POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

EMPRESA SOCIAL DEL ESTADO BARRANCABERMEJA

	NOMBRE	***CARGO***	***FIRMA***
Elaboró	*Claudia Patricia Gómez Romero*	*Profesional Especializado apoyo a la subdirección administrativa y financiera -Contratista ESEB*	
Revisó	*Alexander Alvarado Paternina*	*Jefe Oficina Asesora Planeación*	
Aprobó	*Esmeralda María Otero Alvarez*	*Gerente*	

TABLA DE CONTENIDO

1. INTRODUCCIÓN

En las organizaciones las políticas de seguridad informática surgen como una herramienta organizacional de ayuda para que las personas comprendan la importancia de seguir las reglas y de los beneficios al tomar medidas que ayuden a incrementar la seguridad de sus datos. Estas reglas se tienen que cumplir por todo el personal relacionado con la empresa. Así se asegura la integridad, disponibilidad y privacidad de las infraestructuras informáticas y de la información.

Una política de Seguridad es una declaración escrita de cómo una organización protege sus activos de IT. Y su propósito es mantener a todos los miembros de la organización trabajando hacia un objetivo común, a medida que las amenazas de Seguridad evolucionan y el negocio cambia.

LA ESE BARRANCABERMEJA así como otras organizaciones gubernamentales y no gubernamentales, desarrolla políticas de seguridad que rigen el uso adecuado de la tecnología y hacen recomendaciones para aprovechar sus ventajas y evitar su uso indebido; previendo así problemas en el uso de los bienes y servicios informáticos.

2. JUSTIFICACIÓN

Es sabido que las empresas de nuestro país han sido blanco de ataques por hackers, incluso algunas ya se han visto afectadas por problemas de virus, caída de servidores y pérdida de valiosa información; las amenazas están en todo tipo de entidades, y pueden ser externas o internas, entre ellas tenemos: Uso indiscriminado de la Internet, mala práctica de los usuarios, descuido en la manipulación de los equipos y el desconocimiento de conceptos básicos de manejo de dispositivos informáticos.

Los computadores y toda la información contenida en ellos puede ser blanco de delincuentes cibernéticos por medio de virus informáticos software espía y demás, con los que buscan alterar el funcionamiento del dispositivo y así extraer, dañar o borrar datos. Es por eso, que la política de seguridad de la información cumple un papel determinante en la protección de las redes, los datos y los equipos de una Institución.

Basados en esta realidad y a los antecedentes presentados de equipos infectados que generaron pérdida de información por virus y mala manipulación de la información, y así tratar que la información institucional que es uno de los activos principales quede menos expuesta y en aras de prevenir futuros eventos, se crea la necesidad de implementar medidas de seguridad y protección sean cada vez más eficientes la oficina de Sistemas de Información de la Empresa Social del Estado Barrancabermeja decide elaborar un Manual de Políticas de Seguridad que incluyan medidas preventivas realizando una mejora continua,

para proteger la información y almacenarla desde que se crea hasta que se destruye, evitando de esta forma la fuga de información, robo o manipulación.

3. OBJETIVO GENERAL

Plantear Políticas de Seguridad Informática para la ESE Barrancabermeja, que ayuden a formar una cultura organizacional de buenas prácticas de seguridad informática y fortalecer la seguridad física y lógica de los activos informáticos de la entidad.

3.1 OBJETIVOS ESPECIFICOS

- Establecer normas de cuidado de equipos, periféricos y demás dispositivos físicos.
- Lograr que todos los usuarios de la ESE Barrancabermeja tomen conciencia acerca de la necesidad de la adopción de las políticas de seguridad de la información establecidas.
- Reducir el riesgo de pérdida, robo o corrupción de información al igual que riesgo de pérdida de confidencialidad, integridad y disponibilidad de los activos de información.
- Crear mecanismos de protección a partir de las normas básicas a la hora de utilizar los recursos de red tales como internet o la red Local.
- Definir las responsabilidades relacionadas con el manejo de la seguridad de la información.
- Reglamentar y controlar la instalación de todo tipo de software, entre todos los funcionarios y contratistas de la ESE Barrancabermeja.

- Implementar, documentar y Comunicar la estrategia de seguridad de la información las políticas de seguridad, creadas para la ESE Barrancabermeja.

4. GLOSARIO

Activo: Conjunto de bienes y derechos tangibles e intangibles de propiedad de una persona natural o jurídica que por lo general son generadores de renta o fuente de beneficios, en el ambiente informático llámese activo a los bienes de información y procesamiento, que posee la institución. Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Administración Remota: Forma de administrar (manejar o controlar) equipos informáticos o servicios físicamente separados.

Algoritmo: Conjunto de instrucciones sistemáticas y previamente definidas que se utilizan para realizar una determinada tarea. Estas instrucciones están ordenadas y acotadas a manera de pasos a seguir para alcanzar un objetivo.

