DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LAS ÁREAS ADMINISTRATIVA Y ACADÉMICA DE LA INSTITUCIÓN SYSTEM PLUS PASTO LTDA, BASADO EN EL ESTÁNDAR INTERNACIONAL ISO/IEC 27001:2013

CARLOS ARTURO PULIDO RODRÍGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

PASTO - COLOMBIA

2015

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LAS ÁREAS ADMINISTRATIVA Y ACADÉMICA DE LA INSTITUCIÓN SYSTEM PLUS PASTO LTDA, BASADO EN EL ESTÁNDAR INTERNACIONAL ISO/IEC 27001:2013

CARLOS ARTURO PULIDO RODRÍGUEZ

Tesis de grado para optar por el título:
Especialista En Seguridad Informática

Director de Proyecto:
Ing. Erika Liliana Villamizar Torres

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

PASTO - COLOMBIA

2015

Nota de Aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

San Juan de Pasto, 10 de diciembre de 2015

DEDICATORIA

A Dios por estar conmigo siempre,
A mis Padres, por su constante motivación,
A mi hijo Thomás, por ser la razón de mi vida,
A mis hermanos Diana y Edgar, por el ánimo para no desistir y
A mis amigos, por apoyarme en los momentos difíciles.

AGRADECIMIENTOS

El autor expresa sus agradecimientos a:

Dios, por permitirme disfrutar de buena salud y salir avante a pesar de las dificultades, pero también por todos y cada uno de los días en que me refugiaba en Él y le pedía que me ayudara y que me concediera mucha sabiduría y entendimiento para comprender y asimilar los temas compartidos por nuestros tutores y directores en cada uno de los cursos de la especialización.

A mis Padres porque a pesar de estar lejos, no hubo un instante en el que me hicieran sentir sólo, pues siempre estuvieron muy pendientes de mí, llamándome y preguntándome cómo iban mis estudios. Por haberme apoyado en todo momento, por sus consejos, por la motivación y en especial por sus oraciones y el amor que siempre me han brindado.

A mi hijo por ser mí motivo principal y la razón de ser de los logros alcanzados. Por todos los momentos que estuvo conmigo apoyándome y por aquellos días que no pude estar con él, porque me encontraba estudiando y realizando trabajos. Quiero agradecer y dedicar este trabajo en especial a ese ser maravillo, mi hijo Thomás.

A mis familiares, y mis hermanos Diana y Edgar por el ánimo para no desistir y continuar con mi proceso formativo y poder entregar los trabajos a tiempo. Por ser ellos ejemplo de superación y de los cuales aprendí aciertos que me permitieron superar momentos difíciles.

A mis amigos, que me apoyaron en mi formación profesional y que hasta ahora, seguimos siendo amigos: Lilian Dayana, Aurita, María Eugenia, María Mery Aide, Betsy, Martica y Geraldin.

¡Gracias a los Tutores y Directores!

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

INTRODUCCIÓN

Hasta hace un tiempo se creía que los activos de las empresas estaban en la maquinaria, el dinero en efectivo, los vehículos de la empresa, las deudas, las inversiones, las patentes y demás, pero estos hoy en día no son los únicos activos por los cuales las empresas deben preocuparse, ya que la información en sí es un activo intangible que se debe valorar y proteger.

Entonces surgen varias preguntas a las cuales se desea dar respuesta, tales como ¿está segura la información que se maneja en las empresas? ¿Qué se está haciendo para proteger la información? ¿Quiénes son los responsables del tratamiento de la información? Éstas y muchas otras inquietudes son las que se pretende dar respuesta con el desarrollo del presente trabajo, ya que es una situación muy común que se presenta en muchas empresas del país y del resto del mundo.

En el desarrollo de este proyecto se pretende diseñar e implementar medidas de seguridad en la Institución SYSTEM PLUS PASTO LTDA, y más específicamente las áreas Administrativa y Académica de la Institución, para tratar de ofrecer una adecuada protección a los activos de información los cuales se ven expuestos a una gran cantidad de amenazas y vulnerabilidades que ponen en riesgo la disponibilidad, integridad y confidencialidad de la información, buscando alcanzar un nivel aceptable de los riesgos que actualmente se presentan y que se espera sea un modelo a seguir para todos los miembros de la Institución.

