PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ELABORADO POR:

CARLOS ANDRES POSADA BUITRAGO - Gerente
LIDA ZORAIDA OTALVARO – Asr de Calidad
DUVANIER ALVAREZ POSADA – SISTEMAS ESTADISTICA

Empresa Social Del Estado
HOSPITAL SAN JOSE LA CELIA
La Celia - Risaralda
Julio de 2020

TABLA DE CONTENIDO

INTRODUCCIÓN

Uno de los activos más valiosos de la E.S.E Hospital San Jose La Celia es la información en la que se apoya para ofrecer los servicios a sus usuarios. El presente Manual de Seguridad está enfocado a describir el cómo la entidad gestiona la seguridad de la información.

La información puede pasar por tres estados fundamentales: transmisión, almacenamiento y proceso. Debe protegerse cualquiera que sea la forma que tome o los medios que se utilicen en cada estado. Así mismo, la información posee características relacionadas con la seguridad que se deben salvaguardar para cualquier información o documentación en que se empleen medios electrónicos, informáticos y telemáticos.

El manual de Seguridad de la Información es un documento que contiene lineamientos que apoyan la gestión y administración de los planes y procedimientos de seguridad de la información dando alcance a las prácticas de seguridad a la Institución.

1. OBJETIVO

Establecer los principales lineamientos de seguridad enmarcados dentro de la estrategia de gobierno en línea y gestión de la seguridad de la información para la E.S.E. Hospital San Jose La Celia.

2. ALCANCE

Este manual Contempla los lineamientos de la estrategia de gobierno en línea y los lineamientos principales para la seguridad de la información de la E.S.E. Hospital San Jose La Celia, los cuales deben ser conocidos y apropiados por empleados, contratistas y todo tercero que tenga acceso, almacene, procese o trasmita información de la E.S.E. Hospital San Jose La Celia o sus pacientes.

3. MARCO LEGAL APLICABLE

Ley Estatutaria 1581 de 2012: y Reglamentada Parcialmente por el Decreto Nacional 1377 De 2013: Por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto 2573 de 2014: Por el cual se establecen los lineamientos generales de la estrategia de gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

Decreto 2578 de 2012: Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye "El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles" entre otras disposiciones.

Decreto 2609 de 2012: Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.
Ley 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado "de la protección de la información y los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. "Ley 1341 DE 2009: Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

Norma ISO 27001: Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información.

4. RESPONSABLE

La Gerencia y el administrador de sistemas y TICS de la E.S.E. Hospital San Jose La Celia, o quien ésta designe.

5. DEFINICIONES

- **Información:** Conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

- **Usuario:** Es aquella persona que usa algo para una función en específico

- **Copia de Seguridad.** (BACKUP)**:** Se define como Backup o copia de seguridad, la actividad de resguardar de forma segura la información contenida en un medio de almacenamiento de origen (disco duro) a un medio de almacenamiento de destino de diferente tipo (otro disco duro, servidor de Backup, USB, CD, DVD, ZIP, entre otros)

- **Backup:** Copia idéntica de algo, copia de seguridad o copia respaldo de algo.

- **Rollback o reversión:** Es una operación que devuelve a la base de datos a algún estado previo. Los Rollbacks son importantes para la integridad de la base de datos, a causa de que significan que la base de datos puede ser restaurada a una copia limpia incluso después de que se han realizado operaciones erróneas.

- **Información Sensible:** Son todos aquellos archivos digitales generados desde los sistemas de información con los cuales la Institución cuenta.

- **Confidencialidad:** Es la propiedad de la información, por la que se gestiona que es accesible únicamente a personal autorizado a conocer la información.

- **Incidentes de seguridad de la información** Procesos para detectar, reportar, evaluar, responder, tratar y gestionar los fallos de seguridad de la información. (ISO/IEC 27000)

6. SEGURIDAD DEL RECURSO HUMANO

Todo el personal de la E.S.E Hospital San Jose La Celia, contratistas y/o terceros que tengan la posibilidad de acceder a la información de la Institución o a la infraestructura tecnológica para su procesamiento, son responsables de conocer y cumplir con las políticas institucionales establecidos para el manejo y seguridad de la información. De igual manera, son responsables de la información a reportar por medios electrónicos.

Todos los funcionarios de la E.S.E. Hospital San Jose La Celia, deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgo la seguridad y el buen nombre de la Institución.

Roles y responsabilidades

El área de Talento Humano será la encargada de diseñar, documentar y actualizar el manual especifico de funciones y requisitos por competencias laborales, para los empleos que conforman la planta global de

personal de la E.S.E. Hospital San Jose La Celia, donde se detallan los roles, las responsabilidades, funciones o actividades a ser ejecutadas.

Para los contratistas y/o terceros se describirán las responsabilidades y actividades en los contratos respectivos que intervienen con la Institución.

Selección de personal

Toda vinculación realizada por la E.S.E. Hospital San Jose La Celia se rige por las leyes de la Republica de Colombia y lo dispuesto en el código sustantivo del trabajo.