Amenaza: Evento que puede desencadenar un incidente en la institución, produciendo daños materiales o pérdidas inmateriales en sus activos.

Antivirus: Son una herramienta simple cuyo objetivo es detectar y eliminar virus informáticos.

Área Crítica: Área física donde se encuentra instalado el equipo de cómputo y telecomunicaciones que requiere de cuidados especiales y son indispensables para el funcionamiento continuo de los sistemas de comunicación de la ESE BARRANCABERMEJA.

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Bases de Datos: Conjunto de datos interrelacionados y de programas para accederlos. Una recopilación de datos estructurados y organizados de una manera disciplinada para que el acceso a la información de interés sea rápido.

Cadena: Mensaje que intenta inducir al receptor a realizar algún número de copias de un mensaje de correo para luego pasarlas a uno o más receptores nuevos.

CD (Disco compacto): Soporte digital óptico utilizado para almacenar cualquier tipo de información (audio, imágenes, vídeo, documentos y otros datos).

Chat: Comunicación en tiempo real que se realiza entre varios usuarios cuyas computadoras están conectadas a una red, generalmente Internet; los usuarios escriben mensajes en su teclado, y el texto aparece automáticamente y al instante en el monitor de todos los participantes.

Ciclo de Vida de Sistemas de información: Se refiere al proceso de planificación, creación, pruebas y despliegue en un sistema de información.

COLCERT: Es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, un equipo que es punto de contacto para coordinar la prevención, mitigación, gestión y respuesta ante incidentes de seguridad digital nacional tanto en el sector público como en el privado.

Confidencialidad: Proteger la información de su revelación no autorizada. Esto significa que la información debe estar protegida de ser copiada por cualquiera que no esté explícitamente autorizado por el propietario de dicha información.

Control de Acceso: Técnica usada para definir el uso de programas o limitar la obtención y almacenamiento de datos a una memoria. Característica o técnica en

un sistema de comunicaciones que permite o niega el uso de algunos componentes o algunas de sus funciones.

Crack: Programa que realiza una modificación permanente o temporal sobre otro en su código, para obviar una limitación o candado impuesto a propósito por el programador original. Algunas legislaciones consideran este tipo de programas ilegales por facilitar la vulneración de los derechos de autor de códigos no libres o comerciales.

CSIRT: (Computer Security Incident Response Team) es un equipo de respuesta a incidentes de seguridad informática. Esta unidad tiene como objetivo recibir, revisar y responder a informes de incidentes. Monitoreo de las plataformas de internet de organismos públicos las 24 horas, todos los días de la semana.

Dirección IP: Es una etiqueta numérica que identifica, de manera lógica y jerárquica, una interface de conexión de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol).

DVD (Disco Versátil Digital): Dispositivo de almacenamiento óptico en forma de disco, similar al CD, pero de mayor capacidad de almacenamiento (4.7 GB).

Equipo de Cómputo: Dispositivo con la capacidad de aceptar y procesar información, teniendo la oportunidad de conectarse a una red de equipos o computadoras para compartir datos y recursos, entregando resultados mediante despliegues visuales, impresos o audibles.

Equipo de Telecomunicaciones: Todo dispositivo capaz de transmitir y/o recibir señales digitales o analógicas para comunicación de voz, datos y video, ya sea individualmente o de forma conjunta.

Estabilizador: Dispositivo para la toma de la tensión de la red eléctrica que alimenta al computador y a la red.

Filtro de contenidos web: Herramienta informática que bloquea o permite el acceso a determinados sitios de internet.

FTP (File Transfer Protocol): Protocolo y software que permite la transferencia de archivos entre máquinas conectadas a una red.

Hacking: Acción de infiltrarse ilegalmente a sistemas informáticos y redes de telecomunicación con fines delictivos.

Hardware: Partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos, sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

Integridad: Proteger la información de alteraciones no autorizadas por la institución.

Internet: Red de redes de computadoras conectadas a nivel mundial, se emplea para el intercambio de información, el acceso a bases de datos, entre otros fines.

ISO/IEC 27001: La norma ISO 27001 es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información. La norma proporciona un marco para la seguridad de la información que ayuda a las organizaciones a identificar y gestionar sus riesgos de seguridad de la información de manera efectiva.

Keygen: Programa informático, generalmente ilegal, que al ejecutarse genera un código para que un determinado programa software de pago en su versión de prueba pueda ofrecer los contenidos completos del mismo.

Logs: En el sector IT hacen referencia a los archivos de texto en los que se incluyen de forma cronológica los acontecimientos como cambios, actualizaciones y demás que han ocurrido dentro de un sistema informático, como puede ser un

servidor, una aplicación o un programa, así como la serie de modificaciones que estos han generado.

Mantenimiento: Acciones que tienen como objetivo mantener un artículo o restaurarlo a un estado original.

