EMPRESA SOCIAL DEL ESTADO
PASTO SALUD
Nit. 900091143-9

MANUAL DE GESTIÓN DE SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN

VERSION 2.0

San Juan de Pasto
2015

MANUAL DE GESTION DE SERIDAD INFORMATICA Y SEGURIDAD DE LA INFORMACION
PASTO SALUD E. S. E.

ELABORADO POR:

EQUIPO OFICINA ASESORA DE COMUNICACIONES Y SISTEMAS

San Juan de Pasto
2015

CONTENIDO

RESOLUCIÓN NO. 0180 DE 15 DE MAYO DE 2015.

EMPRESA SOCIAL DEL ESTADO PASTO SALUD Nit. 900091143-9	ACTOS ADMINISTRATIVOS			
	VERSIÓN	PROCESO / PROCEDIMIENTO	CODIGO	NUM
	2.0	GESTION JURIDICA	GJ	062
	GERENCIA			

RESOLUCION No. 0180
(15 de mayo de 2015)

"Por la cual se deroga la Resolución No. 2728 del 01 de diciembre de 2011 y se aprueba el Manual de Gestión de Seguridad Informática y Seguridad de la Información versión 2.0 de la Empresa Social del Estado PASTO SALUD E.S.E".

El Gerente de la Empresa Social del Estado Pasto Salud ESE, en uso de sus atribuciones legales, en especial las conferidas en el Acuerdo No. 004 del 13 de febrero de 2006 del Concejo Municipal de Pasto, el Acuerdo Nº. 018 del 26 de abril de 2007 de la Junta Directiva de la Empresa Social del Estado PASTO SALUD E.S.E., el Decreto 0512 del 26 de julio de 2012 y,

CONSIDERANDO:

Que el artículo 61 de la Constitución Política de Colombia, establece: "*El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley*".

Que es deber de la Empresa Social del Estado PASTO SALUD E.S.E., garantizar la prestación de servicios de salud bajo condiciones de calidad, de tal manera que satisfagan las expectativas de los pacientes y usuarios en general.

Que la Ley 1273 de 2009, modifica el Código Penal, crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y preserva integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

Que las Ley 23 de 1982, modificada por la Ley 44 de 1993 y sus Decretos Reglamentarios, establecen los derechos de autor y de propiedad intelectual.

Que el Decreto 1011 de 2006 del Ministerio de la Protección Social, por el cual se establece el Sistema Obligatorio de Garantía de la Calidad de la Atención en salud del Sistema General de Seguridad Social en Salud, determina los requisitos básicos de estructura y procesos que deben cumplir los Prestadores de Servicios de Salud.

Que mediante Resolución 2728 de diciembre de 2011, se aprobó y adoptó el Manual de Gestión de Seguridad Informática y Seguridad de la Información Versión 1.0 para la Empresa Social del Estado PASTO SASLUD E.S.E.

Que se hace necesario actualizar el Manual de Gestión de Seguridad Informática y Seguridad de la Información, con el objeto de establecer responsabilidades derivadas del uso de los recursos tecnológicos de la Empresa Social del Estado PASTO SALUD E.S.E., con el objetivo de garantizar la eficiencia, confiabilidad, consistencia, integridad y oportunidad de la información y la efectividad de los controles de seguridad en los sistemas de información.

En mérito de lo expuesto,

RESUELVE

ARTÍCULO PRIMERO: Deróguese la Resolución Interna No. 2728 del 01 de diciembre de 2011 que aprobó y adoptó el Manual de Gestión de Seguridad Informática y Seguridad de la Información Versión 1.0 para la Empresa Social del Estado PASTO SALUD E.S.E.

ARTÍCULO SEGUNDO: Apruébese y adóptese el Manual de Gestión de Seguridad Informática Versión 2.0 para la Empresa Social del Estado PASTO SALUD E.S.E., cuyo documento anexo a la presente Resolución forma parte integral y constitutiva de la misma.

EMPRESA SOCIAL DEL ESTADO PASTO SALUD Nit. 900091143-9	ACTOS ADMINISTRATIVOS			
	VERSIÓN	PROCESO / PROCEDIMIENTO	CODIGO	NUM
	2.0	GESTION JURIDICA	GJ	062
	GERENCIA			

ARTICULO TERCERO: El Manual de Gestión de Seguridad Informática Versión 2.0 de la Empresa Social del Estado PASTO SALUD E.S.E., será divulgado por la Oficina Asesora de Comunicaciones y Sistemas de la Empresa.

ARTÍCULO SEXTO: VIGENCIA: La presente resolución rige a partir de la fecha de su expedición y deroga la Resolución No. 2728 del 01 de diciembre de 2011.

PUBLIQUESE, COMUNÍQUESE Y CÚMPLASE

BERNARDO OCAMPO MARTINEZ

Proyectó: David Insuasti, Oficina Asesora de Comunicaciones

Revisó: David Cruz, Oficina Asesora Jurídica
J. Rosero, Profesional Universitario

CONTROL DE CAMBIOS

E: Elaboración del Documento

M: Modificación del Documento

X: Eliminación del Documento

VERSIÓN	CONTROL DE CAMBIOS AL DOCUMENTO	INFORMACIÓN DE CAMBIOS					ACTO ADMINISTRATIVO DE ADOPCIÓN
		E	M	X	ACTIVIDADES O JUSTIFICACIÓN	ELABORÓ /ACTUALIZÓ	
2.0	Actualización del Manual de Gestión de Seguridad Informática y Seguridad de la Información		X		Justificación: La implementación de nuevas herramientas informáticas y lineamientos sobre recursos informáticos dentro de Pasto Salud E.S.E que apoyan los procesos organizacionales hacen necesario la actualización del presente documento.		Resolución No. 0180 del 15 de Mayo de 2015
1.0	Elaboración del Documento Manual de Gestión de Seguridad Informática y Seguridad de la Información	X			Justificación: La alta gerencia de la Empresa Social del Estado Pasto Salud, apoya los objetivos y principios de la seguridad informática y de la información para lo cual determina el obligatorio conocimiento y cumplimiento de la reglamentación y políticas de seguridad informática de la entidad, las cuales están consignadas en el presente manual.		Resolución No. 2728 del 1 de Diciembre de 2012

INTRODUCCION

El propósito de un sistema de gestión de la seguridad informática y de la información es, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un Sistema de Gestión de Seguridad Informática y de la Información.