Dentro de las actividades que buscan proteger la información en las áreas indicadas, se desarrollaran la clasificación de los activos, la identificación de amenazas, vulnerabilidades y riesgos para dichos activos, se diseñaran y definirán unas políticas de seguridad de la información acordes a los procesos y requerimientos de las áreas descritas, se elegirán los controles del Estándar Internacional ISO/IEC 27001:2013 que mejor se adapten a las políticas definidas, se recomendará una metodología de análisis de riesgos que disminuya la ocurrencia de los riesgos y se buscará concienciar al personal del área Administrativa y área Académica de la Institución SYSTEM PLUS PASTO LTDA, sobre los lineamientos de seguridad de la información establecidos en el SGSI.

RESUMEN

La idea de este proyecto es mejorar las condiciones actuales de seguridad de las áreas Administrativa y Académica de la Institución SYSTEM PLUS PASTO LTDA. Para ello se busca diseñar un Sistema de Gestión de Seguridad de la Información SGSI, que permita asegurar la información y los equipos con que cuenta actualmente la Institución en estas áreas específicas, haciendo uso de buenas prácticas de seguridad que permitan disminuir las amenazas, vulnerabilidades y riesgos que ponen en peligro la confidencialidad, la disponibilidad y la integridad de los datos de la Institución.

Para este propósito se desarrollarán actividades de clasificación de activos, identificación de amenazas, vulnerabilidades y riesgos, diseño y definición de políticas de seguridad de la información que estén acordes a los procesos y requerimientos de las áreas descritas, elección de los controles del Estándar Internacional ISO/IEC 27001:2013 que mejor se adapten a las políticas definidas, recomendación de una metodología de análisis de riesgos que disminuya la ocurrencia de los riesgos y concienciación del personal del área Administrativa y área Académica de la Institución SYSTEM PLUS PASTO LTDA, sobre los lineamientos de seguridad de la información establecidos en el SGSI.

Palabras clave: amenazas, información, riesgos, seguridad, vulnerabilidades.

ABSTRACT

The idea of this project is to improve the current security conditions in the areas of Administrative and Academic Institution SYSTEM PLUS PASTO LTDA. To do so will be to develop a Management System Information Security ISMS, thus ensuring the information and equipment currently available to the institution in these specific areas, using good security practices that enable mitigation of threats, vulnerabilities and risks that jeopardize the confidentiality, availability and data integrity of the institution.

For this purpose asset classification activities, identification of threats, vulnerabilities and risks, design and definition of security policies that are consistent information to the processes and requirements of the areas described, choice of controls will be developed International Standard ISO / IEC 27001: 2013 that best meet the defined policies, recommending a risk analysis methodology to decrease the occurrence of risks and awareness of staff in the administrative area and the area Academic Institution SYSTEM PLUS PASTO LTDA, on guidelines Security of information set out in the ISMS.

Keywords: threats, information, risks, security, vulnerabilities.

1. PLANTEAMIENTO DEL PROBLEMA

La Institución SYSTEM PLUS PASTO LTDA, es una Institución de formación para el Trabajo y el Desarrollo Humano, que presta servicios de capacitación en carreras Técnicas desde hace 21 años en la ciudad de San Juan de Pasto. La Institución cuenta con más de 25 funcionarios entre administrativos, docentes y personal de apoyo y más de 300 estudiantes.

Varias situaciones han sido percibidas por los funcionarios y usuarios de las áreas administrativa y académica de la Institución SYSTEM PLUS PASTO LTDA, siendo las más comunes la parálisis de actividades, debida a que los equipos se encuentran fuera de servicio, por razones de falta de mantenimiento periódico, daños producidos por fallas eléctricas, virus u otro tipo de software malicioso. Ante ésta situación ellos deben esperar a que la persona responsable del mantenimiento de los equipos, repare el equipo para continuar las actividades.

En varias oportunidades se han visto afectados por pérdida de información provocada por el mal manejo de los equipos y programas, llegando a situaciones en donde ha sido imposible recuperar los datos, por no contar con una copia de respaldo de dicha información.