Memoria USB: Dispositivo de almacenamiento masivo que utiliza memoria flash para guardar la información que se puede requerir.

Módulo: Parte de un programa de computador.

Online: Que está disponible o se realiza a través de internet o de otra red de datos.

Outsourcing: Es un término en inglés que se utiliza para representar el acto de tercerizar servicios, llevado a cabo por una empresa para reducir la carga de trabajos hechos internamente y escalar el alcance y la productividad del negocio.

Periférico: Dispositivos externos que se conectan al computador.

Red: Conjunto de computadoras y elementos interconectados que permiten una comunicación entre sí y forman parte de un mismo ambiente.

Servicio: Conjunto de aplicativos, programas informáticos o sitios web que apoyan la labor administrativa de la institución, sobre los procesos diarios que demanden información o comunicación en la misma.

Servidor: Es un aparato informático que almacena, distribuye y suministra información. Los servidores funcionan basándose en el modelo “cliente-servidor”. El cliente puede ser tanto un ordenador como una aplicación que requiere información del servidor para funcionar. Por tanto, un servidor ofrecerá la información demandada por el cliente siempre y cuando el cliente esté autorizado. Los servidores pueden ser físicos o virtuales.

Software: Conjunto de componentes lógicos necesarios que hacen posible la realización de tareas específicas.

Software espía: Controla el uso de la computadora sin el conocimiento o consentimiento del usuario. Los software espía pueden grabar la secuencia de pulsación de teclas, el historial de navegación, contraseñas y cualquier otra información confidencial y privada, y enviar estos datos a un tercero vía Internet.

Soporte Técnico: Personal designado o encargado de velar por el correcto funcionamiento de las estaciones de trabajo, servidores o equipo de oficina dentro de la institución.

SPAM: Mensajes no solicitados, no deseados o de remitente no conocido.

UPS (Uninterrupted Power System): Sistema de Potencia Ininterrumpida, es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados.

Usuario: Cualquier personal, que utilice los servicios informáticos de la red institucional y tenga algún tipo de vinculación con la ESE Barrancabermeja.

Virus Informático: Programa software que altera el normal funcionamiento del computador, sin el permiso o el conocimiento del usuario.

Vulnerabilidad: Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La dirección de EMPRESA SOCIAL DEL ESTADO BARRANCABERMEJA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para la dirección de EMPRESA SOCIAL DEL ESTADO BARRANCABERMEJA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de La EMPRESA SOCIAL DEL ESTADO BARRANCABERMEJA.
- Garantizar la continuidad del negocio frente a incidentes.

La EMPRESA SOCIAL DEL ESTADO BARRANCABERMEJA ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Con el objetivo de hacer una implementación transversal de Seguridad de la Información en la Entidad, se tomaron en cuenta la información definidas en la norma ISO/IEC 27001, para definir los procedimientos de seguridad necesarios tales como: .la gestión de activos, seguridad física y ambiental, control de accesos, etc.

A continuación se establecen principios de seguridad

- En La Empresa Social del Estado Barrancabermeja las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.

- La Empresa Social del Estado Barrancabermeja protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de Control de Acceso otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- La Empresa Social del Estado Barrancabermeja protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La Empresa Social del Estado Barrancabermeja protegerá su información de las amenazas originadas por parte del personal.
- La Empresa Social del Estado Barrancabermeja protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La Empresa Social del Estado Barrancabermeja controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La Empresa Social del Estado Barrancabermeja implementará control de acceso a la información, sistemas y recursos de red.
- La Empresa Social del Estado Barrancabermeja garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- La Empresa Social del Estado Barrancabermeja garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La Empresa Social del Estado Barrancabermeja garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La Empresa Social del Estado Barrancabermeja garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

6. ALCANCE

Esta Política aplica a todo el personal de la ESE BARRANCABERMEJA y a todos los funcionarios, contratistas, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, y demás que se conecten a la red de la institución o accedan a cualquier tipo de información y suministra los lineamientos para el correcto uso de las herramientas informáticas de la entidad.

6.2 NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

6.3 FASES DE IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Para realizar una correcta implementación de políticas de seguridad de la información, la Empresa Social del Estado Barrancabermeja decide cumplir con una las fases que se sugieren en la guía No. 2 Elaboración de la política general de seguridad y privacidad de la información, las cuales tienen como objetivo que la entidad desarrolle, apruebe, implemente y socialice e interiorice las políticas para un uso efectivo por parte de todos los funcionarios, contratistas y/o terceros de la entidad.

6.3.1 Desarrollo de las políticas: La Empresa Social del Estado Barrancabermeja responsabilizar al área de Sistemas para la creación de las políticas, estructurarlas, escribirlas, revisarlas y aprobarlas por el Comité de Gestión y Desempeño; para lo cual se requiere que se realicen actividades de verificación e investigación de los siguientes aspectos:

6.3.2 Justificación de la creación de política: La Empresa Social del Estado Barrancabermeja dada su naturaleza requiere proteger su información institucional que es uno de los activos principales es así que la oficina de Sistemas elabora un Manual de Políticas de Seguridad que incluyan medidas preventivas realizando una mejora continua.