CONCEPTOS GENERALES

1.1 ¿QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN?

La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

La seguridad de la información se caracteriza aquí como la preservación de:

a) **su confidencialidad**, asegurando que sólo quienes estén autorizados pueden acceder a la información;

b) **su integridad**, asegurando que la información y sus métodos de proceso son exactos y completos;

c) **su disponibilidad**, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

1.2 ¿PORQUÉ ES NECESARIA LA SEGURIDAD DE INFORMACIÓN?

La información y los procesos que la apoyan, sistemas y redes son importantes activos de la organización. La disponibilidad, integridad y confidencialidad de la información pueden ser esenciales para mantener su competitividad, rentabilidad, cumplimiento de la legalidad e imagen comercial.

Las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y

ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

La dependencia de los sistemas y servicios de información implica que las organizaciones son más vulnerables a las amenazas a su seguridad. La dificultad de conseguir el control de los accesos se incrementa al interconectar las redes públicas con las privadas y al compartir los recursos de información. La tendencia hacia la informática distribuida debilita la eficacia de un control central y especializado.

Muchos sistemas de información no se han diseñado para ser seguros. La seguridad que puede lograrse a través de los medios técnicos es limitada, y debería apoyarse en una gestión y unos procedimientos adecuados. La identificación de los controles que deberían instalarse requiere una planificación cuidadosa y una atención al detalle. La gestión de la seguridad de la información necesita, como mínimo, la participación de todos los empleados de la organización. También puede requerir la participación de los proveedores, clientes o accionistas. La asesoría especializada de organizaciones externas también puede ser necesaria.

Los controles sobre seguridad de la información son considerablemente más baratos y eficaces si se incorporan en la especificación de los requisitos y en la fase de diseño.

1.3 GENERALIDADES SOBRE SEGURIDAD INFORMÁTICA.

Se define los sistemas de información como “el conjunto de recursos (datos, personas, instalaciones, equipamientos y software) que en forma coordinada y alineada a una estrategia institucional, proporcionan soporte a la operación, a la toma de decisiones y al servicio de los usuarios de la organización como a sus clientes”

La información provista y las tecnologías de la información (TI) que los soportan, representan inversiones valiosas para PASTO SALUD ESE, por lo que la administración priorizó las expectativas respecto a la función de las áreas de servicios informáticos, como áreas de soporte a las funciones del la Organización y sujeto de control sobre sus responsabilidades y bienes asignados, para lograr incrementar la productividad, funcionalidad y facilidad de uso, disminuyendo el tiempo de entrega, y aumentando continuamente los niveles de servicio en el paradigma de la calidad, con la premisa que todo esto se logre con menores costos y con la administración de los riesgos asociados a la implementación de nuevas tecnologías de información.

Toda organización se encuentra sometida a amenazas o peligros de diversos orígenes, desde un posible incendio casual o intencional hasta la defraudación, pasando por la más común de las amenazas; el error u omisión cometidos por las personas en el normal desenvolvimiento de sus tareas.
Las organizaciones **pueden estar o no ordenadamente preparadas** para enfrentar los peligros o amenazas latentes. Este aspecto es el que en Pasto Salud E.S.E. denominamos **vulnerabilidad** y representa las **debilidades** que la organización presenta frente a cada una de las eventuales amenazas.

Por los motivos expuestos, los responsables de los sistemas de información y sus tecnologías relacionadas, como así los responsables de la función servicios informáticos, necesitan tener el conocimiento de las nuevas amenazas a que se ven sometidos los organismos por el uso de las tecnologías de la información, como así también de los elementos de control que permiten minimizar o eliminar las mismas, a través de una administración efectiva que permita vincular las amenazas, mecanismos de control y las tecnologías, para minimizar o eliminar el riesgo asociado.

Los controles relacionados a la seguridad se establecen para impedir el acceso físico y lógico a los sistemas de información y sus recursos relacionados por parte de personas que no tienen autorización, como también ayuda a reducir el riesgo de que las personas autorizadas cambien o destruyan accidentalmente los datos.

Los controles se establecen mediante la implementación de un conjunto de medidas **preventivas**, **disuasivas, detectivas** y **correctivas** destinada a proteger aspectos como la **disponibilidad, integridad, confidencialidad** y **privacidad.**

1.4. ¿CUÁL ES EL ALCANCE DE LA SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN?

El alcance del sistema de gestión de seguridad informática y de la información en la Empresa social del estado Pasto Salud está enfocada principalmente en: Procesos, Tecnología y personas.

1.4.1 Procesos

1.4.1.1 Proceso Gestión de la Información:

1.4.1.1.1. Recolección y consolidación de la información.

1.4.1.1.2. Entrega de la información.
1.4.1.1.3. Implementación e Implantación del sistema de información.
1.4.1.1.4. Seguridad de la información.

1.4.1.2 Proceso de Gestión Tecnológica:

1.4.1.2.1. Planeación, Gestión y evaluación de la tecnología.
1.4.1.2.2. Renovación tecnológica.
1.4.1.2.3. Mantenimiento Preventivo.
1.4.1.2.4. Mantenimiento Correctivo.

1.4.1.3 Áreas:

Se incluyen todas las áreas de la sede administrativa y asistencial de la Empresa Social del Estado Pasto Salud.

1.4.1.4 Personas:

Funcionarios, personal contratista que labora en la Empresa Social del Estado Pasto Salud ESE y cliente externo que presta servicios a la empresa.

1.4.1.5 Tecnología:

Hardware, Software, equipos de comunicaciones y servicios informáticos.

1. OBJETIVOS

2.1 OBJETIVO GENERAL

El objetivo general del manual de gestión de seguridad informática y seguridad de la información es brindar a las unidades y a los usuarios de tecnologías de información de la Empresa Social del estado Pasto Salud ESE, un conjunto de lineamientos e instrucciones que permiten garantizar la seguridad en el ambiente informático, la información y demás recursos tecnológicos.

