CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO
CEFIT

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EL CENTRO DE FORMACION INTEGRAL PARA EL TRABAJO CEFIT

ENVIGADO ANTIOQUIA
2019

TÍTULO	**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**
Nombre de la Institución	CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT
Fecha de aprobación	Resolución 161 de junio 20 de 2019
Instancia de aprobación	El Comité Institucional de Gestión y desempeño.
Responsable	Profesional universitario sistemas
Sumario	Este documento presenta las estrategias
Palabras claves	SEGURIDAD DE LA INFORMACIÓN
Formato	PDF - DOC
Responsable de su elaboración:	CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT
Fecha de publicación	Junio 20 del año 2019

1Justificación

El CENTRO DE FORMACION INTEGRAL PARA EL TRABAJO CEFIT determina la información como un activo valioso que debe ser protegido para garantizar la continuidad de la operación de la institución además de generar confianza entre las partes interesadas, a medida que los sistemas de información se convierten en herramientas críticas para el procesamiento de datos se identifica la necesidad de contar con estrategias que permitan el control y administración efectiva de los datos almacenados en ellos y en los demás activos de información.

Con la promulgación de la presente Política de Seguridad de la Información El CENTRO DE FORMACION INTEGRAL PARA EL TRABAJO CEFIT formaliza su compromiso con el proceso de gestión responsable de información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos misionales.

1 Glosario

Seguridad de la información: se entiende como la preservación, aseguramiento y cumplimiento de las siguientes características de la información:

Confidencialidad: los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.

Integridad: El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.

Disponibilidad: Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.

Autenticidad: Los activos de información los crean, editan y custodian usuarios reconocidos quienes validan su contenido.

Posibilidad de Auditoría: Se mantienen evidencias de todas las actividades y acciones que afectan a los activos de información.

Protección a la duplicación: Los activos de información son objeto de clasificación, y se llevan registros de las copias generadas de aquellos catalogados como confidenciales.

No repudio: Los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.

Legalidad: Los activos de información cumplen los parámetros legales, normativos y estatutarios de la institución.

Confiabilidad de la Información: Es fiable el contenido de los activos de información que conserven la confidencialidad, integridad, disponibilidad, autenticidad y legalidad. Datos o información propiedad de la Universidad que

2 Política General de Seguridad de la Información

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración del CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

El CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT
- Garantizar la continuidad del negocio frente a incidentes.

2.1 Alcance

Esta política aplica a toda la institución, sus procesos, sus funcionarios, contratistas, terceros del CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT y la ciudadanía en general.

2.2 Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar

cumplimiento un 100% de la política.

A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI del CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT:

El CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

El CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.

El CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

El CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO protegerá su información de las amenazas originadas por parte del personal.

El CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

El CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

El CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO implementará control de acceso a la información, sistemas y recursos de red.

El CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

El CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

El CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.

El CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

3 Políticas específicas de Seguridad de la Información

3.1 Organización para la Seguridad de la Información

El CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información, del cual hace parte integral la presente política, por medio de la creación de una comisión técnica denominada Comité de Gestión y Desempeño cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

- Directora
- Jefe oficina académica
- Asesor planeación
- Asesora jurídica
- PU Sistemas

En todo caso, dicho comité, deberá revisar y actualizar anualmente esta política presentando las propuestas a la alta dirección de la institución para su aprobación mediante resolución o acto jurídico correspondiente.

Los líderes o gestores de procesos, previa identificación y valoración de sus activos de información, hacen parte del grupo de responsables de Seguridad de la Información y por tanto deben seguir los lineamientos de gestión enmarcados en

esta política y en los estándares, normas, guías y procedimientos recomendados por el Comité de Seguridad de la Información y aprobados por las directivas.

Roles y Responsabilidades

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal del CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

El Comité de Gestión y Desempeño es responsable de revisar y proponer a la alta dirección las modificaciones para su aprobación, el texto de la Política de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora del Sistema de Gestión de Seguridad de la institución. Es responsabilidad de dicho comité definir las estrategias de capacitación en materia de seguridad de la información al interior de la institución.

El Coordinador del Comité de Gestión y Desempeño será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento de la presente Política.

Los propietarios de activos de información (ver su definición en el glosario) son responsables de la clasificación, mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

El jefe de Recursos Humanos cumplirá la función de notificar a todo el personal que se vincula contractualmente con la institución, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación de la presente Política y de los cambios que en ella se produzcan a todo el personal, a través de la suscripción de los Compromisos de Confidencialidad y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por el Comité de Gestión y Desempeño.

Los supervisores de sistemas de información en coordinación con los proveedores

de software deben seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información y los recursos de tecnología de la entidad.

Corresponde a los líderes y gestores de los procesos a determinar el inventario de activos de información y recursos tecnológicos de los cuales son propietarios o custodios, el cual será revisado y avalado por el Comité de Gestión y Desempeño.

La asesora jurídica verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la entidad con empleados y con terceros. Asimismo, asesorará en materia legal a la entidad en lo que se refiere a la seguridad de la información.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.