Para el desarrollo de esta política se determinó su alcance, roles y responsabilidades, revisión de la política, aprobación de la Política mediante la firma y publicación de las mismas todo con el apoyo de la Alta Gerencia de la Entidad para su implementación.

6.3.3 Cumplimiento: Una vez que se escriban las políticas, aprueben y publiquen, en esta fase deben ser implementadas y relacionadas a los controles de seguridad de la Información, esto con el fin de que exista consistencia entre lo escrito en las políticas versus los controles de seguridad implementados y documentados.

6.3.4 Comunicación: Aquí se da a conocer las políticas a los funcionarios, contratistas y/o terceros de la Entidad, esto a través de información verbal o escrita en las reuniones o correos electrónicos que se envíen y en la sede electrónica de la entidad. Todos los usuarios de sistema deben tener el conocimiento del contenido de las políticas para que se les dé el correcto cumplimiento de las mismas; esta fase de la implementación también permitirá obtener retroalimentación de la efectividad de las políticas, permitiendo así realizar excepciones, correcciones y ajustes pertinentes.

6.3.5 Monitoreo: Las políticas sean monitoreadas para determinar la efectividad y cumplimiento de las mismas, esto se realizará mediante indicadores o registro de casos para verificar de forma periódica y con evidencias que la política funciona y si debe o no ajustarse.

6.3.6 Mantenimiento: La política se actualizará con base a los hallazgos encontrados en la fase de monitoreo.

6.3.7 Retiro: En el caso que se haga necesario la eliminación de una política de seguridad en cuanto esta ha cumplido su finalidad o la política ya no es necesaria en la Entidad esto será documentado con el objetivo de tener referencias y antecedentes sobre el tema.

7. POLITICAS ESPECÍFICAS PARA CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Dentro de la organización de la seguridad de la información la Empresa Social del Estado Barrancabermeja estará inmerso en el Comité de Gestión y Desempeño. Cuyo objetivo dentro del comité será el mejoramiento continuo de los programas o las distintas actividades que se realizarán en dicho comité, verificación de avance de los distintos proyectos, la revisión del documento de la política de seguridad entre otros.

7.1 CONTROL DE ACCESO:

El recurso Humano para La ENTIDAD lo constituyen las personas que utilizan la estructura tecnológica de la Institución, ya sean equipos, recursos de red o gestión de la información. Para asegurar la seguridad de la información la oficina de Sistemas de Información establece normas que buscan reducir los riesgos tales como establecimiento de normas que incluyen, restricciones, autorizaciones, denegaciones, perfiles de usuario, y todo lo necesario que permita un buen nivel de seguridad informática.

Las políticas de seguridad de la información deben ser cumplidas por todos los funcionarios, contratistas, colaboradores, proveedores y personal de empresas que provean personal a la ESE BARRANCABERMEJA, para ello durante el proceso de vinculación deberán recibir inducción sobre lo establecido en este Documento y sobre la responsabilidad del cumplimiento de las políticas, procedimientos y estándares definidos.

Se deja claridad que la información contenida en los equipos de cómputo de la institución es propiedad de la ESE BARRANCABERMEJA y cada usuario es responsable por proteger su integridad, confidencialidad y disponibilidad tomando en cuenta que muchos de los datos contenidos en estos equipos o en las bases de datos son de carácter sensible por lo que no es permitido divulgar, alterar, borrar, eliminar información sin la debida autorización.

Los equipos propiedad de la Empresa Social del Estado Barrancabermeja deben usarse solamente para las actividades propias, por lo tanto, los usuarios no deben usarlos para asuntos personales. (Delito contra los bienes de la administración pública).

Los usuarios de los sistemas de la institución se les asignarán Las claves o los permisos de acceso necesarios para el cumplimiento de sus funciones y es responsabilidad exclusiva de cada uno de ellos dar el buen uso a estas y no deben compartirlas con otras personas, excepto cuando los funcionarios de Sistemas la soliciten para la reparación o el mantenimiento de algún servicio o equipo, éstos usuarios y contraseñas serán creados por solicitud de la oficina de recurso humano o de la coordinación de las empresas tercerizadoras quienes suministraran los datos en formato establecido para su correspondiente creación, así mismo en el momento de retiro o movimientos del personal también se debe informar a la oficina de sistemas para realizar los cambios.