Todo el personal contratado por la E.S.E. Hospital San Jose La Celia debe ser seleccionado de forma que cumpla los requisites de le y debera firmar un fomata de confidencialidad y manejo de la informacion. (CARTA DE CONFIDENCIALIDAD DEL MANEJO DE LA INFORMACIÓN), de acuerdo con los requerimientos de cada cargo.

En caso que el proceso de selección o la contratación se realice por intermedio de terceros, la E.S.E. Hospital San Jose La Celia, debe asegurar la definición clara de las responsabilidades y los mecanismos para manejar el incumplimiento de los requisitos. Sin importar el método de contratación, todo funcionario recibe y acepta las políticas de seguridad de la Institución.

Términos y condiciones laborales

Todo el personal, contratista y/o tercero definido por la E.S.E. Hospital San Jose La Celia, deben regirse a las políticas de Seguridad de la Información, así como los términos de uso adecuado de los recursos de información que le son entregados, responsabilidades extensibles aún fuera de la Institución.

Todo el personal, contratista y/o tercero que tengan acceso a información sensible de la Institución o a la Infraestructura tecnológica, debe firmar, previamente a la entrega del acceso, un acuerdo de confidencialidad y no divulgación, en el que se especifique el período por el cual debe mantener el acuerdo y las acciones que se toman cuando se incumpla este requerimiento. Incluye aspectos como propiedad intelectual, protección de la información, leyes aplicables basados en las Políticas Institucionales, Políticas de Seguridad de la Información, Políticas de tratamiento protección de datos personales.

Plan de sensibilización, capacitación y comunicación sobre la seguridad de la información.

La E.S.E. Hospital San Jose La Celia, debe asegurar que todo el personal tenga definidas responsabilidades en de Seguridad de la Información, que son competentes para desempeñar sus funciones y que cuentan con los programas de capacitación y entrenamiento requeridos para ello.

De igual manera, todo el personal, contratista y tercero tendrán un proceso de concientización, mediante el cual se le capacitará sobre las políticas de seguridad de la Institución y los riesgos conocidos a los que se puede ser expuesta, en caso que estas no se cumplan a cabalidad.

Los programas de sensibilización, capacitación y comunicación, se encuentran diseñados de manera apropiada y relevante para los roles, responsabilidades y habilidades de las personas que deben asistir a ellos.

Identificación de necesidades

Ejecutivos, Administrativo y/o Asistencial

Deben conocer y entender las leyes y directivas que forman la base del programa de seguridad, también deben comprender el liderazgo que su rol tiene y que son el ejemplo a seguir de todas las demás unidades.

Personal De Seguridad

Son los asesores expertos en seguridad, deben estar bien preparados en políticas de seguridad y buenas prácticas.

Administradores de Sistemas y Personal de Soporte:

Estos funcionarios deben tener un buen nivel de preparación a nivel técnico de seguridad (implementación y prácticas de seguridad efectivas) para soportar las operaciones críticas de la entidad de manera apropiada.

Usuarios Finales:

Requieren de un alto grado de sensibilización sobre la seguridad y las reglas de comportamiento adecuadas con los sistemas de información a su disposición.

Proceso disciplinario

En el caso de identificarse un incidente de seguridad, éste será registrado en la herramienta de gestión designada, y se hará la investigación respectiva para determinar las causas y responsables; posteriormente, la E.S.E. Hospital San Jose La Celia tomará las acciones pertinentes para el personal y/o tercero vinculado con el incidente, mediante un proceso disciplinario formal de acuerdo con la naturaleza, gravedad y/o el impacto que haya podido generar a la Institución dicho incidente de acuerdo al Procedimiento: PROCEDIMIENTO DE CONTROL INTERNO DISCIPLINARIO.

Terminación o cambio de la contratación laboral

La Oficina encargada de personal y tesoreria, La Coordinacion medica de Servicios de Salud y la Gerencia, serán las encargadas de informar a las áreas implicadas en los procesos de vinculación y desvinculación, los movimientos del personal, contratista y/o tercero según los lineamientos establecidos en la E.S.E Hospital San Jose La Celia.

Responsabilidades en la terminación contractual o cambio de funciones

La Oficina encargada de personal y tesoreria, La Coordinacion medica de Servicios de Salud y la Gerencia, son los encargados del proceso de terminación de labores y asegurar que todos los activos propios de la Institución sean devueltos, los accesos físicos y lógicos sean eliminados, y la información pertinente sea transferida, de acuerdo con los procedimientos establecidos en el proceso de terminación de contrato.

En caso que un funcionario y/o tercero tenga un cambio de funciones, se debe seguir los mismos procedimientos donde se asegure la entrega de activos, el retiro de los accesos físicos y lógicos, la transferencia de información y la posterior entrega de los mismos de acuerdo a su rol.

