POLITICAS DE SEGURIDAD

EMPRESA SOCIAL DEL ESTADO HOSPITAL SAN JOSE
BELEN DE UMBRIA, RISARALDA
2019

POLITICAS DE SEGURIDAD

COMITÉ DE ARCHIVO

Colaboradores:

Dr. JHON FREDY MONTOYA VELASQUEZ
Gerente
CARLOS ALBERTO VELEZ TABARES
Técnico
Dra. ADRIANA MUÑOZ ESCOBAR
Coordinadora de Control Interno
Dra. JACQUELINE SUAREA GALLON
Subdirectora Administrativa
JOHANA CAROLINA MOGOLLON
Odontóloga

EMPRESA SOCIAL DEL ESTADO HOSPITAL SAN JOSE
BELEN DE UMBRIA, RISARALDA
2019

CONTROL DE CAMBIOS

Control de Cambios	
Copia Número	**Distribución**
1	E.S.E. Hospital San José

Personas que participaron en la preparación de este documento	
Función:	**Nombre:**
Gerente	Dr. Jhon Fredy Montoya Velásquez
Técnico	Sr. Carlos Alberto Vélez Tabares
Coordinadora de Control Interno	Dra. Adriana Muñoz Escobar
Subdirectora Administrativa	Dra. Jacqueline Suárez Gallón
Subdirector Científico	Dr. Jhon Alexander García Sánchez

Lista de Revisión		
Versión	**Encargado**	**Fecha**
Versión 01	Carlos Alberto Vélez Tabares	01 de septiembre de 2019

Aprobado por:	**Fecha:**
Comité de Archivo	01 de septiembre de 2019

Historial de cambio	
Versión	**Descripción de la Revisión**
01	➢ Establecimiento del plan en su primera versión.

Documentos Asociados

-

PRESENTACION

Las entidades de salud no son ajenas a los desarrollos de procedimientos que mejoran sus actividades internas en todo campo de acción; es por esto que se definen actualizaciones de los actuares de todos los funcionarios enmarcados al mejoramiento continuo institucional.
Mediante el desarrollo del presente documento, se pretende dar a conocer los principales aspectos en cuanto a las falencias, mejoras y recomendaciones para el manejo de lo referente a la gestión documental de la institución.

Tabla de contenido

1 OBJETIVOS

Establecer diferentes medidas para garantizar la seguridad de todos los componentes del sistema de información de la ESE.

1.1 OBJETIVOS ESPECÍFICOS

- Garantizar la documentación, mantenimiento y actualización de los procedimientos de operación y administración tecnológica.
- Mantener actualizado el inventario de activos de información de la Empresa Social del Estado Hospital San José del Municipio de Belén de Umbría, Risaralda.
- Garantizar que la información reciba un adecuado nivel de protección.
- Impedir el acceso no autorizado a los sistemas de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.
- Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información que pertenece o es custodiada por la ESE.
- Proteger Los Equipos de Procesamiento de información crítica la ESE ubicándolo en Áreas seguras y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.
- Identificar y controlar los Factores de Seguridad Ambiental que Podrían Perjudicar el Normal Funcionamiento de los equipos de procesamiento de la Información de la Entidad.
- Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información.
- Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos de la entidad.

2 ALCANCE

Las políticas y normas definidas en este documento aplican para todos los funcionarios, contratistas y terceros que tengan acceso a los sistemas de información de la ESE.

3 CONTROL DE ACCESO

3.1 RESPONSABILIDADES

3.1.1 Seguridad de la Información

Sugerir procedimientos para la asignación de acceso a los sistemas, bases de datos y servicios de información multiusuario; la solicitud y aprobación de acceso a Internet o redes externas; el uso de computación móvil y trabajo remoto.

Analizar y sugerir medidas a ser implementadas para hacer efectivo el control de acceso de los usuarios a diferentes servicios como VPN, Internet o digitalización entre otros.

Verificar el cumplimiento de las pautas establecidas, relacionadas con control de acceso, creación de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios, uso controlado de utilitarios del sistema.

Concientizar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo.

3.1.2 Los Propietarios de los activos de Información

Evaluar los riesgos a los cuales se expone la información con el objeto de:

- Clasificar la información
- Determinar los controles de acceso, autenticación y utilización a ser implementados en cada caso.
- Aprobar y solicitar la asignación de privilegios a usuarios.
- Llevar a cabo un proceso formal y periódico de revisión de los Privilegios de acceso a la información.