Los usuarios deben renovar su clave de acceso cuando el sistema lo solicite o por temas de seguridad ya que tenga indicios de que ha sido conocida, aspectos como el desbloqueo de usuario o cambios de contraseñas deben solicitarlo a la oficina de Sistemas de Información quienes le facilitarán el acceso y lo acompañarán en el proceso. Está totalmente prohibido: El intento o violación de los controles de seguridad establecidos; El uso sin autorización de los activos informáticos;

El uso no autorizado de la conexión al Sistema; el uso indebido de las contraseñas, firmas digitales, o dispositivos de autenticación e identificación; acceder a servicios informáticos utilizando cuentas, claves, contraseñas de otros usuarios. Aún con la autorización expresa del usuario propietario de la misma. Los usuarios son responsables de todas las actividades llevadas a cabo con su código de usuario.

El usuario será el directo responsable de cualquier daño producido por medidas o decisiones mal tomadas, mantenimientos, reparaciones, conexiones o instalaciones realizados por él que no fueran informadas o consultadas a la oficina de Sistemas de Información de la ESE BARRANCABERMEJA.

Los usuarios del sistema deben Informar inmediatamente a la oficina de Sistemas de Información cualquier anomalía, aparición de virus o programas sospechosos e intentos de intromisión y no intente distribuir este tipo de información interna o externamente.

A cualquier infracción a la política de seguridad informática cometida por un funcionario, personal tercerizado y/o contratista de la ESE BARRANCABERMEJA, se le aplicara lo estipulado en el Código Único Disciplinario (A LA LEY 1952 DE 2019 Modificada por Ley 2094 de 2021) TITULO **IV CAPITULO II ARTÍCULO 38. Num 25**: “Son deberes de todo servidor público: Denunciar los delitos, contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley.”

En caso de presentarse un problema crítico a nivel informático en horario no laboral afectando el normal funcionamiento de la ESE Barrancabermeja, la oficina de Sistemas de Información revisará el caso, y si es necesario informará a la oficina de soporte de los proveedores o brindará soporte del caso y soluciona de lo contrario informará si es necesario actuar conforme al plan de contingencia.

Está prohibido intentar sobrepasar los controles de los sistemas, o tratar de saltar los bloqueos de acceso a internet (cambio de dirección IP, cambio de nombre de equipo, etc.) o introducir intencionalmente software malintencionado que impida el normal funcionamiento de los sistemas. En este caso se le aplicara lo estipulado en el Código Único Disciplinario (A LA LEY 1952 DE 2019 Modificada por Ley 2094 de 2021) **TITULO IV CAPITULO II ARTÍCULO 38. Num 25**: “Son deberes de todo servidor público: Denunciar los delitos, contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley.”

Todo funcionario que utilice los recursos informáticos deberá contar con las habilidades o conocimientos para dicha función y tendrá la responsabilidad de velar por su integridad, confidencialidad y disponibilidad de la información que maneje, especialmente si dicha información es crítica. el Código Único Disciplinario (A LA LEY 1952 DE 2019 Modificada por Ley 2094 de 2021) TITULO **IV CAPITULO II ARTÍCULO 38. Num 23**: “Son deberes de todo servidor público: “Responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización.

La oficina de Sistemas de Información es la única encargada y responsable de capacitar a los usuarios en el manejo de las herramientas informáticas que son ***exclusivas*** de la misión y función de la institución. La asistencia a la capacitación es obligatoria y requisito indispensable para acceder al sistema de información de lo contrario no se le asigna claves y contraseñas. Está totalmente prohibido el uso de contraseñas o claves de otro usuario.

En equipos o dispositivos de propiedad de los funcionarios o contratistas no se permitirá la instalación de software o el almacenamiento y/o procesamiento de información propiedad de la ESE Barrancabermeja. En todos los contratistas de los funcionarios o colaboradores se debe redactar una deben firmar una cláusula de confidencialidad, que permita a la ESE Barrancabermeja proteger la información.

7.1.1 Procedimiento De Capacitación Y Sensibilización Del Personal:

La metodología empleada por la Ese Barrancabermeja para realizar la capacitación y sensibilización del personal en temas de seguridad de la información es brindada por el personal de Sistemas y se realiza en la charla dada en el proceso de inducción a la institución y también de manera periódica en las visitas a los diferentes puestos de trabajo mediante recomendaciones a los usuarios.

7.1.2 Procedimiento De Ingreso Y Desvinculación Del Personal:

Este procedimiento está soportado por el mapa de riesgo institucional donde se indica cómo la entidad gestiona de manera segura el ingreso y desvinculación, teniendo como controles e indicadores el cumplimiento de circular emitida por Gerencia y que se actualiza cada año, en ésta se detallan los responsables del envío de los datos del personal al área de sistemas para dar acceso o denegar a los usuarios del sistema de información de la entidad, por tanto no deben vincular funcionarios o colaboradores que deban realizar actividades en los sistemas de la entidad sin el envío de los datos requeridos para su asignación de usuarios y contraseñas.

7.1.3 Perímetros de Seguridad: Aquí definimos los perímetros físicos de seguridad donde se encuentra información crítica, sensible o se realice almacenamiento y/o procesamiento de información.