2.2 OBJETIVOS ESPECÍFICOS

- Promover el uso de las mejores prácticas de seguridad informática en el trabajo, para que los usuarios colaboren con la protección de la información y recursos institucionales.

- Proponer los mecanismos de seguridad lógica, en el ambiente informático de modo que se contribuya con la confidencialidad, integridad y disponibilidad de la información.

- Servir de guía para el comportamiento profesional y personal de los funcionarios de la E.S.E. Pasto Salud, en procura de minimizar los incidentes de seguridad internos, como hurto de información.

- Promover las mejores prácticas de seguridad física, mediante la implementación de ambientes adecuados que permitan la correcta custodia de los datos y equipos administrados por los diferentes Centros de Gestión, utilización eficiente de los recursos de tecnologías de información.

- Regular el cumplimiento de aspectos legales y técnicos en materia de seguridad informática.

- Homologar la forma de trabajo de personas de diferentes unidades y situaciones que tengan responsabilidades y tareas similares.

3. MARCO LEGAL

Ley 1273 de 5 de enero de 2009 **:** Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado “DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones entre otras disposiciones.

Ley 23 de 1982**:** Sobre derechos de autor

ISO IEC 27001-2005**:** Estándares internacionales sobre tecnología de la información, técnicas de seguridad, Administración de seguridad de la información, los cuales proporcionan un marco de gestión de la seguridad de la información, utilizable por cualquier tipo de empresa.

Ley Estatutaria 1581 De 2012: Protección de los datos personales

COBIT**:** Buenas prácticas que promueve un conjunto de objetivos de control para la información y la tecnología.

ITIL**:** Marco de trabajo de mejores prácticas para el manejo de servicios de TI.

4. POLÍTICAS DE SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN

4.1 GENERALIDADES

La alta gerencia de la Empresa Social del Estado Pasto Salud, apoya los objetivos y principios de la seguridad informática y de la información para lo cual determina el obligatorio conocimiento y cumplimiento de la reglamentación y políticas de seguridad informática de la entidad, las cuales están consignadas en el presente manual.

En este documento de describen las políticas definidas por la gerencia de la empresa con respecto al uso adecuado de la Red de Datos Corporativa de Pasto Salud E.S.E., esto con el fin de que los usuarios de la red hagan el uso adecuado del hardware, software e información de la empresa.

El presente documento estará sujeto a cambios los cuales únicamente se podrán efectuar mediante acto administrativo firmado por el Gerente de la Empresa.

Este manual será publicado en la Intranet de la empresa y debe ser divulgado a todos los funcionarios y contratistas vinculados con Pasto Salud ESE.

El acatamiento de las directrices y políticas definidas a continuación evita incurrir en posibles sanciones y/o perjuicios tanto a la empresa como a los funcionarios y contratistas de la misma.

“TODO AQUELLO QUE NO SE AUTORICE EN FORMA EXPRESA, ESTÁ PROHIBIDO”

4.2 POLITICA 1: SOBRE ACCESO A LA INFORMACIÓN

El acceso a la información debe ser regulada por una jerarquía de permisos y niveles de autorización con el fin de proteger la información que existe y fluye en la organización. El otorgamiento de acceso a la información y definición de perfiles de usuario están regulados mediante las normas y procedimientos definidos para tal fin.

4.2.1 Instrucciones de Obligatorio Cumplimiento

En el caso de que personas ajenas a Pasto Salud ESE requieran información específica y confidencial de la empresa, es exclusivamente el Gerente quien puede y debe autorizar el acceso ó entrega de dicha información, previa solicitud formal en donde se describa la información requerida y el uso se que le dará a la misma.

4.3 POLITICA 2: SOBRE ADMINISTRACION DE CAMBIO

Los cambios generados en la plataforma de software de la empresa deben realizarse de conformidad al procedimiento establecido por la empresa y contar con un registro de operaciones a fin de hacer un seguimiento y control de su ejecución.

4.3.1 Instrucciones de Obligatorio Cumplimiento:

- Todo cambio (creación, eliminación ó modificación de programas, aplicativos, formatos y reportes) que afecte los recursos informáticos, debe ser solicitado formalmente por los usuarios de la información y aprobado formalmente por el responsable de la administración de la misma, el nivel de jefe inmediato ó por quienes estos formalmente deleguen. El responsable de la administración de los accesos a la información tendrá la facultad de aceptar o rechazar la solicitud.

- Bajo ninguna circunstancia un cambio de la información o de los sistemas de información puede ser aprobado, realizado e implantado por la misma persona o por una misma área.

- Todos los requerimientos de mantenimiento de los sistemas de información (software o hardware) y/o necesidades de suministros ó elementos, deben ser solicitados de forma escrita al Jefe de la Oficina Asesora de Comunicaciones y Sistemas de manera formal mediante oficio, correo electrónico o en el formato oficialmente establecido y adoptado por la empresa.

4.4 POLÍTICA 3: SOBRE LA SEGURIDAD DE LA INFORMACIÓN

Los trabajadores de planta y contratistas son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales establecidos por la entidad, por las normas que reglamenten el archivo documental, con el fin de garantizar su custodia, integridad, confidencialidad, disponibilidad y confiabilidad y así evitar pérdidas, accesos no autorizados, exposición, modificación y/ó utilización indebida de la misma, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

4.4.1 Instrucciones de Obligatorio Cumplimiento:

- Los trabajadores de planta, contratistas y pasantes no deben suministrar información de la empresa a ningún ente externo sin las autorizaciones respectivas.

- Los funcionarios, contratistas y terceros vinculados a Pasto Salud ESE deberán firmar y renovar cada año, un acuerdo de cumplimiento de las políticas de seguridad de la información, de confidencialidad y de buen manejo de la información que manejen o a la que tengan acceso durante la vinculación a la empresa. Después de que el trabajador deja de prestar sus servicios a la Entidad, se compromete entregar toda la información respectiva de su trabajo realizado. Una vez desvinculados los funcionarios o contratistas, ellos deben comprometerse a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la entidad, directamente o través de terceros, así mismo, los trabajadores que detecten el mal uso de la información está en la obligación de reportar el hecho al Jefe de la Oficina de Control Interno ó a los entes de vigilancia y control pertinentes.