3.1.3 Los Líderes de los Procesos

Autorizarán el trabajo del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, acatando las normas vigentes. Así mismo, autorizarán el acceso de los usuarios a su cargo a los servicios y recursos de red y a Internet.

3.1.4 Jefe Oficina de Sistemas

Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.
Evaluar el costo y el impacto de la implementación de “enrutadores” o “Gateway” adecuados para subdividir la red y recomendar el esquema apropiado.

Implementar el control de puertos, de conexión a la red y de ruteo de red.
Implementar el registro de eventos o actividades de usuarios de acuerdo a lo definido por los propietarios de la información, así como la depuración de los mismos.

3.2 POLITICAS GENERALES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

3.2.1 Políticas

Deben establecerse medidas de control de acceso a nivel de red, sistema operativo, sistemas de información y servicios de TI. Los controles de acceso deben ser conocidos por todos los servidores públicos de la entidad y limitar el acceso hacia los activos de información de acuerdo a lo establecido por el perfil de cargo.

Se deben implementar procedimientos para la asignación de privilegios de acceso a los sistemas de información, bases de datos y servicios, estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

3.3 CONTROL DE ACCESO

3.3.1 NORMAS

3.3.1.1 Requerimientos para el Control de Acceso

Los controles de acceso deberán contemplar:

a) Requerimientos de seguridad de cada una de las aplicaciones.
b) Definir los perfiles o privilegios de acceso de los usuarios a las aplicaciones de acuerdo a su perfil de cargo en la entidad.

3.3.1.2 Administración de Accesos de Usuarios

La Oficina de Sistemas establece procedimientos para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

3.3.1.3 Creación de Usuarios

La Oficina de Sistemas, deberá mantener los registros donde cada uno de los líderes responsables de los procesos haya autorizado a los servidores públicos o terceros el acceso a los diferentes sistemas de información de la entidad.
Los datos de acceso a los sistemas de información deberán estar compuestos por un ID o nombre de usuario y contraseña que debe ser único por cada servidor público o tercero.
Cuando se retire o cambie de contrato cualquier servidor público o tercero, se deberá aplicar la eliminación o cambios de privilegios en los sistemas de información a los que el usuario estaba autorizado.

El proceso de gestión de información y comunicaciones deberá realizar revisiones de privilegios de acceso a los diferentes sistemas de información por parte de los servidores públicos y terceros, manteniendo los registros de las revisiones y hallazgos.

3.3.1.4 Administración de Contraseñas de Usuario

Las contraseñas de acceso deberán cumplir con un mínimo de 8 caracteres y la combinación de números, letras mayúsculas y minúsculas, en lo posible utilizar caracteres especiales.
Ningún usuario debe darle o "prestarle" sus credenciales de acceso a los aplicativos de la ESE a otro usuario con el fin de realizar labores en el sistema, por mínimas que estas sean.
Todos los servidores públicos deberán cambiar permanentemente su contraseña de acceso a los diferentes sistemas de información.
Los sistemas de información deberán adaptarse para bloquear permanentemente al usuario luego de 5 intentos fallidos de autenticación.

3.3.1.5 Uso de Contraseñas

Los usuarios deben cumplir las siguientes normas:

a) Mantener los datos de acceso en secreto.
b) Contraseñas fáciles de recordar y difíciles de adivinar.
c) Que las contraseñas no estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo, nombres, números de teléfono, fecha de nacimiento, etc.
d) Notificar de acuerdo a lo establecido cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

3.3.1.6 Equipos Desatendidos en Áreas de Usuarios

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

a) Los equipos instalados en áreas de usuarios, por ejemplo, estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.
b) Salir de aplicativos críticos al abandonar el puesto de trabajo.
c) Bloquear el equipo de cómputo tras abandonar el puesto de trabajo.
d) Bloqueo automático de la sesión en el equipo de cómputo tras inactividad superior a 5 minutos.
e) Apagar los equipos de cómputo al finalizar la jornada laboral.

3.3.1.7 Control de Acceso a la Red

El proceso de Gestión de la Información debe asegurar el bloqueo al acceso de páginas de contenido para adultos, redes sociales, hacking, descargas (FTP), mensajería instantánea y cualquier página que represente riesgo potencial para la Entidad mediante el uso de servidor proxy, firewall o el software que mejor se ajuste a la necesidad. Excepciones de acceso, serán aprobados por el jefe inmediato, según la necesidad del cargo y verificación previa de que las paginas solicitadas no contengan código malicioso con el visto bueno del área de información.