Los funcionarios de La oficina de Sistemas de Información de la ESE Barrancabermeja son los únicos autorizados para manejar, mantener y velar por la integridad y seguridad de los servidores centrales de la institución, así como tener las claves de ingreso, también son autorizados para brindarlas a los ingenieros de las empresas que brindan soporte a los sistemas ahí alojados en caso que se necesite.

Dentro de los servidores no deben almacenarse archivos de ningún tipo sólo se dejan los archivos de configuración de los sistemas, por la tanto en el caso que mediante la red local sean enviados archivos a carpetas de los servidores, la oficina de sistemas en aras de proteger la información tomará las acciones necesarias para eliminarlas.

En la Empresa Social del Estado Barrancabermeja, los servidores que alojan los diferentes sistemas utilizados en la institución estarán un área reservada para el data center dentro de la oficina de Sistemas, la cual contará con las condiciones de iluminación y climatización óptimas para que no afecte su rendimiento, NO está permitido el acceso de personal ajeno al área de sistemas.

7.1.4 Política De Uso De Correo Institucional

• La cuenta de correo electrónico institucional es el correo oficial de la institución y será creado por cada dependencia, la clave asociada asignada es personal, intransferible y por razones de seguridad deberá ser cambiada periódicamente, con periodicidad.

• Los mensajes de correo electrónico, chat y archivos adjuntos como información es propiedad de la Ese Barrancabermeja.

• La cuenta de correo es de uso exclusivo para cumplir las funciones misionales del servidor público al cual fue asignada, no deberá usarse para otros fines.

• Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

• Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera exclusiva a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.

• El usuario será responsable de revisar y depurar su buzón de correo periódicamente, a fin de evitar que éste se sature.

• Todo funcionario, contratista, personal tercerizado, etc. Que tenga asignada una cuenta de correo institucional, y éste se desvincule de la Entidad, deberá entregar a la oficina de Sistemas los usuarios y contraseña asignados, de igual manera dicha información debe entregarse.

7.2 GESTION DE ACTIVOS:

Este grupo de políticas se refiere a todas aquellas directrices mediante las cuales se indica a los funcionarios los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de Información, las políticas relacionadas con gestión de activos deben contemplar como mínimo:

7.2.1 Identificación de Activos: Esta política establece la periodicidad con la cual se va a realizar al interior de la Entidad la identificación o inventario de Activos ésta actividad será realizada por el área de Almacén con la periodicidad de 2 veces al año, para lo cual se dispondrá de personal para realizar dichas

funciones y en los casos que se requiera se brindará apoyo por parte de la oficina de Sistemas igualmente cuando se haga la adquisición de equipos o movimientos de equipos serán informados a la oficina de Almacén de la entidad para realizar las correspondientes novedades al inventario.

7.2.2 Clasificación de Activos: La Entidad basadas en las diferentes normas Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014, Decreto 103 de 2015 determina la clasificación de los activos de información de acuerdo a la criticidad, sensibilidad y reserva de la misma, este registro de Activos de información fue diseñado por la oficina de gestión documental estipulando el formato de la información, responsable, ubicación el tipo de activo de información entre otros y será actualizado en los caso que se requiera .

7.2.3 Devolución de los Activos: Esta política determina que los funcionarios, contratistas y/o terceros que cuenten con activos de la entidad una vez se termine el vínculo con la entidad el funcionario debe hacer entrega de éstos para lo cual la oficina de Almacén firmará el correspondiente Paz y Salvo, en cuanto a la información que tenga debe permanecer almacenada en el equipo de cómputo asignado y no podrá ser extraída, borrada o alterada para hacer copias previas de la respectiva información se debe contactar a la oficina de sistemas para que sea realizada y tenerlas en custodia.

7.2.4 Gestión de medios removibles: Esta política contempla que No se permite el uso de dispositivos de almacenamiento extraíble tales como memorias USB, CD o DVD, discos duros externos, o cualquier otro tipo de medio removible en los equipos de la ESE Barrancabermeja, exceptuando aquellos casos en donde por

fuerza mayor se requiera y previamente evaluado y aprobado por la oficina de Sistemas de Información.

7.2.5 Disposición de los activos: Esta política cumplir con un procedimiento seguro y correcto en la eliminación, retiro, traslado o re uso de activos cuando ya no se requieran.

Es así como se establece que para casos como el traslado, asignación y re uso de equipos será de acuerdo a necesidades de las áreas tomando en cuenta los requerimientos técnicos de los equipos de acuerdo al uso que se les dará, también cuando se presenten situaciones como renovación de hardware la oficina de sistemas hará la solicitud de acuerdo con las necesidades de cada puesto de trabajo priorizando los que más afecten en la prestación del servicio, en caso de daños de los equipos, se revisará en equipos embodegados por baja si cuentan con los repuestos que sirvan para poner en funcionamiento en caso que no sea así se realizará el pedido de compra de los repuestos. Para dar de baja los equipos la oficina de sistemas enviará al Almacén la solicitud y la justificación del retiro del inventario de dicho activo y la oficina de Almacén actualizará su inventario con esos datos.