- El software adquirido y desarrollado por funcionarios de Pasto Salud E.S.E., es exclusivo para el funcionamiento de las operaciones de la compañía y en ningún momento debe ser copiado o prestado o vendido para otros fines distintos a los que se adquirieron o se desarrollaron. En caso de que terceros requieran de éstos, debe ser autorizado por la Gerencia General.

- Las políticas, normas y procedimientos relacionados con la seguridad de la información que tiene establecida la empresa, se deben socializar a funcionarios, contratistas y clientes externos, para efectos de aplicabilidad y uso**.**

4.5 POLITICA 4: SOBRE SEGURIDAD EN RECURSOS INFORMÁTICOS.

Los funcionarios y contratistas de la empresa son responsables de los recursos informáticos (hardware) que manejan y les sean entregados para su uso en cumplimiento de sus funciones, objetos contractuales o actividades y deberán garantizar su custodia, integridad, buen uso, para evitar pérdidas, daño ó deterioro injustificado.

4.5.1 Instrucciones de Obligatorio Cumplimiento:

- No mover o desconectar el equipo de cómputo o algunos de sus dispositivos cuando se encuentre encendido, para evitar un daño del mismo.
- Cerrar y apagar el equipo correctamente para no dejar ninguna tarea pendiente en su computador y evitar el riesgo de incendios en su sitio de trabajo o interrupción de la copia de seguridad.

- Apagar el computador e impresoras en el momento de ausentarse de su puesto de trabajo por periodos prolongados (Al medio día, al finalizar la jornada laboral, durante las reuniones) evitando accesos de otros personas desde su computador a la red corporativa, o en caso de ausentarse por corto tiempo deberá dejar el equipo bloqueado.

- La red eléctrica regulada permanece debidamente señalizada y no puede ser utilizada para conectar equipos tales como: herramientas, electrodomésticos, impresoras láser, fotocopiadoras, grabadoras, equipos de iluminación, cargadores etc. En caso de requerirse utilizar un equipo de estos, se debe consultar previamente a la oficina Asesora de Comunicaciones y Sistemas.

- Conectar únicamente a la red eléctrica regulada identificada de color naranja el monitor y la CPU.

- Todos los usuarios tendrán el Panel de control desactivado para evitar cambios a la configuración de los PC.

- Queda expresamente prohibido el copiar o distribuir música y videos en cualquier formato (MP3, WAV, AVI, etc.) en los computadores de la entidad dado que la empresa acata y respeta las leyes de propiedad intelectual y de

derechos de autor, la posesión y distribución de música y videos en dichos formatos podrá acarrearle al usuario sanciones de tipo disciplinario y legal.

- No se deben instalar programas sin la autorización de la Oficina Asesora de Comunicaciones y Sistemas. El software debe estar debidamente soportado por una licencia de uso. Así mismo no es permitido la carga o descarga de software u otro elemento por Internet o por cualquier otro medio que viole las leyes de derechos de autor; si se requiere de este servicio, se debe solicitarlo de manera formal por oficio o por correo electrónico a la Oficina Asesora de Comunicaciones y Sistemas con la justificación y confirmación de que es de libre uso (free), antes de ser descargado e instalado.

- Cada vez que se instalen equipos de cómputo, o de comunicaciones, la oficina de Almacén le debe entregar al funcionario que lo va a utilizar un formato de Inventario de Software y Hardware debidamente diligenciado; el software que se encuentre instalado en los equipos de los funcionarios debe estar debidamente licenciado.
- Los equipos (PC, servidores, LAN etc.) no deben reubicarse en nuevos ambientes de trabajo sin la aprobación previa del Jefe de la Oficina Asesora de Comunicaciones y Sistemas.

- Pasto Salud E.S.E. no es dueño del software licenciado, ni de la documentación adjunta con el software, a menos que así lo autorice el titular de los derechos de autor. Ningún empleado tiene el derecho de reproducirlo a menos que sea la copia de respaldo. Las licencias que posee Pasto Salud E.S.E. solo le otorgan el derecho al uso del software dentro de la compañía.

- Los funcionarios y contratistas de la empresa deberán usar el software solamente de la manera establecida en la licencia por el fabricante.

- Los funcionarios y contratistas de la empresa que tengan conocimiento del uso no autorizado de software o de su documentación relacionada dentro de la empresa, deberán notificar a la jefatura de la Oficina Asesora de Comunicaciones y Sistemas de ello.

- Los funcionarios y contratistas de la empresa que hagan mal uso o adquieran de forma ilegal cualquier tipo de software u otro elemento que posea marca registrada, podrán ser sancionados por la misma entidad de conformidad con los procesos establecidos o serán denunciados a los entes de investigación competentes para que se actúe según lo establecido en las leyes de derechos de autor.

- Para la adquisición de nuevo software, los funcionarios y contratistas de la empresa deberán consultar previamente a la Oficina Asesora de Comunicaciones y Sistemas con el fin de determinar si los equipos soportan la instalación y funcionamiento de dicho software o si se deben realizar previamente adecuaciones del hardware.

- Las unidades de lectura y/o grabación de CD, DVD, USB etc. permanecerán inactivas para la protección de la información contenida en la red de información corporativa y para evitar la instalación de software no licenciado por la empresa. Únicamente serán autorizados los equipos que la Jefatura de la oficina de comunicaciones y sistemas autorice.

- Cuando se requiera hacer el uso de medios extraíbles de almacenamiento de información, para lectura y/o escritura, estos deberán ser analizados inicialmente con software anti virus por el personal de la Oficina Asesora de Comunicaciones y Sistemas para evitar la infección por virus informático o malware en general.

- No está permitido compartir los recursos de los computadores (disco duro o carpetas) a todos los usuarios. Solo se puede compartir a los usuarios específicos que se determine con la ayuda del área de Informática, para evitar que sean copiados o modificados los archivos ubicados en su computador por un usuario no autorizado. Solo se admite compartir una carpeta pública donde se puedan colocar los diferentes documentos a compartir con restricción de lectura o clave de acceso.

- Cualquier cambio que se requiera realizar en los equipos de cómputo de la entidad (cambios de procesador, adición de memoria, cambio de discos o tarjetas etc.) debe tener previamente una evaluación y concepto técnico de la necesidad de dicho cambio y autorización de la Oficina Asesora de Comunicación y Sistemas.