3.3.1.8 Autenticación de Usuarios para Conexiones Externas

La autenticación de usuarios remotos deberá ser aprobada por el líder del proceso de Gestión de la Información.

3.3.1.9 Control de Conexión a Redes

La infraestructura de la ESE deberá estar separada por Vlans para garantizar la confidencialidad de los datos que se transmitan.

3.3.1.10 Seguridad en los Servicios de Red

Mantener instalados y habilitados sólo aquellos servicios y puertos que sean utilizados por los sistemas de información y software de la entidad.

Controlar el acceso lógico a los servicios, tanto a su uso como a su administración mediante bloqueo de puertos en el firewall de la entidad.

3.3.1.11 Control de Identificación y Autenticación de Usuarios.

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de Usuario) solamente para su uso personal exclusivo, de manera que las actividades tengan trazabilidad.

3.3.1.12 Sistema de Administración de Contraseñas

El sistema de administración de contraseñas debe:

a) Obligar el uso de User ID´s y contraseñas individuales para determinar responsabilidades.
b) Permitir que los usuarios seleccionen y cambien sus propias contraseñas luego de cumplido el plazo mínimo de mantenimiento de las mismas o cuando consideren que la misma ha sido comprometida e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
c) Obligar a los usuarios a cambiar las contraseñas provisionales o que han sido asignadas por el administrador del sistema de información.
d) No permitir mostrar las contraseñas en texto claro cuando son ingresadas.
e) Almacenar las contraseñas en forma cifrada.

3.3.1.13 Sesiones Inactivas

Si el usuario debe abandonar la estación de trabajo momentáneamente, activará protectores de pantalla con contraseñas, con el fin de evitar que Terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.
Si los sistemas de información detectan inactividad por un periodo igual o superior a diez minutos, deben automáticamente aplicar, “timeout” es decir, finalizar la sesión de usuario.

3.3.1.14 Limitación del Tiempo de Conexión

Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo:

a) Limitar los tiempos de conexión al horario normal de oficina, de no existir un requerimiento operativo de horas extras o extensión horaria.

Documentar los funcionarios o contratistas que no tienen restricciones horarias y los motivos y evidencia de la autorización expedida por el líder del proceso de Gestión de la Información.

4 SEGURIDAD FISICA

4.1 RESPONSABILIDAD

Las Políticas y Normas de Seguridad de la Información son de Carácter Obligatorio para todos los funcionarios y terceros vinculados con la ESE independientemente del nivel de las tareas que desempeñe.

4.1.1 El Responsable de Seguridad de la Información

El Responsable del proceso Gestión de la Información junto con los Responsables de Información de cada proceso de la entidad, establecerá los controles necesarios de seguridad física y ambiental para la Protección de los Activos de Información, en función a un análisis de riesgos; Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en la Presente Norma.

4.1.2 Líderes de Procesos de la ESE

Definirán los niveles de acceso físico de los Funcionarios de la Entidad a las áreas restringidas bajo su responsabilidad.

Autorizarán formalmente el trabajo fuera de las instalaciones con Información de su Dependencia a los Funcionarios de la ESE cuando lo crean conveniente.

4.1.3 Control Interno

O en su defecto quien sea propuesto por el Comité GEL revisará los registros de acceso de los funcionarios, Contratistas o Terceros a las instalaciones físicas, áreas seguras definidas, con el fin de verificar la eficacia de los controles físicos en la entidad.

Nota: **Sanciones Previstas por Incumplimiento**

El incumplimiento de las Políticas podrá dar lugar a un proceso disciplinario para los funcionarios y se podrá convertir en un incumplimiento del contrato respecto de los contratistas, que pueda dar lugar a la imposición de sanciones e incluso su terminación, sin perjuicio de la iniciación de otro tipo de acciones a las que haya lugar.

4.2 POLÍTICAS Y NORMAS DE SEGURIDAD DE LA INFORMACIÓN

4.2.1 Políticas

Todas las áreas destinadas al procesamiento de la información según los niveles de clasificación establecidos por la entidad, (Público, Interno, Confidencial y Secreto) deben contar con protecciones físicas o perímetros de seguridad (tales como paredes, puertas de acceso controlado,

recepcionistas, cámaras de seguridad), éstas deben cubrir con las necesidades en cuanto a: controles de entradas físicos, seguridad de oficinas, espacios y medios, protección contra amenazas externas y ambientales. Los controles deben ser de acuerdo a la necesidad de aseguramiento, clasificación y valoración de los activos de información establecidos por los responsables.