7. GESTION DE ACTIVOS

Las diferentes áreas con el fin de garantizar la administración y control sobre los activos de la Institución, deben mantener un inventario actualizado de los activos que se encuentran dentro del alcance del modelo de gestión de seguridad de la información y que están cargados a cada proceso, el cual debe estar alineado con el inventario general de activos de información.

Asignación de Activos

En el inventario se identificará el propietario del activo, quien debe asegurar que la información y los activos asociados con su proceso están clasificados de manera apropiada, así como de establecer controles necesarios para el acceso a éstos de acuerdo con los procedimientos definidos.

Devolución de Activos

Todo el personal, contratista y/o tercero de la E.S.E Hospital San Jose de La Celia, al momento de su retiro o cambio de funciones en la Institución debe hacer entrega a su jefe inmediato del equipo que se le había asignado, con toda la información contenida en él y una relación de la misma, previó diligenciamiento de acta o formato establecido para tal fin.

Traslado de activos

Cualquier traslado de equipos de cómputo se realizará con la coordinación con el proceso de TICs previo diligenciamiento de FORMATO: SI-F-02 REGISTRO DE ACTIVOS FIJOS Y VERIFICACIÓN DE LAS CONDICIONES TÉCNICAS Y DE SEGURIDAD.

Uso aceptable de los activos

La información, archivos físicos, los sistemas, los servicios y los equipos (estaciones de trabajo, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) propiedad de la E.S.E. Hospital San Jose La Celia, son activos de la Institución y se proporcionan al personal, contratista y/o tercero autorizado, para cumplir con las funciones o actividades asignadas.

La E.S.E. Hospital San Jose La Celia podrá monitorear, supervisar y utilizar su información, sistemas, servicios y equipos, de acuerdo con lo establecido en este manual y en cualquier proceso legal que se requiera.

El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso del personal, contratistas y/o terceros determinadas por los líderes de área y Subgerencias, Oficina Asesora de Desarrollo de Servicios correspondientes.

La consulta de expedientes o documentos que reposan en las diferentes oficinas y/o áreas la E.S.E. Hospital San Jose La Celia, se permitirá en días y horas laborales, con la presencia del personal o servidor responsable de los mismos.

El personal, contratista y/o tercero se compromete a cumplir con los procedimientos establecidos para el servicio y consulta de documentos según lo definido en el proceso de Planificación y Consolidación del Sistema de Gestión Integral de Calidad y el área propietaria de la información.

Para la consulta de documentos cargados en el Software SIFAS PUNTOEXE se establecerán privilegios de acceso al personal, contratista y/o terceros de acuerdo con el desarrollo de sus funciones y competencias. Estos privilegios serán establecidos por el proceso de TICS o el líder administrador del Software.

El Jefe del área, será quien determine el carácter de reserva o restricción de los documentos físicos. Todo el personal, contratista y/o terceros que manipulen información en el desarrollo de sus funciones deberán firmar un Acuerdo de Confidencialidad de la Información Formato SI-F-03 CARTA DE CONFIDENCIALIDAD DEL MANEJO DE LA INFORMACIÓN, donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los lineamientos definidos en las Políticas de Seguridad de la Información y Políticas de tratamiento protección de datos personales y los lineamientos del presente documento. En caso de violación de la información será considerado como un incidente de seguridad y se procederá de acuerdo a lo definido al tratamiento de este tipo de incidentes.

8. ACCESO A INTERNET

No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, o que atente contra las leyes vigentes o políticas aquí establecidas.

No está permitido el acceso y el uso de servicios interactivos o mensajería instantánea que tengan como objetivo crear comunidades para intercambiar información o bien para fines diferentes a las actividades propias de la E.S.E Hospital San Jose La Celia.

No está permitido el intercambio no autorizado de información de propiedad de la E.S.E. Hospital San Jose La Celia, de sus clientes, usuarios y/o de sus funcionarios, con terceros.

No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten

contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

No está permitido la descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el proceso de TICS, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

La E.S.E. Hospital San Jose La Celia realizará monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios, contratistas y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la legislación nacional vigente.

Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

El personal, contratistas y/o terceros, no pueden asumir en nombre de la E.S.E. Hospital San Jose La Celia, posiciones personales en encuestas de opinión, foros u otros medios de comunicación externos similares.

El uso de Internet no considerado dentro de las restricciones anteriores, es permitido 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 E.S.E. Hospital San Jose La Celia.

9. CORREO ELECTRÓNICO

El correo electrónico institucional es una herramienta de comunicación o intercambio de información oficial entre personal o instituciones, no es una herramienta de difusión indiscriminada de información.

La cuenta de correo electrónico institucional debe ser usada para el desempeño de las funciones asignadas por la E.S.E. Hospital San Jose La Celia.

Los mensajes y la información contenida en los buzones de correo son propiedad de la E.S.E. Hospital San Jose La Celia y cada usuario, como responsable de su buzón debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

El tamaño de los buzones de correo es determinado por el proceso de TICS de la institución de acuerdo con las necesidades de cada usuario y previa autorización del Jefe y/o Líder del área correspondiente.