- La reparación técnica de los equipos de cómputo, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado de la Oficina Asesora de Comunicación y Sistemas o personal técnico contratado

- Los usuarios no pueden romper el sello de seguridad ya que representa la garantía del mantenimiento efectuado a los equipos de cómputo.

- No se debe ingerir alimentos líquidos o sólidos encima de los equipos de cómputo para evitar daños del PC.

- Siempre se deberá registrar el ingreso y salida de la empresa de todos los computadores portátiles, equipos de comunicación y demás equipos electrónicos no podrán ser retirados de la entidad a menos que se cuente con la respectiva autorización por Almacén.

- Los particulares en general, entre ellos, los familiares de los trabajadores, no están autorizados para utilizar los recursos informáticos de la empresa.

4.6 POLITICA 5: SOBRE MANEJO DE CORREO ELECTRÓNICO, HERRAMIENTAS TECNOLÓGICAS Y USO DE LA INTERNET

El uso de la Internet estará restringido en concordancia con las políticas de seguridad informática de la Empresa. Desde la Oficina Asesora de Comunicación y Sistemas se administrarán todos los accesos a Internet de los funcionarios que lo necesiten, evitando de esta forma colapsar el servicio. El usuario que sea sorprendido según el reporte diario del web máster visitando sitios no autorizados por la empresa, en primera instancia se le hará el llamado de atención y si reincide se informara a la oficina de control interno disciplinario para personal de planta o si es un contratista se informará a la oficina de Talento Humano para que informe a la empresa que presta los servicios.

4.6.1 Instrucciones de Obligatorio Cumplimiento:

- El correo electrónico institucional no se deberá utilizar para enviar mensajes como cadenas o mensajes con contenido censurable. En general el correo electrónico institucional es de uso empresarial y no personal.

- Se debe eliminar periódicamente los mensajes del correo electrónico institucional para no llegar al límite establecido por el área de Informática, porque el sistema bloquea el buzón de correo una vez se ha excedido el límite. El tamaño del límite de capacidad del buzón del correo electrónico institucional depende de las necesidades de cada funcionario o contratista.

- Se debe almacenar en el disco duro los documentos importantes que fueron recibidos por el correo electrónico institucional, teniendo en cuenta que el buzón de correo electrónico es un sitio de intercambio de información mas no un sitio de almacenamiento de información. Una vez almacenado en el disco duro debe ser eliminado del correo.

- Está terminantemente prohibido usar la red corporativa de internet para consultar, divulgar o promover lugares en Internet con contenido erótico, pornográfico, Intolerancia (racial, político), religioso, juegos virtuales, violencia, uso de drogas o lugares donde se use lenguaje soez.

- Está prohibido el uso del internet para el manejo de cuentas personales de acceso a correos, redes sociales como: facebook, sónico, twiter, msn, google+, twitter, entre otras y servicios de chat externos, con excepción de los autorizados por la jefatura de sistemas para manejo institucional.

4.7 POLITICA 6: SOBRE ALMACENAMIENTO Y RESPALDO DE LA INFORMACIÓN

La Oficina Asesora de Comunicaciones y Sistemas implementará mecanismos para el almacenamiento seguro y protección de la información en medios magnéticos o electrónicos, perpetuarla y garantizar su recuperación en caso de fallas de los equipos de cómputo u ocurrencia de eventos de contingencia o situaciones fortuitas.

4.7.1 Instrucciones de Obligatorio Cumplimiento:

- La realización de copias de respaldo debe ser acorde al procedimiento para copias de seguridad de los sistemas de información establecido en la empresa, lo cual permitirá garantizar la oportuna recuperación de la información en la eventualidad que ocurra algún percance.

- Se debe mantener las copias de seguridad de la información según la periodicidad establecida en el procedimiento de backups y proveer de un lugar externo a las instalaciones de Pasto Salud E.S.E. la cual permita recuperar la información en caso de una contingencia.

- La custodia de las copias de respaldo de la información se realizará externamente con una compañía de seguridad especializada en este tema, contratada por la empresa.

- Es responsabilidad de la Oficina Asesora de Comunicaciones y Sistemas, verificar mensualmente que se hayan realizado todas las copias de seguridad de la información almacenada en cada equipo y que estas se encuentren en buen estado para su almacenamiento y posterior restauración.

- Al final de cada año, la Oficina Asesora de Comunicaciones y Sistemas, guardará una copia de seguridad de toda la información almacenada en la vigencia, en medios magnéticos, para su conservación y custodia.

- La Oficina Asesora de Comunicaciones y Sistemas deberá garantizar la privacidad y confidencialidad de la información en aquellas áreas que la soliciten mediante el manejo de claves de seguridad y el encriptamiento de la información.

- Se debe informar a la oficina asesora de comunicaciones y sistemas del retiro de funcionarios o contratistas que manejen contraseñas, permisos de usuarios ó claves de seguridad cuando estos finalicen su contrato o terminen labores con la empresa, desactivar las cuentas de usuario, claves, contraseñas, permisos y similares, dentro de los sistemas de información de la empresa.

- Los dispositivos o medios que contengan copias de seguridad (backups) deberán mantenerse almacenados en un lugar seguro previamente definido por la Oficina Asesora de Comunicaciones y Sistemas y su manejo será exclusivo de dicha área.

4.8 POLITICA 7: SOBRE CONTROL DE CLAVES DE ACCESO (CONTRASEÑAS)

Los sistemas de información deberán protegerse por medio de un modelo de claves de acceso que sean seguras y que garanticen un nivel de confiabilidad aceptable para la protección de información de accesos no deseados ni permitidos.

4.8.1 Instrucciones de Obligatorio Cumplimiento:

- Cada funcionario o contratista deberá tener una clave personal e intransferible de acceso que le permitirá ingresar de forma exclusiva tanto a los sistemas operativos, a las bases de datos y a los aplicativos a los que está autorizado. Cada funcionario o contratista es responsable del uso de su clave de acceso y es su responsabilidad mantenerla en secreto, ya que cualquier modificación no autorizada de la información, daño o acceso irregular que ocurra y se detecte, es responsabilidad del usuario que maneje la clave y por tanto puede hacerse acreedor a las sanciones de tipo legal y disciplinario que esto conlleve.