La ESE debe contar con perímetros de seguridad en las áreas donde se encuentren instalados los centros de procesamiento de la Información, Suministro de Energía Eléctrica, de Aire Acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los Sistemas de Información de la ESE.

Los Equipos de Cómputo de la ESE deben estar protegidos frente a posibles fallas en el Suministro de Energía Eléctrica, para asegurar la continuidad del servicio.

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información de la ESE estará protegido contra intercepción o daños.

4.3 SEGURIDAD FÍSICA Y AMBIENTAL

4.3.1 NORMAS

4.3.1.1 Perímetro de Seguridad Física y Ambiental:

- Los perímetros de seguridad deben estar delimitados por una barrera, por ejemplo, una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas para controles de acceso físico.
- Se Debe establecer y documentar claramente los perímetros de Seguridad.
- Se debe ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida. Las paredes externas del área deben ser sólidas y casi todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, (Mecanismos de control, vallas, alarmas, cerraduras, entre otras).
- Identificar claramente todas las Salidas de Emergencia en caso de escenarios catastróficos en la entidad.
- Nota: El Responsable de la Seguridad de la Información debe llevar un registro actualizado de las Áreas Seguras, donde se indique la identificación del Edificio y Área, principales Activos de información a proteger y medidas de protección física.

4.3.2 Controles de acceso físico

Todas las áreas destinadas al procesamiento o almacenamiento de información confidencial y secreta, así como aquellas en las que se encuentren los equipos y demás infraestructura que soporte a los sistemas de información y comunicaciones debe ser protegida con medidas de control de acceso físico tales como:

- Los Centros de Cómputo debe contar con mecanismos de control de acceso tales como puertas de seguridad, cerradura, sistemas de control con tarjetas inteligentes, sistema de alarmas o controles biométricos.
- El ingreso de terceros a los Centros de Cómputo y Centros de Cableado, debe estar debidamente registrado mediante una bitácora.
- Todos los funcionarios, Contratistas o Terceros deben portar el carnet que los acredite que prestan sus servicios a la ESE, no deben intentar ingresar a las áreas donde no tengan la debida autorización.

4.3.3 Seguridad de Las Oficinas

- Los escritorios o puestos de trabajo de los servidores públicos deben mantenerse limpios y sin documentos fuera del horario de trabajo o en ausencia prolongada del sitio, esto para evitar el acceso no autorizado a la información.
- Los Servidores Públicos deben colocar las pantallas de sus computadores en una posición en la que se evite que personal no autorizado pueda ver la información que se encuentre desplegada en ellas.
- Las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a las oficinas solo deben ser utilizados por los funcionarios autorizados y, salvo situaciones de Emergencia, estos no deben ser transferidos a otros funcionarios de la Entidad, Contratista o Terceros con su debida autorización.
- Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.
- No dejar abandonada en las impresoras información Confidencial y Secreta, una vez se haya impreso.

4.3.4 Protección contra Amenazas Externas y Ambientales

- Las Oficinas e instalaciones donde se procesa y/o almacena la información confidencial o secreta debe contar con sistemas de alarmas y cámaras de seguridad, sistema de detección y extinción automáticas de incendios.
- Se debe mantener buena ubicación de los equipos, aislado de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.
- Los equipos del Centro de Cómputo deben tener control de los niveles de temperatura y humedad, estos deben ser mantenidos dentro de los límites requeridos por la infraestructura de cómputo allí instalada.
- Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipo que registre información, a menos que hayan sido formalmente autorizadas por el responsable del proceso involucrado y el responsable de Seguridad Información.
- No se permite comer, beber y fumar dentro de las instalaciones de procesamiento de la información de la ESE o puestos de trabajo.

4.3.5 Seguridad en los Servicios de Suministro Eléctrico

- Disponer de múltiples enchufes o líneas de suministro de energía eléctrica regulada.
- Contar con un Sistema de Energía Ininterrumpible UPS y/o plantas eléctricas con intercambio automático, para asegurar el Apagado Regulado y Sistemático de los Equipos de Cómputo de la ESE y Asegurar la continuidad de las operaciones Mientras se restablecen las fallas en el suministro de energía eléctrica.
- Se debe contar con Interruptores de Emergencias que deben estar ubicados cerca de las salidas de emergencia de las Instalaciones donde se encuentren los equipos de cómputo, con el fin de facilitar un corte rápido de la energía en caso tal se presente una situación crítica.
- La ESE debe contar con iluminación de emergencia en caso de producirse una falla en el suministro principal de energía.
- La ESE debe contar con protección contra descargas eléctricas en los edificios donde se ubica.