El tamaño de envío y recepción de mensajes, sus contenidos y demás características propios de estos deberán ser definidos e implementados por el proceso de TICS de la E.S.E. Hospital San Jose La Celia.

El envío de información institucional debe ser realizado exclusivamente desde la cuenta de correo bajo el dominio **@hlacelia.gov.co** y cumpliendo con las normas para el uso del correo electrónico institucional de la E.S.E. Hospital San Jose La Celia, establecidas mediante Circular emitida por la Gerencia, de la Institución. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal dentro de la Institución.

El envío masivo de mensajes publicitarios dentro de la Institución solo se deberá realizar a través de la cuenta de correo electrónico informacion**@hlacelia.gov.co**, perteneciente al área de Comunicaciones de la institución y única autorizada para tal fin, previa aprobación si se requiere por parte de la gerencia de la institución y una vez diligenciado el FORMATO CODIGO SI-F-04 SOLICITUD DE ELEMENTOS COMUNICATIVOS.

Toda información de la E.S.E. Hospital San Jose generada con los diferentes programas computacionales (Office, starOffice, Access, Wordpad, etc.), que requiera ser enviada fuera de la Institución, y que por sus características de confidencialidad e integridad deba ser protegida, debe encontrarse en membrete Institucional, en formatos no editables, utilizando las características de seguridad que brindan las herramientas proporcionadas por el proceso de TICS. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

Todos los mensajes enviados deben respetar el estándar de formato e imagen Institucional definido por la E.S.E. hospital San Jose La Celia y deben conservar en todos los casos el mensaje legar corporativo de confidencialidad y deben cumplir con la siguiente estructura.

Nombre del Funcionario
Cargo

ESE Hospital San Jose La Celia
Teléfono 3127770183, 3127770187
Carrera 02 No 5-62 La Celia- Risaralda
Colombia
Correo electrónico institucional: hospital.lacelia@risaralda.gov.co
www.hlacelia.gov.co

Los archivos que se adjuntan en los mensajes de correo en lo posible deben comprimirse para evitar la saturación en las diferentes cuentas de correo.

El usuario que tiene asignada una cuenta de correo electrónico es el único y directo responsable de todas las acciones y mensajes que se lleven a cabo en su nombre, por lo tanto, la E.S.E. Hospital San Jose La Celia no se hace responsable por lo que diga o haga. Esta información se incluirá en todos los mensajes que se envíen.

El correo electrónico Institucional es la única vía de remisión o envío de documentos de carácter administrativo interno en la E.S.E. Hospital San Jose La Celia.

Se prohíbe él envió cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Institución, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.

Se prohíbe utilizar la dirección de correo electrónico bajo el dominio **@hlacelia.gov.co** como punto de contacto en comunidades interactivas de contacto social, tales como Facebook, Twitter, Instagram, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.

El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por el proceso de TICS de la E.S.E. Hospital San Jose La Celia.

10. SISTEMA DE GESTION DOCUMENTAL

Toda la correspondencia recibida y enviada debe realizarse a través del Sistema de la ventanilla unica establecida por la E.S.E. Hospital San Jose La Celia, cumpliendo con todos los parámetros establecidos.

11. RECURSOS TECNOLÓGICOS

La instalación de cualquier tipo de software o hardware en los equipos de cómputo de la E.S.E. Hospital San Jose La Celia es responsabilidad del proceso de TICS, y por tanto son los únicos autorizados para realizar

esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por la E.S.E. Hospital San Jose La Celia a través de esta área.

Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios son realizados únicamente por el proceso de TICS.

El proceso de TICS de la E.S.E. Hospital San Jose La Celia definirá y actualizará, de manera periódica, la lista de software y aplicaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones instaladas y administradas por la E.S.E. Hospital San Jose La Celia.

En el caso de personal, contratistas y/o terceros que requieran acceso a internet mediante la red inalámbrica Wi-Fi serán conectados, previa autorización del proceso de TICS. Bajo ningún motivo se permite el acceso a la red de la E.S.E. Hospital San Jose La Celia por parte de terceros no autorizados.

La sincronización de dispositivos móviles, tales como, Tablet´s, smartphones, celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Institución, debe ser autorizado de forma explícita por el líder de la dependencia respectiva, en conjunto con el apoyo del proceso de TICS de la E.S.E. Hospital San Jose La Celia.

Las estaciones de trabajo y en general cualquier recurso de la organización no debe ser empleado para actividades recreativas, entre otras, jugar o grabar música.

El personal, contratistas y/o terceros no podrán copiar para uso personal archivos o programas de propios de la E.S.E. Hospital San Jose La Celia.