- Política de directorio activo para el manejo de las contraseñas a las cuenta de usuarios: los usuarios debe seguir los siguientes lineamientos en relación con las claves de acceso:

- Las claves de acceso deben ser cambiada, mínimo cada 3 meses, y en ningún caso debe ser igual a la anterior.

- La clave de acceso debe ser compleja, La longitud mínima de la clave de acceso debe ser como mínimo de ocho caracteres, contener al menos una Letras mayúscula, un número, letras minúsculas y un carácter especial y debe ser diferente al nombre del usuario, la fecha de nacimiento ó el número de identificación.

- Se mantendrá un registro histórico de hasta tres cambios de cuentas y el funcionario o contratista no podrá utilizar nuevamente ninguna de las tres contraseñas anteriores.

- La persona responsable del área de sistemas de cada red será responsable de informar de forma escrita a la Oficina Asesora de Comunicaciones y Sistemas la necesidad de un nuevo punto de acceso a la red, la creación de un nuevo correo electrónico institucional o la creación de una nueva cuenta de usuario y clave de acceso. En caso de que el usuario requiera algún permiso especial o algún cambio en la configuración del perfil de usuario, estos cambios deberán ser solicitados a la Oficina Asesora de Comunicaciones y Sistemas por el gerente, funcionario del nivel directivo o asesor responsable del área o dependencia en donde se solicita el cambio.

4.9 POLITICA 8: SOBRE CONTROL DE VIRUS INFORMATICOS

La Empresa Social del Estado PASTO SALUD ESE para la protección de su información, deberá contar con herramientas informáticas para el control de los software maliciosos incluidos los virus informáticos, así como un grupo de prácticas que eviten su masificación y su influencia negativa.

4.9.1 Instrucciones de Obligatorio Cumplimiento:

- La empresa mantendrá instalado en todos sus equipos de cómputo un software anti malware ó antivirus que garantice la seguridad en la información, el cual se actualizará a través de la red una vez a la semana al iniciar sesión el equipo.

- En caso de que el usuario detecte la presencia de un virus en algún archivo o algún comportamiento anormal de las funciones dentro de los equipos de cómputo, Tiene el deber de notificar el hecho a la Oficina Asesora de Comunicaciones y Sistemas, para que se tomen las acciones pertinentes y evaluar su impacto en los demás equipos o en la red.

- No se deben abrir o reenviar archivos de dudosa procedencia para evitar el contagio de software mal intencionado ó virus.

- Se debe evitar al máximo el usar medios extraíbles de almacenamiento como CD, DVD, memorias USB etc. que pueden infectar a los equipos con software mal intencionado ó virus.

- Se deben eliminar correos electrónicos de remitentes desconocidos, o con mensajes o archivos adjuntos sospechosos, ya que estos pueden traer keyloogers, virus, sniffer, spam, etc. Esto puede ocasionar un ataque a nuestra red corporativa de datos a través de hackers y/o crackers informáticos.

4.10 POLITICA 9: SOBRE REQUERIMIENTOS Y/O CORRECCIÓN DE PROGRAMAS.

Para el buen desarrollo y ejecución de los paquetes informáticos de la empresa se deberá realizar de forma permanente el seguimiento y control del funcionamiento del software que maneje la empresa al igual que a las correcciones o cambios al mismo.

Toda irregularidad en el funcionamiento de los programas (software) deberá ser dada a conocer al personal competente para atender el asunto o solicitar el apoyo técnico requerido.

4.10.1 Instrucciones de Obligatorio Cumplimiento:

- En caso de que se presenten errores en los aplicativos de la empresa, estos deberán ser notificados a la Oficina Asesora de Comunicaciones y Sistemas, el usuario debe abrir un caso para reportar el incidente en la plataforma tecnológica disponible para tal fin.

- Si se requiere un nuevo desarrollo de software o una nueva funcionalidad para la empresa, se debe hacer el requerimiento a través de ofició a la

Oficina Asesora de Comunicaciones y Sistemas por parte del jefe o responsable de la dependencia, para su análisis y sustentación ante el comité de desarrollo o con los proveedores de software, si es del caso, y solo una vez sea aprobado, se procederá al desarrollo ó la implementación de la solución.

- Los responsables de los procesos o de las diferentes áreas o dependencias de la empresa deberán estar atentos e informar de los requerimientos y correcciones a los módulos de los aplicativos, de que estos se atiendan oportunamente y de verificar si efectivamente los inconvenientes fueron solucionados y los requerimientos fueron atendidos satisfactoriamente.

4.11 POLITICA 10: SOBRE SEGURIDAD EN COMUNICACIONES.

Todo funcionario o contratista de la empresa deberá conocer y ejecutar cuando se requiera, el procedimiento oficial para la administración, configuración e implementación de la infraestructura de la red corporativa, así como su uso, cambios u operaciones de gestión definidas por prácticas seguras para la información que por ellas fluye.

4.11.1 Instrucciones de Obligatorio Cumplimiento:

- Todo intercambio electrónico de información o interacción entre sistemas de información de la empresa con entidades externas, deberá estar soportado con un acuerdo, convenio o documento de formalización de dicho procedimiento.

- Los equipos de cómputo que se conecten de forma directa con un proveedor externo para suministrar un servicio se realizará a través de VPN (redes privadas virtuales o IP pública) mediante conexiones seguras, previa autorización de la Oficina Asesora de Comunicación y Sistemas y con los debidos mecanismos y sistemas de seguridad informática de la empresa y del proveedor de servicios.

- Toda información secreta y/o confidencial que se transmita por las redes de comunicación de la Entidad e Internet deberá contemplar cifrado o encripción el cual debe ser garantizado por el proveedor de servicio de comunicaciones bajo el monitoreo y supervisión de la Oficina Asesora de Comunicación y Sistemas.