4.3.6 Seguridad del Cableado

- Cumplir con los Requisitos Técnicos Vigentes de la República de Colombia.
- Realizar las Conexiones Adecuadas para la Energía Eléctrica y la Red De Datos.
- Proteger el Cableado de red contra Intercepción no Autorizada, el cableado debe contar con conductos como canaletas para su adecuada protección.
- El cableado Eléctrico debe estar separado del cableado de Red para Evitar posibles Interferencias.

4.3.7 Mantenimiento de Equipos

- Se debe dar cumplimiento al programa de mantenimiento a los equipos de la entidad.
- Se deben realizar mantenimientos preventivos y pruebas funcionales al Sistema de UPS y/o plantas eléctricas, sistemas de detección y extinción de incendios, sistemas de aire acondicionado, servidores, equipos de comunicaciones, equipos de seguridad que conforman la plataforma tecnológica de la ESE.
- Los trabajos de mantenimiento de redes eléctricas, cableado de datos y voz, deben ser realizados por el personal especialista y debidamente autorizado e identificado.
- Se deben someter a las estaciones de trabajo, portátiles, servidores, equipos de comunicaciones, al mantenimiento preventivo, de acuerdo con el cronograma establecido y las especificaciones del proveedor, con la debida autorización formal del responsable del proceso Gestión de Tecnologías de la Información de la ESE.
- El Responsable del proceso Gestión de Tecnologías de la Información deberá tener un Listado con las especificaciones o características de los equipos, así como también la fecha en la que cada equipo requiere actividades de mantenimiento.
- Registrar las fallas de los mantenimientos de las estaciones de trabajo, portátiles, equipos de comunicaciones y operaciones ya sean preventivo o correctivos, este tipo de registro debe indicar la fecha en la que fue realizado el mantenimiento, falla que presentó y quien realizó el mantenimiento.

4.3.8 Seguridad del equipo Fuera de la entidad

- El uso de equipos de cómputo, portátiles, discos removibles destinado al procesamiento de información, fuera de las instalaciones de la ESE, será autorizado por el responsable del proceso al que pertenezca el servidor público.
- El Usuario que está autorizado a retirar un equipo de cómputo o portátil debe tener el mismo nivel de protección de la información como si estuviese en las instalaciones de la entidad.

Periódicamente se debe monitorear la eficacia del control de Registros de Los Equipos, para detectar el Retiro No Autorizado de Activos de Información de la ESE, Control que será llevado a cabo por el Líder de Seguridad de la Información.

5 GESTION DE COMUNICACIONES Y OPERACIÓN

5.1 RESPONSABILIDADES

5.1.1 El Responsable de Seguridad de la Información

- Deberá crear procedimientos para el control de cambios a los procedimientos operativos, los sistemas de información e instalaciones de procesamiento de información.
- Establecer criterios de aprobación para los cambios en seguridad de la información a los componentes de la plataforma tecnológica, el cual conlleve modificación de accesos, modificación o mantenimiento de software, actualización de versiones o modificación de parámetros.
- Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento y procesamiento de la información.
- Crear y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso para garantizar la seguridad de las comunicaciones y operaciones de la entidad.
- Desarrollar procedimientos adecuados para la Creación de Usuarios, Control de Acceso al sistema y Administración de Cambios.
- Sugerir procedimientos para la administración de equipos de cómputo, portátiles, discos removibles, USB, destinados al procesamiento de información de la entidad.

5.1.2 Jefe de Sistemas:

- Verificar la existencia de documentación actualizada relacionada con los procedimientos de comunicaciones y operaciones de la ESE.
- Administrar los recursos necesarios para permitir la segregación de los ambientes de Desarrollo, Pruebas y Operación.
- Garantizar la separación de ambientes de desarrollo, pruebas y operación, estas deben ser documentadas y aprobadas formalmente con los cambios solicitados, así como la independencia de los funcionarios que ejecutan dichas labores, con el fin de reducir el riesgo de acceso no autorizado o cambios en el sistema de operación.
- Controlar la realización de las copias de respaldo o Backup de información, así como la prueba periódica de su restauración.
- Implementar sistemas de barrera, defensa o detección contra Intrusos como cortafuegos, antivirus control de accesos no autorizados con el fin de preservar la Confidencialidad, Disponibilidad e Integridad de los activos de Información.

5.1.3 Todos Los Funcionarios, Contratistas o Terceros

- Son responsables de dar cumplimiento a todas las políticas y normas de seguridad descritas en este documento.