12. ACUERDOS SOBRE CONFIDENCIALIDAD

Todo el personal, contratistas y/o terceros que presten sus servicios a la E.S.E. Hospital San Jose La Celia deberán aceptar los acuerdos de confidencialidad **FORMATO CÓDIGO. SI-F-10 CARTA DE CONFIDENCIALIDAD DEL MANEJO DE LA INFORMACIÓN** definidos por la Institución, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Para los contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de la E.S.E. Hospital San Jose La Celia, a personas o entidades externas.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

Se prohíbe a todo el personal, contratistas, terceros y/o acompañantes de pacientes que ingresen o presten sus servicios a la E.S.E. Hospital San Jose La Celia la toma de fotos de la institución, incluye equipos, instalaciones, personas, etc.

El Circuito Cerrado de Televisión (CCTV) es un mecanismo de apoyo al procedimiento de seguridad de la institución; por lo tanto, sólo se tendrá acceso a las imágenes o material videográfico generado dentro de la institución, en aquellos casos en que material se requiera como prueba dentro de un proceso adelantado por autoridad civil, penal, fiscal o disciplinaria; La Gerencia de la E.S.E. Hospital San Jose La Celia será el único medio autorizado de hacer entrega de copia de grabaciones y certificación de imágenes grabadas.

13. PARTES EXTERNAS

La E.S.E. Hospital San Jose La Celia, identifica los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura tecnológica para su procesamiento por parte de los terceros, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga.

En el caso de que se requiera soporte externo se usará el **FORMATO AUTORIZACIÓN DE INGRESO SOPORTE TÉCNICO,** previo visto bueno de área usuaria y Subgerencias o la Oficina Asesora de Desarrollo de Servicios correspondiente.

los controles que se establezcan como necesarios a partir del análisis de riesgos deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos.

14. CLASIFICACIÓN DE LA INFORMACIÓN

La E.S.E. Hospital San Jose La Celia con el fin de resguardar la información que pueda ser divulgada de forma no autorizada o manipulada erróneamente por parte de personal, contratistas y/o terceros, ha establecido niveles para la clasificación de la información, incluyendo la información que puede encontrarse en medio electrónico, impreso, verbal o que sea transmitida por cualquier medio.

Toda la información de la E.S.E. Hospital San Jose La Celia debe ser identificada, clasificada y documentada de acuerdo con los criterios de clasificación establecidos por la oficina de Gestion Documental

Los niveles de clasificación de la información definidos en la E.S.E Hospital San Jose La Celia son:

Nombre del inventario de información	Área	Información confidencial	Reserva Legal	Soporte Jurídico
Informes de jurídica	Jurídica	X		Información confidencial
Derechos de petición	Jurídica	X		Información confidencial

Tutelas	Jurídica	x		Información confidencial
Procesos Jurídicos	Jurídica	X		Información confidencial
Procesos Disciplinarios	Jurídica	X		Información confidencial
Información de Historia Clínica	Archivo de Historia Clínica	X	X	La Ley 23 de 1981 y la resolución del MINSALUD de 1995 del 1999, establecen como carácter de reservado a la historia clínica.
Información Contable	Contabilidad	X	X	Ley 43 de 1990 art 63 y 64, 65, 67 Por la cual se reglamenta el ejercicio del contador público y contempla el carácter de reserva de la información que maneja.
Historia laboral del personal	Recursos Humano	X	x	**1.** Ley 1437 de 2011, artículo 24
Hojas de vida	Recursos Humano	X	X	**2.** Ley 1437 de 2011, artículo 24
expedientes pensionales	Recursos Humano	X	X	**3.** Ley 1437 de 2011, artículo 24

Nombre del inventario de información	**Área**	**Información confidencial**	**Reserva Legal**	**Soporte Jurídico**
Quejas	SIAU	X		Información confidencial
Notificaciones a entes de control de la infancia y adolescencia	Trabajo Social	X		Ley 1712 de 2014, artículo 19
Informes de aptitud ocupacional	Salud Ocupacional	X		Decreto 1443 de 2014, Resolución 1918 de 2009 –MiniSalud, Sentencia T-161 de 1993

Los criterios, niveles de clasificación y aplicación se encuentran detallados en los Lineamientos del manual MANUAL DE ADMINISTRACIÓN DE INFORMACIÓN PRIVILEGIADA Y DE RESERVA LEGAL.

Los propietarios de los activos de información son los responsables de identificar y asociar el nivel de clasificación a cada activo, teniendo en cuenta los criterios de clasificación, y su protección.

15. CONTROL DE ACCESO

Acceso Físico

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran área de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

De igual forma, los centros de cómputo, cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), especificados por los fabricantes de los equipos que albergan y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones.

Cuando se requiere el soporte técnico o mantenimiento de equipos de infraestructura tecnológica dentro de las Instalaciones de la E.S.E Hospital San Jose La Celia de bebe diligenciar el AUTORIZACIÓN DE INGRESO SOPORTE TÉCNICO, previo visto bueno del área usuaria y la persona encargada del area según corresponda.