4.12 POLITICA 11. SOBRE SEGURIDAD PARA USUARIOS TERCEROS.

Tanto los recursos informáticos como la información suministrada a, y por terceros ajenos a la empresa, deberán tener un tratamiento particular con el objeto de que los datos y los elementos del sistema de información de la empresa sean resguardados y utilizados adecuadamente. La empresa se reserva el derecho de monitorear los sistemas de información de terceros ajenos a la entidad sin previo aviso para evaluar la seguridad de los mismos. La empresa se reserva el derecho de cancelar y terminar la conexión a sistemas de información de terceros que no cumplan con los requerimientos internos y de seguridad informática establecidos por la entidad.

4.12.1 Instrucciones de Obligatorio Cumplimiento:

- Los recursos Informáticos que no sean propiedad de la entidad y deban ser ubicados y administrados por ésta, deberán garantizar la legalidad del recurso para su funcionamiento. Adicionalmente debe suscribir un documento de acuerdo oficial entre las partes.

- Los usuarios terceros tendrán acceso exclusivamente a los Recursos Informáticos de la empresa que sean estrictamente necesarios para el cumplimiento de su función, como soporte técnico y este acceso deberá ser aprobado por el Jefe de la Oficina Asesora de Comunicaciones y Sistemas, firmando un acuerdo de buen uso de los Recursos Informáticos.

- La conexión entre equipos, redes y/o sistemas internos de la entidad y otros de terceros deberá ser aprobada, certificada y monitorizada por el Jefe de la Oficina Asesora de Comunicaciones y Sistemas y deberán cumplir con todas las normas de seguridad informática establecidas en la empresa.

4.13 POLITICA 12: SOBRE CONTINUIDAD DEL FUNCIONAMIENTO DE LOS SISTEMAS DE INFORMACIÓN Y RECURSOS INFORMÁTICOS.

La Empresa debe contar con un plan de contingencia que permita dar continuidad al funcionamiento de sus sistemas de información y a sus recursos informáticos, garantizando su disponibilidad en el evento de una emergencia ó desastre como terremoto, erupción volcánica, terrorismo, inundación etc. Este plan de contingencia deberá socializarse en toda la empresa, deberá actualizarse y probarse periódicamente para que se aplique en el evento en que se ponga en

riesgo la continuidad de los sistemas de información o el funcionamiento de los recursos informáticos.

4.13.1 Instrucciones de Obligatorio Cumplimiento:

- El plan de contingencia en el área informática es de cumplimiento obligatorio en toda la empresa.

4.14 POLÍTICA 13: SOBRE EL ACCESO y SEGURIDAD DE LOS AMBIENTES FÍSICOS DONDE SE ENCUENTREN RECURSOS INFORMÁTICOS.

Todas las áreas de la empresa relacionadas directa o indirectamente con el procesamiento o almacenamiento de información de la entidad, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se considerarán como áreas de acceso restringido y por lo tanto se deben implementar medidas de control de acceso del personal a dichas áreas.

La Empresa deberá contar con los mecanismos de control de acceso a los ambientes físicos donde se encuentren recursos informáticos, tales como puertas de seguridad, sistema de alarmas y circuitos cerrados de televisión en las lugares que la entidad considere críticas.

4.14.1 Instrucciones de Obligatorio Cumplimiento:

- Se restringe el acceso de funcionarios, contratistas, proveedores de materiales y demás personas ajenas a la Oficina Asesora de Comunicaciones y Sistemas, al Centro de Cómputo, sitio donde están ubicados los Servidores, Planta Telefónica y Equipos de Comunicaciones. Este lugar deberá permanecer en todo momento cerrado con llave. La llave de este sitio debe ser manejada por el Profesional Universitario Sistemas de la Oficina Asesora de Comunicaciones y Sistemas.

- Todo visitante o personal ajeno a la empresa debe ser identificado mediante un sistema de registro y control de forma previa al ingreso a cualquier área ó dependencia de la entidad.

- Cualquier persona que ingrese a centros de cómputo o áreas de almacenamiento de información que la entidad considere criticas o de acceso restringido, deberá registrar el motivo del ingreso y estar

acompañada permanentemente por el personal que labora cotidianamente en estos lugares.

- En los centros de cómputo o áreas de almacenamiento de información que la entidad considere criticas, deberán existir elementos de control de incendio, control de inundación y alarmas y deberán contar con demarcación de las zonas de circulación y zonas de acceso restringido.

- Las centrales de conexión de los sistemas de información o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.

4.15 POLITICA 14: SOBRE POLITICA EDITORIAL Y DE ACTUALIZACIÓN DE LA INFORMACIÓN EN LA PÁGINA WEB.

La información publicada en la página web de la empresa debe ser actualizada permanentemente y además será objetiva, clara, imparcial, sin emisión de juicios de valor, veraz, institucional, accesible y confiable para la consulta tanto de los usuarios internos como externos de la empresa.

La información publicada en la página web de la empresa deberá mantener un formato y un estilo constante, con fuentes de información claramente definidas y confiables y ser presentada en concordancia con la plataforma estratégica de la empresa y las políticas de comunicación y seguridad informática.

4.15.1 Instrucciones de Obligatorio Cumplimiento:

- La información publicada en la página web de la empresa será entregada por cada una de las dependencias responsables de los procesos generadores de la misma, con revisión y aprobación del jefe o líder del proceso, área o dependencia respectiva quien respalda y da validez al contenido de dicha información.

- El administrador de la Página Web de la empresa será el responsable y compartirá las funciones de actualización de los datos y contenidos de las diversas secciones de la página, junto con el responsable de su edición. Dicha actualización se realizara simultáneamente al proceso de publicación, cuando sea necesaria o se presente alguna novedad.

- La Página Web de la empresa podrá contar con enlaces hacia otros sitios Web, cuando se considere que estos son útiles y de relevancia bien sea

para comunidad en general o para el personal del sector salud. Una vez que el usuario acceda a otro portal a través de un link almacenado en la página web de Pasto Salud E.S.E, estará sujeto a la política de privacidad y a la política editorial del portal nuevo.

- Los derechos de propiedad intelectual de cualquier material presentado en la Página Web de la empresa, incluyendo textos, fotografías, otras imágenes, sonidos y otros, son de propiedad de sus autores, incluyendo a Pasto Salud E.S.E., así se reservan todos los derechos de propiedad intelectual sobre los contenidos de su autoría y sobre las que sean cedidas.

