Todos los equipos de cómputo deben ser registrados al ingreso y al retirarse de las instalaciones de la ESE Manuel Castro Tovar.

Retiro de Activos

Ningún equipo de cómputo, información o software debe ser retirado de la ESE Manuel Castro Tovar sin una autorización formal.

Se debe realizar periódicamente comprobaciones puntuales para detectar el retiro no autorizado de activos de la ESE Manuel Castro Tovar.

4.1.11 POLÍTICA DE PROTECCIÓN CONTRA CÓDIGO MALICIOSO

Objetivo: Definir las medidas de prevención, detección y corrección frente a las amenazas causadas por códigos maliciosos en la ESE Manuel Castro Tovar.

Toda la infraestructura de procesamiento de información de la ESE Manuel Castro Tovar, cuenta con un sistema de detección y prevención de intrusos, herramienta de Anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos.

Se debe restringir la ejecución de aplicaciones y mantener instalado y actualizado el antivirus, en todas las estaciones de trabajo y servidores de la ESE Manuel Castro Tovar.

Todos los Funcionarios, Colaboradores y Terceros que hacen uso de los servicios de tecnología de la información y comunicaciones de la ESE Manuel Castro Tovar son responsables del manejo del antivirus para analizar, verificar y (si es posible) eliminar virus o código malicioso de la red, el

computador, los dispositivos de almacenamiento fijos, removibles, archivos, correo electrónico que estén utilizando para el desempeño de sus funciones laborales.

La ESE Manuel Castro Tovar cuenta con el software necesario como antivirus para protección a nivel de estaciones de trabajo, contra virus y código malicioso, el servicio es administrado por la Oficina de Gestión de las Tecnologías.

Los antivirus adquirido por la ESE Manuel Castro Tovar, sólo debe ser instalados por los responsables de la Oficina de Gestión de las Tecnologías.

Los equipos de terceros que son autorizados para conectarse a la red de datos de la ESE Manuel Castro Tovar deben tener antivirus y contar con las medidas de seguridad apropiadas.

Se debe mantener actualizado a sus últimas versiones funcionales las herramientas de seguridad, incluido, motores de detección, bases de datos de firmas.

Se debe hacer revisiones y análisis periódicos del uso de software no malicioso en las estaciones de trabajo y servidores. Durante la realización de los mantenimientos correctivos y preventivos.

Se deben hacer campañas de sensibilización a todos los Funcionarios, Colaboradores y Terceros de ser el caso de la ESE Manuel Castro Tovar, con el fin de generar una cultura de seguridad de la información entre los Funcionarios, Colaboradores y Terceros de la ESE Manuel Castro Tovar.

Los Funcionarios, Colaboradores y Terceros de la ESE Manuel Castro Tovar pueden iniciar en cualquier momento un análisis bajo demanda de cualquier archivo o repositorio que consideren sospechoso de contener software malicioso. En cualquier caso, los Funcionarios, Colaboradores y Terceros cuando sea necesario siempre podrán consultar a la Oficina de Gestión de las Tecnologías sobre el tratamiento que debe darse en caso de sospecha de malware.

Los usuarios no podrán desactivar o eliminar la suite de productos de seguridad, incluidos los programas antivirus o de detección de código malicioso, en los equipos o sistemas asignados para el desempeño de sus funciones laborales.

Todo usuario es responsable por la destrucción de archivos o mensajes, que le haya sido enviado por cualquier medio provisto por la ESE Manuel Castro Tovar, cuyo origen le sea desconocido o sospechoso y asume la responsabilidad de las consecuencias que puede ocasionar su apertura o ejecución. En estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos, el usuario debe reenviar el correo a la cuenta sistemas@esemanuelcastrotovar.com

El único servicio de antivirus autorizado en la ESE Manuel Castro Tovar es el asignado directamente por la Oficina de Gestión de las Tecnologías, el cual cumple con todos los requerimientos técnicos y de

seguridad necesarios para evitar ataques de virus, spyware y otro tipo de software malicioso. Además este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura. Excepcionalmente se podrá realizar la ejecución de otro programa antivirus, únicamente por personal autorizado por la Oficina de Gestión de las Tecnologías, a efectos de reforzar el control de presencia o programación de virus o código malicioso.

La Oficina de Gestión de las Tecnologías es la responsable de administrar la plataforma tecnológica que soporta el servicio de Antivirus para los equipos de cómputo conectados a la red de la ESE Manuel Castro Tovar.

La Oficina de Gestión de las Tecnologías se reserva el derecho de monitorear las comunicaciones y/o la información que se generen, comuniquen, transmitan o trasporten y almacenen en cualquier medio, en busca de virus o código malicioso.

La Oficina de Gestión de las Tecnologías se reserva el derecho de filtrar los contenidos que se trasmitan en la red de la ESE Manuel Castro Tovar, con el fin de evitar amenazas de virus.

Todos los correos electrónicos serán revisados para evitar que tengan virus. Si el virus no puede ser eliminado, la información será borrada.