5.2 POLITICAS Y NORMAS DE SEGURIDAD DE LA INFORMACIÓN

5.2.1 Políticas

1) Los procedimientos y responsabilidades de operación y administración de la plataforma tecnológica y de seguridad deben estar documentados, garantizando un adecuado control de cambios y un manejo eficiente de incidentes de seguridad de la información en la entidad.
2) Los activos de información deben administrarse y operarse con una segregación de funciones adecuada con el valor del activo establecida por el responsable, para disminuir la exposición a riesgos de seguridad de la información y asegurar que la planificación y puesta en producción de los sistemas de información tengan en cuenta los requerimientos de seguridad de la información.
3) Los ambientes de desarrollo, prueba y operaciones de los sistemas de información de la ESE deben estar separados, para garantizar la seguridad en cada ambiente.
4) Se deben implementar protecciones contra software malicioso y asegurar que el mantenimiento, la administración de la red, el cuidado de los medios de almacenamiento y el intercambio de información se realice ejecutando los controles de seguridad de la información definidos.

5.3 GESTION DE COMUNICACIONES Y OPERACIONES

Se debe garantizar la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica que apoya los procesos de negocio en la entidad.
Se deben definir procedimientos para el control de los cambios en el ambiente de pruebas y operación. Los cambios deben ser evaluados previamente en aspectos técnicos y de seguridad de la información.

Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferiblemente en forma física.
Para ello, se tendrán en cuenta los siguientes controles:

a) Ejecutar el software de desarrollo y de operaciones, en diferentes ambientes de operaciones, equipos, o directorios.
b) Bloqueo de acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente operativo, cuando no sean indispensables para el funcionamiento del mismo.
d) Control de accesos independientes para los diferentes ambientes, así como los privilegios de acceso a los sistemas.
e) Definir Responsables de la información para cada uno de los ambientes de procesamiento existentes.

En la tercerización de la administración de las instalaciones de procesamiento, se acordarán controles con el proveedor del servicio y se incluye en los acuerdos de niveles de servicio:

a) Identificar las aplicaciones sensibles o críticas que convenga retener en la ESE.
b) Asignar funciones específicas y procedimientos para monitorear todas las actividades de seguridad de la Información.
c) Establecer niveles de disponibilidad y continuidad de la prestación de los servicios.

d) Establecer niveles de soporte a los sistemas de información tercerizados.

Se debe garantizar la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica que apoya los procesos de negocio en la entidad
La Oficina de Sistemas debe garantizar la gestión de la capacidad y aceptación de los sistemas de información en la entidad.

Para realizar aceptación de los sistemas de información se debe:

a) Verificar el impacto en el desempeño y los requerimientos de capacidad de los computadores.
b) Garantizar la recuperación ante errores.
c) Asegurar que la instalación del nuevo sistema no afectará negativamente los sistemas existentes.
d) Realizar programas de capacitación en la operación y/o uso del nuevo sistema.

La Oficina de Sistemas mantiene actualizado y monitorea el software establecido para detección y control de códigos maliciosos.
La Oficina de Sistemas establece un procedimiento de copias de seguridad de los activos críticos garantizando su disponibilidad.
Los funcionarios, contratistas o terceros que necesiten conectarse a la infraestructura de la Entidad deberán estar autorizados mediante un correo electrónico emitido bien sea por el área de Recurso Humano o por los propietarios de la información.
Toda comunicación externa a la infraestructura de la ESE que transporte información confidencial o secreta deberá ser por medio de una VPN y el cifrado mínimo será de 256 bits.

6 DESARROLLO Y MANTENIMIENTO DE SISTEMAS

6.1 RESPONSABILIDADES

6.1.1 El Responsable de Seguridad de la Información

Identificar y sugerir los controles a ser implementados en los sistemas desarrollados internamente o por terceros.
Verificar el cumplimiento de los controles establecidos para el desarrollo y Mantenimiento de sistemas.
Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas.

6.1.2 Jefe del proceso de Gestión de Tecnologías de la Información y Comunicación

Administración de las técnicas criptográficas y claves.
Licenciamiento, calidad del software y la seguridad de la información en los contratos con terceros para el desarrollo de software.

6.2 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN - DESARROLLO Y MANTENIMIENTO DE SISTEMAS

6.2.1 Políticas

Durante el análisis y diseño de las aplicaciones, se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.
La ESE debe asegurar que se realice el análisis e implementación de los requerimientos de seguridad en el software y/o sistemas de información que se desarrollen o se adquieran, debe incluir controles de autenticación y auditoría de usuarios, verificación de los datos de entrada y salida, y que se implementen buenas prácticas para un desarrollo seguro.