Los funcionarios, contratistas y/o terceros de la E.S.E. Hospital San Jose La Celia, así como los visitantes, deben portar su identificación y/o carnet de manera visible durante el tiempo que permanezca dentro de las instalaciones de la Institución. En el caso de visitantes se debe portar Ficha de identificación de ingreso.

Los privilegios de acceso a las áreas seguras y restringidas de la E.S.E. Hospital San Jose La Celia deben ser periódicamente revisados, actualizados y monitoreados.

En caso de retiro o desvinculación laboral del funcionario, contratistas y/o tercero, éste debe hacer devolución del respectivo Carnet asignado en desarrollo de sus funciones, previo diligenciamiento del ACTA DE ENTREGA PUESTO DE TRABAJO para la liquidación de sus prestaciones sociales y demás obligaciones.

Usuarios y contraseñas de acceso a software y/o aplicativos

Toda contraseña asignada para acceder al sistema de información o equipo de cómputo, deberá ser asignada de manera individual, y cada usuario deberá mantenerla de manera confidencial y queda prohibido divulgarla o prestarla; el usuario es responsable por el acceso a todos los recursos informáticos que sean realizados con su usuario y contraseña.

16. SEGURIDAD FÍSICA Y DEL ENTORNO

La E.S.E Hospital San Jose La Celia, será el responsable de definir el perímetro de la seguridad física de acuerdo a la clasificación de los activos de la información, controlando el acceso a la información a través de controles (Ejemplo: acceso a áreas restringidas con tarjeta, registro de entrada de equipos, autenticación), los cuales disminuyen la posibilidad de riesgo de divulgación o pérdida de información.

Protección y disposición de los equipos

Todos equipos que hacen parte de la infraestructura tecnológica de la E.S.E. Hospital San Jose La Celia tales como servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan o brinden servicios de soporte a la información crítica de las áreas, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, agua, polvo, vandalismo, entre otros.

El personal, contratista y/o tercero, que tenga acceso a los equipos que componen la infraestructura tecnológica de la E.S.E Hospital San Jose La Celia no pueden fumar, beber o consumir algún tipo de alimento que atente contra la integridad de los mismos.

Todo personal, contratistas y/o terceros que note algún problema de funcionamiento o ataque de virus en una estación de trabajo debe reportarlo de inmediato al correo electrónico: **sistemas@hlacelia.gov.co** de la E.S.E. Hospital San Jose La Celia.

La E.S.E. Hospital San Jose La Celia debe proveer suministros y equipamiento de soporte como electricidad, planta eléctrica y un sistema de alimentación no interrumpida (UPS) que asegure el tiempo necesario para apagar adecuadamente los servidores donde se alojan los sistemas de información ante una falla en el suministro de cualquiera de estos elementos, evitando así la pérdida o corrupción de información. Estos suministros deben ser monitoreados, revisados y medidos permanentemente para asegurar su funcionamiento y condiciones normales de operación y evitar futuros daños.

De igual forma, la E.S.E. Hospital San Jose La Celia, debe establecer un programa de planeación y ejecución de mantenimientos preventivos, a la infraestructura tecnológica.

Ningún empelado, contratistas o tercero podrá desarmar o destapar equipos sin previa autorización del proceso de TICS.

Seguridad de los equipos y medios de información fuera de la Institución

Independientemente del propietario, todos los funcionarios son responsables de velar por la seguridad de los equipos de la E.S.E Hospital San Jose La Celia, que se encuentren fuera de las instalaciones de la Institución.

• Bajo ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista, en el caso que esté siendo transportado en un vehículo.

• Los equipos de infraestructura de la E.S.E. Hospital San Jose La Celia, deben ser transportados con las medidas de seguridad apropiadas, que garanticen la integridad física de los dispositivos.

• Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

• Los equipos de la E.S.E. Hospital San Jose La Celia deberán contar con un seguro que los proteja de robo.
• En caso de pérdida o robo de un equipo de la E.S.E. Hospital San Jose La Celia, se deberá informar inmediatamente al correo electrónico: sistemas@hlacelia.gov.co, para que se inicie el trámite interno y se deberá poner la denuncia ante la autoridad competente.

• El retiro de equipos de cómputo, periféricos, dispositivos de almacenamientos, software e información considerada crítica propiedad de la E.S.E. Hospital San Jose La Celia, fuera de las instalaciones de la Institución debe seguir los procedimientos establecidos por el proceso de TICS.

Eliminación o reutilización segura de equipos y medios

La E.S.E Hospital San Jose La Celia, debe identificar los riesgos potenciales que puede generar destruir, reparar o eliminar equipos y medios de almacenamiento. Para ello, debe definir e implementar los mecanismos y controles adecuados para que la información sensible contenida en ellos sea eliminada de manera segura Cuando un equipo sea reasignado o dado de baja, se deberá realizar el proceso de acuerdo al Procedimiento Baja de Activos Fijos y Formato de Activos Fijos Para dar de Bajas.