4.1.12 POLÍTICA DE BACKUP

Objetivo: Proporcionar medios de respaldo de información adecuados en la ESE Manuel Castro Tovar para asegurar la información crítica y que el software asociado se pueda recuperar después de una falla.

El proceso de Gestión de las Tecnologías, realizará copias del Sistema de Información Institucional, de acuerdo al procedimiento registrado en la última versión de la carpeta SISTEMA DE GESTIÓN DE CALIDAD.

Los usuarios que requieran respaldo de los archivos ubicados en el equipo que le ha sido asignado para sus labores, deben solicitarlo formalmente a la oficina Gestión de las Tecnologías.

Se debe tener en cuenta los lineamientos de la ley 594 de 2000 o cualquiera que la modifique, adicione o derogue.

Respaldo de Información para Usuarios Finales

La Oficina de Gestión de las Tecnologías, debe mantener los respaldos de información en condiciones adecuadas de medio ambiente, temperatura, humedad, y otros.

Ningún usuario puede realizar copias de respaldo en sus dispositivos de almacenamiento removibles personales, ya que esto puede ser denominado como fuga de información.

Todos los Funcionarios, Colaboradores y Terceros de la ESE Manuel Castro Tovar deben dar estricto cumplimiento a esta política y el que haga caso omiso puede ser sujeto a acciones disciplinarias o civiles, incluyendo la terminación del respectivo contrato.

4.1.13 POLÍTICA DE GESTIÓN DE SEGURIDAD DE LAS REDES

Objetivo: Establecer los controles necesarios para proteger la información de la ESE Manuel Castro Tovar transportada desde la red interna.

La Oficina de Gestión de las Tecnologías es la responsable de administrar y gestionar la red de la ESE Manuel Castro Tovar.

La Oficina de Gestión de las Tecnologías es la responsable de establecer los controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de mantener los niveles de seguridad apropiados.

La ESE Manuel Castro Tovar proporciona a los Funcionarios, Colaboradores y Terceros todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones y actividades laborales, por lo cual no es permitido conectar a las estaciones de trabajo o a los puntos de acceso de la red corporativa, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por la Oficina de Gestión de las Tecnologías.

Separación de las Redes

La ESE Manuel Castro Tovar debe establecer un esquema de segregación de redes, con el fin de controlar el acceso a los diferentes segmentos de red y garantizar la confidencialidad, integridad y disponibilidad de la información.

Se deben seguir los procedimientos de acceso o retiro de componentes tecnológicos para la solicitud de servicios de red.

Se deben establecer parámetros técnicos para la conexión segura de la red con los servicios de red.

4.1.14 POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Objetivo: Gestionar todos los incidentes de seguridad de la información reportados en la ESE Manuel Castro Tovar, adecuadamente, dando cumplimiento a los procedimientos establecidos.

Reporte sobre los eventos y las debilidades de la seguridad de la información

Todos los Funcionarios, Colaboradores y Terceros de la ESE Manuel Castro Tovar y terceras partes tienen la responsabilidad de reportar de forma inmediata los eventos, incidentes o debilidades en cuanto a la seguridad de la información que identifiquen o se presenten.

Se debe dar un tratamiento adecuado a todos los incidentes de seguridad de la información reportados.

Se deben establecer las responsabilidades en la Gestión de Incidentes de Seguridad de la Información.

Se debe recolectar las evidencias (CCP, Fiscalía, colcert, mintic) necesarias lo más pronto posible después del reporte del incidente.

Escalar los incidentes a niveles superiores en caso de que sea requerido.

Se debe hacer evaluaciones de los incidentes presentados ya que se puede necesitar de controles adicionales.

Para el transporte de elementos, se debe llevar la cadena de custodia. Se deben documentar todos los incidentes de seguridad reportados.

Se debe realizar sensibilización a todos los usuarios sobre incidentes de seguridad de la información.

4.1.15 POLÍTICA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Objetivo: Garantizar que los planes de continuidad de negocios se ejecuten de forma segura sin exponer la información de la ESE Manuel Castro Tovar.

La ESE Manuel Castro Tovar debe establecer los requisitos necesarios de seguridad de la información y la continuidad de la operación en caso de situaciones adversas, como desastres naturales o crisis.

Se debe contar con un Servidor alterno con todas las configuraciones predeterminadas para el funcionamiento del Sistema de Información Institucional en caso de falla del Servidor Principal.

5 BIBLIOGRAFIA

Departamento Administrativo de la Función Pública, Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano.

Modelo de seguridad y privacidad de la información emitido por MINTC Guías del modelo de seguridad y privacidad

Departamento Administrativo de la Función Pública, Guía para la administración del riesgo.

Departamento Administrativo de la Función Pública, Norma Técnica de Calidad en la Gestión Pública NTCGP 1000:2009.

Departamento Administrativo de la Función Pública, Planeación de los Recursos Humanos-Lineamientos de política, estrategias y orientaciones para la implementación.

Presidencia de la República - Secretaría de Transparencia, Documento "Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano.

CONTROL DE CAMBIOS

VERSIÓN	APROBACIÓN	DESCRIPCIÓN DEL CAMBIO
01		Versión inicial implementación SGC