4.16 POLITICA 15: SOBRE PROTECCION DE DOCUMENTOS

Los documentos de la empresa, independientemente del medio en que se encuentren almacenados o archivados, deberán estar protegidos contra toda modificación indebida y se implementarán una serie de medidas de control para garantizar su confidencialidad. Los documentos institucionales no pueden ser copiados, reproducidos o ser entregados a terceros, sin autorización del Representante Legal de la Empresa Social del Estado Pasto Salud E.S.E. con mayor énfasis en aquellos clasificados como confidenciales.

Se debe limitar el acceso, reproducción y la distribución de la información clasificada como confidencial, definiendo claramente que personas están autorizadas para ello en cada caso en particular.

4.16.1 Instrucciones de Obligatorio Cumplimiento:

- Todos los documentos confidenciales deben ser marcados o identificados como tales en cada una de sus hojas.

- Todo documento que se transmita a terceros y que en su contenido comprometa la responsabilidad de PASTO SALUD E.S.E en cualquier sentido debe estar protegido contra escritura para garantizar la integridad del mismo, utilizando herramientas o software para la protección.

- No se debe transmitir información estrictamente confidencial por correo electrónico, fax o medio similar, si no cuenta con las medidas apropiadas para asegurar que no va a caer en manos de personas no autorizadas y para garantizar su absoluta integridad.

- Se debe emplear un método absolutamente seguro de destrucción para la información confidencial cuando esto se requiera. La destrucción debe llevarse a efecto exclusivamente bajo la supervisión de una persona autorizada que levante acta de este proceso.

- Se debe destruir la información confidencial impresa en papel utilizando los mecanismos para este fin, por ejemplo, máquinas destructoras de papel.

- Se debe borrar la documentación confidencial almacenada electrónicamente, usando el proceso habitual para ello, siempre que esté seguro que no tengan acceso a sus medios de almacenamiento otras personas autorizadas. Se puede recurrir a la destrucción de los medios extraíbles de almacenamiento de información tales como memorias USB, CD ó DVD.

- Se debe destruir y nunca reparar los soportes de datos magnéticos u ópticos con información confidencial que estén defectuosos. No se deben devolver al fabricante a cambio de un nuevo dispositivo.

5. GLOSARIO

Entiéndanse para el presente documento los siguientes términos:

Política: Son instrucciones que indican la intención de la alta gerencia respecto a la operación de la organización respecto a un asunto determinado.

Recurso Informático: Elementos informáticos (base de datos, sistemas operacionales, redes, equipos de computo, sistemas de información y comunicaciones) que facilitan servicios informáticos.

Información: Puede existir en muchas formas. Puede estar impresa en papel, almacenada electrónicamente, transmitida por correo electrónico o utilizando medios magnéticos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

Usuarios Terceros: Todas aquellas personas naturales o jurídicas, que no son funcionarios o contratistas de Pasto Salud ESE, pero que por las actividades que realizan en la Entidad, deban tener acceso a recursos Informáticos.

Ataque cibernético: Intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.

Brecha de seguridad: Deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

Criptografía de llave publica: Es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

Cifrar: Se refiere a transformar un mensaje en un documento no legible, y el proceso contrario se llama “descodificar" o “descifrar". Los sistemas de cifrado se llaman sistemas criptográficos".

Certificado Digital: Es un bloque de caracteres que acompaña a un documento y que certifica quién es su autor (autenticación) y que no haya existido ninguna manipulación de los datos (integridad). Para firmar, el firmante emisor utiliza una clave secreta que le vincula al documento. La validez de la firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

Controles sobre la seguridad: Representan los procedimientos de control interno establecidos por Pasto Salud E.S.E. para asegurar que el uso de las tecnologías de información alcance sus objetivos. En un concepto moderno y basado en los lineamientos que define la re-ingeniería organizacional, los controles generales se han direccionado al control de los procesos informáticos.

Procesos informáticos: Son los procesos que tienen relación directa con los servicios que se prestan a los usuarios de los sistemas de información y sus tecnologías relacionadas, procesos que consisten en tomar un insumo, agregarle valor y generar un producto que satisface a un cliente interno o externo.

Amenaza: Es el conjunto de los peligros a los que están expuestos los sistemas de información y sus recursos tecnológicos relacionados, los que pueden ser de tipo accidental o intencional.

Amenaza Accidental: Cuando no existe un deliberado intento de perjudicar a la organización.

Amenaza Intencional: Su móvil es perjudicar a la organización u obtener beneficios en favor de quien comete la acción.

Confidencialidad: Asegurar que los sistemas de información y sus recursos relacionados sean solo accedidos por los funcionarios o contratistas de Pasto Salud E.S.E, basados en la necesidad de saber o de hacer de sus cargos.

Integridad: Exactitud y plenitud de los sistemas de información y sus recursos relacionados, limitando la gestión sobre los mismos a personas autorizados y programas de aplicación aprobados y autorizados, protegiéndolos contra pérdida, destrucción o modificaciones accidentales o intencionales.

Disponibilidad: Asegurar que los usuarios autorizados tienen acceso a los sistemas de información y sus recursos relacionados, en tiempo y forma, cuando sean requeridos.

Privacidad: Evitar que trascienda a terceras personas información de Pasto Salud E.S.E., referida a individuos, protegiendo a los mismos contra la divulgación indebida de su información personal y protegiendo la responsabilidad de la empresa sobre este tipo de divulgaciones.

TI: Tecnología de la Información.

Hacker: Usuario de computadores responsable de acceder indebidamente en las bases de datos de sistemas informáticos estatales con el fin de obtener información secreta y en algunos casos provocar daños.

Spam: Se llama spam, al correo basura o a los mensajes no solicitados, no deseados o de remitente desconocido.

Keylogger: Es un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet.

Sniffer: El sniffer es un software que permite capturar tramas de la red. Generalmente utilizado con fines maliciosos para capturar textos de emails, chats, datos personales, contraseñas, etc.

Phishing: El phishing es un tipo de engaño creado por hackers malintencionados, con el objetivo de obtener información importante como números de tarjetas de crédito, claves, datos de cuentas bancarias, etc.