7.2.6 Dispositivos móviles: Esta política determina que los funcionarios, contratistas o terceros no están autorizados para que en sus equipos personales cuenten con acceso de las redes inalámbricas de la ESE Barrancabermeja, salvo en casos autorizados por la gerencia y asumiendo la responsabilidad del caso, también los funcionarios que manejen los dispositivos móviles instituciones con y los planes de datos y minutos contratados por la entidad deben dar el correcto uso

a éstos (demanda inducida, confirmación de citas, seguimiento a pacientes entre otras) NO se deben tomar como de uso personal o familiar (no deben almacenarse contactos personales ni fotos, videos que no sean de carácter institucional ,tampoco descargar aplicaciones no autorizadas por la oficina de sistemas, es la oficina de sistemas la autorizada para que cuando se asigna un equipo móvil a un área o funcionario realice la asignación de las cuentas de correo para cada dispositivo y descarga las aplicaciones autorizadas para su uso quien cuando haga mal uso de éstos equipos y servicio se le aplicará el Código Único Disciplinario (A LA LEY 1952 DE 2019 Modificada por Ley 2094 de 2021) **TITULO IV CAPITULO II ARTÍCULO 38. Num 23**: “Son deberes de todo servidor público: “Responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización.

7.2.7 Perímetros de Seguridad:

En este dominio se define los perímetros físicos de seguridad donde se encuentra información crítica, sensible o se realice almacenamiento y/o procesamiento de información, estableciendo a los cuales los funcionarios, contratistas o terceros, tienen acceso y a cuáles no, la política debe definir los responsables de autorizar o no ingresos a las áreas delimitadas como de acceso restringido.

En la oficina de Sistemas de Información es donde se encuentra el data center de la Sede Administrativa, y es el personal de esta oficina quien tiene acceso a esta sección y administra los servidores, la red y demás dispositivos allí alojados. Ningún funcionario, contratista, terceros etc. externo a esta área puede ingresar a

esta sección así mismo aplica para las sedes de la institución, en casos que se requiera que un operador externo realice revisiones en el data center lo hará por orden y acompañamiento del personal del área.

Todo equipo de la Institución, debe estar ubicado en un área que cumpla con los requerimientos de: seguridad física, condiciones ambientales adecuadas, seguridad y estabilidad en la parte eléctrica, garantías que deben proporcionarse en conjunto con el área de mantenimiento de la ESE Barrancabermeja. Deben estar lejos de dos factores principales: La luz directa del Sol y de humedades, filtraciones y demás medios que puedan hacer que el equipo tenga contacto con el agua.

Todo equipo o periférico perteneciente a la red de la ESE Barrancabermeja, deberá contar con un dispositivo de protección eléctrica, ya sea estabilizador de corriente o UPS, que resguarde al equipo ante un cambio en la corriente eléctrica de la entidad o del sector donde se ubica. Por lo tanto, los equipos y dispositivos, deben conectarse a la red cableada instalada en cada una de las sedes según como se entrega a cada usuario, por lo cual no se autorizan movimientos de conexión de equipos en otras conexiones eléctricas. En caso que se necesite poner en funcionamiento un equipo que no tenga UPS o estabilizador, podrá hacerse de manera temporal y con el acompañamiento de un funcionario de la oficina de Sistemas de Información o del área de Mantenimiento.

Cuando se presentan tormentas eléctricas se recomienda apagar los equipos de cómputo y demás dispositivos para no exponerlos a daños.

La protección física, cuidado y la limpieza externa de los equipos corresponde al le corresponde al funcionario que lo manipula y quien debe notificar las eventualidades, tales como daños, pérdidas y demás en el menor tiempo posible a la oficina de Sistemas de Información de la ESE Barrancabermeja.

Está totalmente prohibido el consumo o ubicación de alimentos cerca de los equipos e impresoras, así como pegar distintivos, calcomanías y demás.

En caso que ocurra un incidente producido por el derrame de algún tipo de alimentos sobre un equipo, periférico o accesorio, este debe apagarse y desconectarse de inmediato e informar oportunamente a la oficina de Sistemas de Información quien hará el mantenimiento necesario he informara a quien corresponda para que se tomen las medidas correctivas necesarias.

Toda instalación de equipo, mantenimiento o proceso de soporte técnico a nivel de hardware, sin importar su nivel de complejidad, debe ser única y exclusivamente realizado por personal de la oficina de Sistemas de Información de la ESE Barrancabermeja. Bajo ningún concepto se autoriza que personal ajeno a la oficina de Sistemas de Información manipule los equipos de la Entidad, salvo las excepciones que se tienen cuando tengamos contratos de mantenimientos con empresas externas y esto con la autorización y/o acompañamiento del personal de área.