3.2 Seguridad de la información en el Recurso Humano

Todo el personal del CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT, cualquiera sea su situación contractual, el área a la cual se encuentre adscrito y el nivel de las tareas que desempeñe debe tener asociado un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. El PU de Sistemas debe mantener un directorio completo y actualizado de tales perfiles.

Se debe capacitar y sensibilizar a los funcionarios durante la inducción sobre las políticas de seguridad de la información.

Se debe asegurar que los funcionarios, contratistas y demás colaboradores del CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT, adopten sus responsabilidades en relación con las políticas de seguridad de la información de la institución y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información, el conocimiento de las políticas de seguridad de la información se notificaran mediante el diligenciamiento y firma del formato de inducción .

En situaciones de incumplimiento y/o violaciones a las políticas de seguridad de la información se deberá tramitar el cumplimiento de la ley 734 de 2013, ley 200 de

1995 y demás normas que reglamenten los procesos disciplinarios para los empleados del estado.

Actualmente los usuarios que tienen cuenta de usuario de la entidad, pueden realizar el cambio de su fotografía para el chat y correo electrónico institucional, de tal forma que al realizar la inclusión y/o cambio de fotografía, al ser considerada un dato sensible, “una foto contiene la imagen de una persona, la cual es un dato biométrico” el titular está dando su aprobación, en cuanto al tratamiento de sus datos personales de acuerdo a la Ley Estatutaria 1581 de 2012 y el decreto 1377 de 2013.

El funcionario o contratista debe entregar los activos de información de acuerdo al Informe de entrega o el Informe final de supervisión el cual deberá ser verificado por el supervisor del contrato.

3.3 Gestión de Activos

3.3.1 Identificación de activos de información.

Cada área, debe elaborar y mantener un inventario de los activos de información que poseen (procesada y producida) y este deberá ser actualizado cada 6 meses después de su creación. Las características del inventario, donde se incorpore la identificación, clasificación, valoración, ubicación y acceso de la información, las especifica el Comité de Gestión y Desempeño, correspondiendo al PU Sistemas brindar herramientas que permitan la administración del inventario por cada dependencia, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

El PU sistemas tiene la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la institución.

3.3.2 Clasificación de Activos.

Cada área debe clasificar sus activos de información según el nivel de criticidad del activo, sensibilidad y reserva de la información teniendo en cuenta las leyes vigentes respecto a la protección y privacidad de la información y los lineamientos establecidos en el Sistema de Gestión Documental.

3.3.3 Devolución de Activos

Finalizadas las actividades que le corresponde a cualquier de los funcionarios vinculados, contratistas, docentes o proveedores, estos deberán realizar la entrega

de los activos de información que haya producido o gestionado durante el desempeño de sus funciones, el responsable de ejecutar esta actividad cuando se trate de personal vinculado o docentes será el líder de Gestión Humana, en caso de tratarse de contratistas el supervisor y para los docentes será el jefe de oficina académica el encargado de verificar la entrega de los activos de información, esta actividad se debe ejecutar con el respaldo del PU Sistemas y el almacenista general, para verificar la ubicación e disponibilidad de los activos.

3.3.4 Medios y equipos

La entidad establece actividades para evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados por El CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT, velando por la disponibilidad y confidencialidad de la información.

Los medios y equipos donde se almacena, procesan o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

El servicio de acceso a Internet, Intranet, Sistemas de información, medio de almacenamiento, aplicaciones (Software), cuentas de red, navegadores y equipos de cómputo son propiedad de la Entidad y deben ser usados únicamente para el cumplimiento de la misión de la Entidad.

El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.), pueden ocasionalmente generar riesgos para la entidad al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información o pudiera extraviarse junto con los activos que contenga. Los usuarios deberán contar con la autorización de la alta dirección para usar este tipo de dispositivos y serán responsables por los daños o perjuicios que se puedan generar por no tener las precauciones suficientes para evitar la pérdida o fuga de información y serán completamente responsables por los daños causados al activo afectado.

3.3.5 Copias de seguridad en estaciones de trabajo usuario final

Asegurar la operación de realización de copias de información en estaciones de trabajo incluidas en el inventario de activos de información una vez a la semana.

La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información y solicitadas a través de la herramienta de gestión de requerimientos establecida por entidad.

Los medios que vayan a ser eliminados o que cumplan el periodo de retención deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

Todos los mensajes son sujetos a análisis frente a amenazas y ataques dirigidos, y pueden ser conservados, puestos en cuarentena y/o eliminados permanentemente por parte de la Entidad.

3.3.6 Redes Sociales

El CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT define las pautas generales para asegurar una adecuada protección de la información en el uso del servicio de las redes sociales, por parte de los usuarios autorizados.

La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador del CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT, que sea creado a nombre personal en redes sociales como: Twitter, Facebook, YouTube LinkedIn, Blogs, Instagram, etc. se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

Toda información distribuida en las redes sociales institucionales que sea originada por la entidad, debe ser autorizada por la PU Comunicaciones y con un vocabulario institucional.

No se debe utilizar el nombre de la entidad en las redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la institución.

3.3.7 Tercerización de servicios

Mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas.