6.3 DESARROLLO Y MANTENIMIENTO DE SISTEMAS

6.3.1 Requerimientos de Seguridad de los Sistemas

El proceso de Gestión de la Información deberá exigir los requerimientos en seguridad de la información para nuevos sistemas o mejoras a los sistemas de información o desarrollo existentes en la entidad.

6.3.2 Seguridad de los Sistemas de Información

Es necesario implementar controles y registros de auditoría, verificando:

a. La validación de datos de entrada.
b. El procesamiento interno.
c. La autenticación de mensajes (interfaces entre sistemas)
d. La validación de datos de salida.

6.3.3 Validación de Datos de Entrada

Se definirá un procedimiento que, durante la etapa de diseño, especifique controles que aseguren la validez de los datos ingresados.

Este procedimiento considerará los siguientes controles:

a. Control de secuencia.
b. Control de monto límite por operación y tipo de usuario.
c. Control del rango de valores posibles y de su validez, de acuerdo a Criterios predeterminados.
d. Control contra valores cargados en las tablas de datos.
e. Controles por oposición, de forma tal que quien ingrese un dato no pueda autorizarlo y viceversa.

6.3.4 Integridad del Mensaje

Cuando una aplicación o software tenga previsto el envío de mensajes que contengan información de acuerdo a los criterios de la información de Confidencialidad, Integridad y Disponibilidad, se implementarán los controles criptográficos determinados en el punto “Controles Criptográficos”.

6.3.5 Validación de Datos de Salida

En las validaciones de seguridad de la información, se debe exigir a los desarrolladores internos o externos las validaciones de los datos de salida de modo que se garantice las ejecuciones correctas de acuerdo a los requerimientos funcionales por parte de la entidad.

6.3.6 Administración de Claves

Todas las claves serán protegidas contra modificación y destrucción, y serán protegidas contra copia o divulgación no autorizada mediante almacenamiento cifrado en las bases de datos.

6.3.7 Protección de los Datos de Prueba del Sistemas

Para las pruebas de los sistemas, se utilizarán datos extraídos del ambiente operativo. Para proteger los datos de prueba se establecerán normas que contemplen lo siguiente:

- Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización.

- Eliminar inmediatamente completadas las pruebas, la información operativa utilizada.
- Los datos del ambiente operativo no deben permanecer más de un mes en pruebas. Una vez cumplido este periodo deben ser borrados.

6.3.8 Control de Acceso a los Códigos Fuente

Para reducir la probabilidad de alteración de programas fuentes, se aplicarán las siguientes normas:

- Proveer al Área de Desarrollo los programas fuente solicitados para su modificación, manteniendo en todo momento la correlación programa fuente /ejecutable.
- Llevar un registro actualizado de todos los programas fuente en uso, Indicando nombre del programa, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).
- Administrar las distintas versiones de una aplicación.
- Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.
- Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuente.
- Realizar las copias de Seguridad y pruebas de restauración de los programas fuente cumpliendo los requisitos de seguridad establecidos por la ESE en los procedimientos que surgen de la presente política.

6.3.9 Procedimiento de Control de Cambios

A fin de minimizar los riesgos de alteración de los sistemas de información, se implementarán controles estrictos durante la realización de cambios.
Para ello se deben contemplar los siguientes controles

a. Verificar que los cambios sean propuestos por usuarios autorizados y respete los términos y condiciones que surjan de la licencia de uso.
b. Solicitar la autorización del propietario de la Información, en caso de tratarse de cambios a sistemas de procesamiento de la misma.
c. Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.
d. Solicitar la revisión del Oficial de Seguridad de la Información para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.
e. Mantener un control de versiones para todas las actualizaciones de software.

6.3.10 Revisión Técnica de los Cambios en Sistema Operativo

Cada vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

Para ello, se debe contemplar:

a. Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.
b. Garantizar que los cambios en el sistema operativo sean informados con antelación a la implementación.

6.3.11 Restricciones del Cambio de Paquetes de software

En caso de considerarlo necesario la modificación de paquetes de software suministrados por proveedores, y previa autorización del responsable del activo de información y el líder de Gestión de la Información se debe:

a. Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
b. Evaluar el impacto que se produce si la ESE se hace cargo del mantenimiento.
c. Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

6.3.12 Desarrollo Externo de Software

Para el caso que se considere la tercerización del desarrollo de software, se establecerán normas:

a. Acuerdos de licencias, propiedad de código y derechos de Propiedad Intelectual.
b. Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.

Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos.

7 MANEJO DE LOS ACTIVOS DE INFORMACIÓN

7.1 RESPONSABILIDAD

Los Integrantes de la Alta Dirección, Funcionarios, Contratistas son responsables de la implementación de las siguientes Políticas de Seguridad de la Información:

Las Políticas de Seguridad de la Información son de Carácter Obligatorio para todo el personal de la Entidad, cualquiera sea su situación laboral o el área en la cual se encuentre laborando. Estas Políticas también aplican a los terceros que tengan alguna relación con la entidad.

7.1.1 El Responsable de Seguridad de la Información

Cumplirá funciones relativas a la seguridad de los sistemas de información de la ESE, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política.

7.1.2 Los usuarios de la Información y de los Sistemas utilizados para su procesamiento

Son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.
Son responsables los líderes de proceso de mantener actualizado los activos de información a su cargo.

7.1.3 Control Interno

O en su defecto quien sea propuesto por el Comité GEL es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por estas Políticas y por las Normas, Procedimientos y prácticas que de ella surjan.

Nota: **Sanciones Previstas por Incumplimiento**

El incumplimiento de las Políticas podrá dar lugar a un proceso disciplinario para los funcionarios y se podrá convertir en un incumplimiento del contrato respecto de los contratistas, que pueda dar lugar a la imposición de sanciones e incluso su terminación, sin perjuicio de la iniciación de otro tipo de acciones a las que haya lugar.

7.2 POLÍTICAS Y NORMAS DE SEGURIDAD DE LA INFORMACIÓN – ACTIVOS DE INFORMACIÓN

POLÍTICAS

La ESE mantiene un inventario de los activos de información de la entidad, teniendo en cuenta los niveles de clasificación como Confidencialidad, integridad, disponibilidad y ubicación para lo cual debe realizar asignación de los responsables de los activos de información.

7.2.1 ACTIVOS DE INFORMACIÓN

7.2.1.1 Responsabilidad de los Activos de Información

Se identifican los activos de información de mayor importancia asociados a cada Sistema de Procesamiento de la Información en su respectivo proceso, con sus Responsables y su Ubicación, para luego elaborar un inventario con dicha información.

El Inventario se deberá identificar, documentar y actualizar ante cualquier modificación de la información y los Activos asociados con los Medios de Procesamiento. Este debe ser revisado con una periodicidad no mayor a un (1) año.
La responsabilidad de realizar y mantener actualizado el inventario de activos de información es de cada Responsable de proceso de la ESE.
El uso de los activos de información pertenecientes a la ESE es responsabilidad del propietario asignado; es su deber proteger y mantener la confidencialidad, integridad y disponibilidad de los activos de información.

7.2.1.2 Clasificación de la Información

Para la Clasificación de la Información se debe tener en cuenta los criterios de Confidencialidad, Integridad y Disponibilidad.

Definición de los Criterios de clasificación de la Información:

USO PÚBLICO:

Información que por sus características puede o debe estar a disposición de cualquier persona natural o jurídica en el Estado Colombiano. Dentro de esta clasificación se puede considerar: noticias, informes de prensa, información de rendición de cuentas, información sobre trámites, normatividad.

USO INTERNO:

Información cuya divulgación no causa daños serios a la ESE y su acceso es libre para los funcionarios a través de la intranet o de cualquier otro medio, como protocolos, guías, manuales, formatos, etc.

USO CONFIDENCIAL:

Información cuya divulgación no autorizada puede afectar considerablemente el cumplimiento de la misión de la ESE. La divulgación de esta información, requiere de la aprobación de su respectivo

propietario. En el caso de terceros rige el acuerdo de confidencialidad que exista entre la ESE y dicho tercero.

USO SECRETO:

Información que sólo puede ser conocida y utilizada por un grupo muy reducido de Funcionarios, generalmente de la Alta Dirección de la ESE, y cuya divulgación o uso no autorizados podría ocasionar graves pérdidas al mismo, a Contratistas o a Terceros.

Sólo el Funcionario Responsable de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes Requisitos Mínimos:

- Comunicárselo al Responsable del almacenamiento donde se encuentre el Activo de Información.

7.2.1.3 Etiquetado y Manejo de la Información:

Se deben Desarrollar procedimientos para el Etiquetado y Manejo de la Información, de acuerdo al esquema de clasificación definido por la ESE. Los mismos contemplarán los Activos de Tecnología de la información tanto en formatos Físicos, Digital, Activos Tecnológicos.