17. SEGURIDAD DE LAS COMUNICACIONES Y OPERACIONES

Documentación de procedimientos operativos

Se debe contar con procedimientos, registros e instructivos de trabajo debidamente documentados y actualizados, con el fin de asegurar el mantenimiento y operación adecuada de la infraestructura tecnológica de la E.S.E Hospital San Jose La Celia. Cada procedimiento debe tener un responsable para su definición y mantenimiento y debe garantizar la disponibilidad del mismo.

Control de Cambios

Todo cambio que se realice sobre la infraestructura tecnológica para el procesamiento de la información, comunicaciones y seguridad electrónica debe ser controlado, gestionado y autorizado adecuadamente, y debe ser sometido a una evaluación que permita identificar los riesgos, que pueden afectar la operación del negocio de acuerdo con los lineamientos establecidos.

Los cambios estructurales que se planteen realizar sobre las plataformas críticas deben ser revisados por el Comité de Seguridad de la Información, el cual debe establecer los requerimientos de seguridad necesarios

conforme a las políticas establecidas por la E.S.E Hospital San Jose La Celia, que tengan como fin evitar un impacto adverso en las operaciones del negocio.

La Gestión de Cambios debe contener como mínimo la identificación, justificación y evidencia de los cambios que se vayan a realizar sobre la infraestructura tecnológica, el alcance, autorización, el plan de trabajo para la definición de pruebas funcionales, responsabilidades definidas, la evaluación apropiada sobre el impacto potencial que estos pueden generar, un plan alternativo para abortar cambios no satisfactorios (Rollback), eventos imprevistos y cualquier otro aspecto que se considere importante por los responsables del cambio.

Segregación de funciones

Toda tarea en la cual el personal tengan acceso a la infraestructura tecnológica y a los sistemas de información, debe contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la Institución.

Todos los sistemas de disponibilidad crítica o media de la Institución, en lo posible, deben implementar las reglas de acceso de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

Separación de los ambientes de desarrollo, prueba y producción

La E.S.E Hospital San Jose La Celia, ha definido diferentes ambientes para la ejecución de actividades de desarrollo, pruebas y puesta en producción de sus aplicaciones de negocio, con el fin de garantizar la integridad de la información procesada y evitar interferencias en el desempeño y seguridad de cada uno de los ambientes.

Dado lo anterior, los ambientes establecidos por la E.S.E Hospital San Jose La Celia se definen así:

Ambiente de Desarrollo: Conjunto de elementos de hardware y software como compiladores, editores, instaladores de lenguajes de programación, donde residen todos los recursos informáticos necesarios para efectuar tareas relacionadas con la generación o modificación de aplicaciones, entre otros.

Ambiente de Pruebas: Conjunto de elementos de hardware y software que soportan los sistemas de información utilizados para verificar la funcionalidad de los desarrollos de software y aplicativos para realizar los ajustes necesarios antes de ser puestos en funcionamiento en el ambiente de producción de la E.S.E. Hospital San Jose La Celia.

Ambiente de Producción: Conjunto de elementos de hardware y software que soportan los sistemas de información utilizados por los funcionarios para la ejecución de las operaciones de la E.S.E. Hospital San Jose La Celia. En este ambiente deben residir aplicaciones en producción, bibliotecas o directorios que contengan archivos de datos, base de datos, programas ejecutables o compilados.

A través de las políticas de control de acceso físico y lógico definidas por la Institución, se controla el acceso a cada uno de los ambientes. Adicionalmente, los ambientes de desarrollo, pruebas y producción están totalmente separados, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros dos ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.

El proceso de TICS debe proveer los mecanismos, controles y recursos necesarios para tener niveles adecuados de separación física y lógica entre los ambientes de desarrollo, pruebas y producción para toda su plataforma tecnológica, con el fin de reducir el acceso no autorizado y evitar cambios inadecuados.

Igualmente debe asegurar, mediante los controles adecuados, que los usuarios utilicen diferentes perfiles para el ambiente de desarrollo, pruebas y de producción, así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.

Gestión de la capacidad

La E.S.E. Hospital San Jose La Celia, mantendrá un proceso continuo de monitoreo, análisis y evaluación del rendimiento y capacidad de su infraestructura tecnológica de procesamiento de información, con el fin de identificar y controlar el consumo de sus recursos y prever su crecimiento de forma planificada.

Periódicamente, se realizarán mediciones de las variables críticas de operación de la infraestructura tecnológica con el objetivo de verificar el estado y uso de los recursos. De esta forma, es posible definir proyecciones de crecimiento que aseguren la integridad de procesamiento y disponibilidad de la infraestructura.

Los resultados de dichas mediciones serán analizados y presentados al Comité de Seguridad de la Información y/o Comité de Gobierno en Línea y en caso de ser necesario la adquisición de nuevos recursos o elementos para soportar la demanda, se proceda a planificar la consecución de dichos elementos previa autorización de la alta dirección.