7.2.8 Políticas De Acceso A Internet

Los servicios de correo electrónico e internet, son administrados por la oficina de Sistemas de la Empresa Social del Estado Barrancabermeja, el proveedor es el responsable de garantizar su disponibilidad siempre que se encuentren los servicios con los pagos respectivos.

No se podrá utilizar el internet de la institución, como un medio de acciones que vayan en contra de la Ley.

En la institución se establecieron controles para el acceso a páginas de redes sociales y algunos canales que consumen mucho tráfico en la red. Por lo que se prohíbe el acceso a éstas páginas y así mismo la instalación de programas que le brinden saltos a dichos controles.

7.2.9 Política De Seguridad De Software

La instalación de software informático y de telecomunicaciones sólo será realizado por el personal de la oficina de Sistemas de la ESE Barrancabermeja.

Está prohibido el uso de software no licenciado en los equipos de cómputo de la ESE Barrancabermeja Está prohibido el uso de aplicaciones ilegales y el uso de “Cracks”, “Keygens” y demás aplicativos.

Está totalmente prohibido la instalación de juegos, programas de mensajería o aplicativos que no estén relacionados con las labores institucionales que se realizan en la Barrancabermeja

Todos los equipos deben disponer de software de seguridad (antivirus, filtros de contenido web, controles de acceso, entre otros). Equipo que no cuente con estos aplicativos de seguridad, no puede conectarse a la red de la institución.

La adquisición y actualización de software para los equipos de cómputo y de telecomunicaciones se llevará a cabo de acuerdo a requerimientos que sean propuestos por la oficina de Sistemas y a la disponibilidad presupuestal con el que se cuente.

Es obligación de todos los usuarios que manejen información masiva y/o crítica, solicitar respaldo correspondiente a la Oficina de sistemas sobre la generación copias de seguridad ya que se considera como un activo de la institución que debe preservarse. Las copias de respaldo a la información generada por el personal y los recursos informáticos de la institución deben estar resguardadas en sitios debidamente adecuados para tal fin.

La oficina de Sistemas de Información administrará los diferentes tipos de licencias de software con la que cuenta la ESE Barrancabermeja vigilará su vigencia de acuerdo a sus fechas de caducidad y solicitará la adquisición y/o la renovación del caso.

7.3 NO REPUDIO

La política de no repudio proporciona prueba del origen, autenticidad e integridad de los datos. Brinda seguridad al remitente de que su mensaje fue entregado, así como una prueba de la identidad del remitente al destinatario. Es por eso que ninguna de las partes puede negar que un mensaje fue enviado, recibido y procesado.

Para garantizar el no repudio en seguridad informática la Ese Barrancabermeja en procesos tales como el manejo de correos electrónicos, transacciones bancarias, movimientos en el sistema de información y manejo de certificados de firma digital la Entidad cuenta con .establecer los siguientes mecanismos:

Identificación y autenticación: que provee la capacidad de identificar a un usuario de un sistema esto se logra mediante las claves de ingreso, identificación de direcciones de red, logs de auditoría del sistema, seguimiento a correos electrónicos y criptografía en las certificados digitales y transacciones bancarias los cuales cuentan con llaves privadas que generan la seguridad que es el asegurar que un usuario es quien dice ser.

Certificado digital

Los funcionarios autorizados para el uso de estas firmas deben actuar de acuerdo con la responsabilidad del caso conociendo que el certificado digital es un documento que nos identifica en internet para poder realizar trámites online (envío de archivos a ministerio, Supersalud entre otros.) y que permite la firma electrónica, por lo que deben dar un buen uso a éstas sólo es autorizado. Ejemplos de firma electrónica los certificados digitales de Certicámara que mediante encriptación ayuda a ocultar la información transmitida por la red o almacenada en los equipos, para que cualquier persona ajena no autorizada, sin el algoritmo y clave de descifrado, pueda acceder a los datos que se quieren proteger.

Por la naturaleza de estas firmas se debe dejar claro que Solo el titular de la clave privada puede acceder a esta clave y crear esta firma, demostrando que un documento fue firmado electrónicamente por ese titular.

También las aplicaciones para lograr la firma digital deben instalarse en los equipos de la entidad no se autoriza su instalación en equipos personales.

Las transacciones bancarias deben ser realizadas por la pagadora únicamente desde el equipo asignado el cual cuenta con las configuraciones requeridas para acceder a las aplicaciones bancarias.

7.4 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:

La EMPRESA SOCIAL DEL ESTADO BARRANCABERMEJA deberá documentar una política general de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información. Para ello la oficina de Sistemas, desarrollará el Procedimiento de Gestión de Incidentes de Seguridad de la Información y en él se establecerá como actividad el reporte de los incidentes a las autoridades como el CSIRT o COLCERT.