En ocasiones se han encontrado funcionarios pertenecientes a otras áreas de la Institución, así como estudiantes y personas externas, utilizando los equipos de las áreas administrativa y académica de la Institución SYSTEM PLUS PASTO LTDA, algunas de ellas con el consentimiento de los mismos funcionarios que allí laboran y otras veces sin la debida autorización.

Las personas realizan sin ninguna restricción actividades de interés personal en los equipos de estas áreas, tales como navegar en internet sin limitaciones, consultar correos electrónicos, acceder a redes sociales, descargar archivos ejecutables de internet, imprimir documentos, copiar información desde y hacia un disco sin tener en cuenta las mínimas medidas de seguridad como el análisis de virus.

Todos los equipos de la Institución están conectados a la misma red, sin que exista una segmentación por áreas, lo que permite que personas internas como externas a las áreas administrativa y académica, puedan ver la información que se comparte en la red, tal como instaladores, programas con sus respectivas licencias, documentos, trabajos, registros de estudiantes con información

personal, cuestionarios, guías, módulos de clases y demás información confidencial, pudiendo fácilmente ser consultada, copiada, modificada, borrada o extraída sin ningún impedimento.

Se emplea el mismo correo personal para las actividades de la Institución dando lugar a que se introduzcan virus o cualquier otro software malicioso y acceda, altere, borre o extraiga información del área administrativa y académica de la Institución, incluso sin que los funcionarios se percaten de ello.

Se han detectado varias aplicaciones instaladas sin la debida autorización del encargado de Soporte Técnico, las cuales alojan virus, malware, troyanos, software espía y demás software dañino, haciendo que se vea afectado el normal funcionamiento de los equipos, los programas y la red cableada e inalámbrica.

Las anteriores amenazas y vulnerabilidades dejan ver los problemas de confidencialidad, integridad y disponibilidad de la información en las áreas administrativa y académica de la Institución SYSTEM PLUS PASTO LTDA, las cuales pueden ser aprovechas por quienes intentan valerse de algún descuido de los funcionarios, estudiantes o visitantes, para poner en riesgo la seguridad de la información. A esto se suman la falta de políticas de seguridad, la falta de divulgación de información a los funcionarios de estas áreas en temas de seguridad y la falta de controles que disminuyan los riesgos.

2. FORMULACIÓN DEL PROBLEMA

¿Cómo se puede garantizar la seguridad de la información de las áreas administrativa y académica de la Institución SYSTEM PLUS PASTO LTDA?

3. JUSTIFICACIÓN

El presente proyecto permitirá establecer una solución viable a los problemas que se presentan en las áreas Administrativa y Académica de la Institución SYSTEM PLUS PASTO LTDA, con el propósito de establecer medidas que mejoren la protección de la seguridad de la información.

Todo el trabajo se desarrolla en base a las medidas de prevención y protección de la información, teniendo en cuenta que debemos mantener los tres pilares fundamentales que son la confidencialidad, la integridad y la disponibilidad de la información.

Una de las principales razones de esta implementación es conocer y gestionar de manera adecuada los riesgos a los cuales está expuesto el sistema informático, además considerar procedimientos apropiados y planificar e implantar controles de seguridad que se ajusten a las necesidades de las áreas de la Institución SYSTEM PLUS PASTO LTDA.

Todas las vulnerabilidades descritas en el planteamiento del problema son producto de la falta de políticas, de procedimientos y controles que vayan de la mano con los propósitos de las áreas Administrativa y Académica de la Institución SYSTEM PLUS PASTO LTDA, las cuales deben permitir garantizar que los posibles riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados de una forma documentada y organizada.

Si el área Administrativa y el área Académica de la Institución SYSTEM PLUS PASTO LTDA continúa sin la implementación de un conjunto de políticas de administración de equipos y de información que permitan minimizar los riesgos y disminuir las vulnerabilidades observadas, se seguirán presentando pérdida de datos, alteraciones accidentales o intencionales de la información y modificación de los equipos, accesos no autorizados, carencia de soluciones oportunas para restaurar los servicios en el menor tiempo posible. Todo esto conllevará a las áreas a no ser competitivas y ofrecer un entorno poco seguro, haciendo que la presencia de estos incidentes de seguridad a nivel Institucional, afecten la operatividad y continuidad de la Institución en el mercado, logrando verse afectada a nivel económico, legal y de imagen.