Se deben establecer criterios de selección que contemplen la experiencia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes,

estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad.

Se debe establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información del CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT, las cuales deben se divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.

En los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad de la información

Los contratistas, oferentes y/o proveedores deben aceptar y firmar el acuerdo de confidencialidad establecido por el CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT.

El PU Sistemas deberá mitigar los riesgos de seguridad con referencia al acceso de los proveedores y/o contratistas a los sistemas de información del CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT.

Se debe identificar y monitorear los riesgos relacionados con los contratistas o proveedores en relación a los objetos contractuales, incluyendo la cadena de suministro de los servicios de tecnología y comunicación.

Se deben identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas al CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT. El resultado del análisis de riesgos será la base para el establecimiento de los controles.

Los funcionarios del CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT que cumplen como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas.

Se deben establecer mecanismos o condiciones con los contratistas o proveedores que permitan realizar la gestión de cambios en los servicios suministrados.

3.4 Control de acceso

La Entidad define las reglas para asegurar un acceso controlado, físico o lógico, a la información y plataforma informática del CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT, considerándolas como importantes para el SGSI.

La conexión remota a la red de área local del CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT debe realizarse a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada, por el Área de Sistemas.

3.4.1 Control de acceso con usuario y contraseña

El acceso a información restringida debe estar controlado. Se recomienda el uso de sistemas automatizados de autenticación que manejen credenciales o firmas digitales.

Ningún usuario deberá acceder a la red o a los servicios TIC del CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT, utilizando una cuenta de usuario o clave de otro usuario.

3.4.2 Suministro del control de acceso

El CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT suministrará a los usuarios a través del área de Gestión Humana las claves respectivas para el acceso a los servicios de red, equipos de cómputo, correo electrónico y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.

3.4.3 Gestión de contraseñas

El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta, comunicándose al área de Sistemas en donde se llevará a cabo la validación de los datos personales; en caso de ser solicitado el cambio de contraseña para otra persona, debe ser realizada por su supervisor o líder de procesos previa autorización por parte de la directora.

Las contraseñas referentes a las cuentas “predefinidas” incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas. De no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.

3.4.4 Parámetros de seguridad

Las claves o contraseñas deben:

Tener mínimo ocho (8) caracteres alfanuméricos.

La contraseña debe cumplir con tres de los cuatro requisitos:

- Caracteres en mayúsculas
- Caracteres en minúsculas
- Base de 10 dígitos (0 a 9)
- Caracteres no alfabéticos (Ejemplo: ¡,$,%,&)

3.5 Privacidad y confidencialidad

Con el fin de garantizar la privacidad y confidencialidad de la información el CENTRO DE FORMACION INTEGRAL PARA EL TRABAJO CEFIT establecerá controles para evidenciar la autorización por parte de los usuarios para el tratamiento de los datos personales y les informara lo fines para los cuales estos son solicitados y dispondrá los medios para que estos sean actualizados, modificados, eliminados según su solicitud según lo dispuesto en la ley 1581 de 2012 y el decreto 1377 de 2013, además el CENTRO DE FORMACION INTEGRAL PARA EL TRABAJO CEFIT firmara acuerdos de confidencialidad de la información con terceros para la protección de la propiedad intelectual y la protección de los datos en caso de tener que suministrarlos para el logro de los objetivos institucionales.

3.6 Integridad

Toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información En el caso de vinculación contractual, el Compromiso de administración y manejo integro e integral de la información interna y externa hará parte de las cláusulas del respectivo contrato, bajo la denominación de Cláusula de integridad de la información.

3.7 Registro y auditoria

3.7.1 Responsabilidad

La Oficina de Control Interno es responsable de gestionar con la alta dirección las auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información. Es su responsabilidad informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

3.7.2 Almacenamiento de registros

El PU Sistemas es responsable de implementar y documentar los registros de las copias de seguridad realizadas en estaciones de trabajo de usuario final y servidores, además llegar registro de los incidentes de seguridad que se detecten durante la gestión.

3.7.3 Normatividad

- 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 2693 de 2012: Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, 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 1437 de 2011: Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo

- 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 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.
- Ley 1150 DE 2007: Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos.
- NTC 27001:2013: Sistema de Gestión de Seguridad de la Información (SGSI).
- Ley 599 DE 2000: Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa.
- Decreto 1078 de 2015 Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- 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.

3.8 Capacitación y sensibilización en seguridad de la información

La alta dirección se compromete a destinar recursos suficientes para el desarrollo de programas de capacitación en temas relacionados con la seguridad de la información para funcionarios, docentes y contratistas con el fin de disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano.

El CENTRO DE FORMACIÓN INTEGRAL PARA EL TRABAJO CEFIT gestionara capacitación para el personal administrativo y contratistas respecto a los temas relacionados a la seguridad de la información y sensibilizara al personal docente para mitigar los riesgos de seguridad de la información.

Los programas de capacitación ejecutados deberán ser periódicamente evaluados con el fin de determinar el mejoramiento de los procesos.

El personal capacitado se comprometerá a aplicar los conocimientos adquiridos en los programas de sensibilización y entrenamiento para el aseguramiento de la información.