Aceptación de sistemas

El proceso de TICS debe asegurar que los requerimientos y criterios, tanto funcionales como técnicos, para la aceptación de nuevos sistemas, actualizaciones y nuevas versiones de software estén claras y adecuadamente definidos, documentados y aprobados acordes a las necesidades de la E.S.E. Hospital San Jose La Celia. Estos nuevos requerimientos, actualizaciones y/o nuevas versiones de tecnología, sólo deben ser migrados al ambiente de producción después de haber sido formalmente aceptados de acuerdo a las necesidades técnicas y funcionales establecidas.

Todo sistema que se implemente o instale en la E.S.E. Hospital San Jose La Celia, sea comprado o en comodato, debe tener la capacidad de integrarse al sistema corporativo y será evaluado por el proceso de TICS para verificar su buen funcionamiento y los procedimientos de mantenimiento y soporte.

Protección contra software malicioso

La E.S.E. Hospital San Jose La Celia, velará porque todos los recursos informáticos esten protegidos mediante herramientas y software de seguridad como Antivirus, Antispam, Antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red institucional, en donde se cuente con los controles para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso. Será responsabilidad del proceso de TICS autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente.

Así mismo, la E.S.E. Hospital San Jose La Celia define, que bajo ningún motivo está permitido:

• La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por el proceso de TICS.

• Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.

Copias de Respaldo

La E.S.E. Hospital San Jose La Celia, debe asegurar que la información con cierto nivel de clasificación, definida en conjunto con el proceso de TICS y las áreas responsables de la misma, contenida en la plataforma tecnológica de la Institución, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad.

• Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

• El proceso de TICS establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con las dependencias los períodos de retención de la misma. Además, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

• Los medios magnéticos que contienen la información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados, cumplir con máximas medida de protección y seguridad física apropiados.

Es responsabilidad de todo funcionario realizar periódicamente una copia de seguridad de la información almacenada en el disco duro del equipo que le fue asignado, para ello solicitará al proceso de TICS los medios necesarios, los cuales entregará para que sean resguardados de acuerdo con las medidas de protección y seguridad física apropiados.

Gestión de medios removibles

El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias Flash, discos duros externos, Ipods, celulares, cintas) sobre la infraestructura para el procesamiento de la información de la E.S.E Hospital San Jose La Celia, estará autorizado para aquellos funcionarios cuyo perfil de cargo y funciones lo requiera, con supervisión de su administrador de sistemas.

El proceso de TICS es responsable de implementar los controles necesarios para asegurar que en los sistemas de información de la E.S.E Hospital San Jose La Celia, los funcionarios autorizados pueden hacer uso de los medios de almacenamiento removibles. Así mismo, el funcionario se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información de la Institución.

Intercambio de información

La E.S.E Hospital San Jose La Celia firmará acuerdos de confidencialidad con los funcionarios, clientes y/o terceros que por diferentes razones requieran conocer o intercambiar información restringida o confidencial de la Institución CARTA DE CONFIDENCIALIDAD DEL MANEJO DE LA INFORMACIÓN. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deber firmar antes de permitir el acceso o uso de dicha información.

Todo funcionario de la E.S.E Hospital San Jose La Celia es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada, cuyo uso aceptable se especifica en el presente manual "Uso aceptable de los activos".

Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad y requeridos.

En todo caso no se permite el acceso al equipo y/o datos de otro funcionario a través de la red sin el consentimiento de éste.

18. RELACION CON LOS PROVEEDORES

Todos los proveedores que por actividades internas tengan un contrato con la E.S.E Hospital San Jose de La Celia, deberán acogerse a los siguientes lineamientos:

• Todo proveedor deberá cumplir con los lineamientos de seguridad de la información establecidos en E.S.E Hospital San Jose La Celia, así mismo como con la normatividad definida en sus procesos internos.

19. EVALUACIÓN

La E.S.E. Hospital San Jose La Celia debe realizar la evaluación periódica de los riesgos inherentes a la gestión y seguridad de la información, para lo cual se apoyará en metodologías y documentos, estructurados y aceptados, que avalen la adecuada gestión de la Información.

La E.S.E. Hospital San Jose La Celia debe evaluar los riesgos identificados y la tolerancia al riesgo, para determinar su tratamiento y documentación en un Plan de Tratamiento de Riesgos.

20. REFERENCIAS BIBLIOGRAFICAS

Procedimientos De Seguridad de La Información
https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

Guía para la Gestión y Clasificación de Activos de Información
http://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

Plan de Capacitación, Sensibilización Y Comunicación De Seguridad De La Información
http://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.
http://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Modelo de Seguridad y Privacidad de la Información
http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Código Penal Colombiano
http://perso.unifr.ch/derechopenal/assets/files/legislacion/l_20130808_01.pdf

Código de Policía
http://static.elespectador.com/archivos/2017/02/ddaded47db60946fd9e1e59cec13710d.pdf

21. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS			
Versión	**Fecha**	**Elaboro**	**Descripción del cambio**
00	07/07/2020	Duvanier Alvarez Posada	Versión Original