La Institución SYSTEM PLUS PASTO LTDA., es actualmente vulnerable a los ataques de personas internas o externas que tengan como propósito destruir o robar datos confidenciales. Se recomienda por lo tanto que la Institución adopte

estándares de seguridad y tenga en cuenta las razones por las cuales las áreas mencionadas requieren medidas de seguridad claras, que mejoren su situación frente a la seguridad de la información, que les permita mantener una ventaja competitiva en el mercado y proveer seguridad a sus usuarios y/o aliados.

Con todas estas actividades se pretende que las áreas mencionadas sepan qué hacer y cómo recuperarse lo antes posible en caso de presentarse un incidente, evitando tener que parar sus actividades por culpa de una falla humana, de hardware, de software, o por culpa de amenazas naturales como desastres naturales.

4. OBJETIVOS DEL PROYECTO

4.1 GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información para las áreas administrativa y académica de la Institución SYSTEM PLUS PASTO LTDA, basado en el estándar internacional ISO/IEC 27001:2013

4.2 ESPECÍFICOS

- Clasificar los activos de las áreas administrativa y académica de la Institución SYSTEM PLUS PASTO LTDA, que se someterán al SGSI.
- Identificar las amenazas, vulnerabilidades y riesgos que pueden comprometer la seguridad de los activos de las áreas administrativa y académica de la Institución SYSTEM PLUS PASTO LTDA.
- Diseñar y definir las políticas de seguridad de la información que estén acordes a los procesos y requerimientos de las áreas administrativa y académica de la Institución SYSTEM PLUS PASTO LTDA.
- Elegir los controles aplicables para las áreas administrativa y académica de la Institución SYSTEM PLUS PASTO LTDA de acuerdo al anexo A del Estándar Internacional ISO/IEC 27001:2013 y realizar las recomendaciones de implementación.
- Concienciar al personal del área administrativa y área académica de la Institución SYSTEM PLUS PASTO LTDA, acerca de los lineamientos de seguridad de la información establecidos en el SGSI.

5. MARCO REFERENCIAL

5.1 MARCO TEÓRICO

Delito informático: Se denomina a una forma de "Delincuencia informática. Es todo Acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico Cualquiera"[1].

Hacking: Se denomina a la conducta de entrar a un sistema de información sin autorización, es decir violando las barreras de protección establecidas a tal fin.

ISO 27001: Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001[2].

Profesional en Seguridad Informática: Las organizaciones deben estar preparadas para proteger sus activos de información. Para ello se requiere de recursos humanos profesionales debidamente capacitados y actualizados, que puedan aplicar de forma adecuada los conceptos, metodologías, tecnologías, herramientas, normativas y estándares existentes para las distintas áreas en las que la seguridad informática tiene su aplicación tales como redes, sistemas operativos, aplicaciones, entre otras y que sean capaces de gestionar los incidentes, los riesgos y garantizar la continuidad del negocio, protegiendo los activos críticos.

[1] ACURIO DEL PINO, Santiago. Delitos Informáticos: Generalidades. {En línea}. {06 diciembre de 2014}. Disponible en: (http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf)
[2] 27001ACADEMY. ¿Qué es norma ISO 27001? {En línea}. {06 diciembre de 2014}. Disponible en: (http://www.iso27001standard.com/es/que-es-iso-27001/)

5.2 MARCO CONCEPTUAL

Confidencialidad: la información sólo es accesible a personas, entidades o procesos a los cuales se ha autorizado.

Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de personas, aplicaciones, entidades o procesos autorizados cuando así lo requieran.

Información: es un conjunto de datos significativos y pertinentes, que describen sucesos o entidades[3].

La información es considerada uno de los principales activos de las empresas y un factor clave para mejorar la productividad.

Proteger ese conjunto de datos es una acción que a menudo, no se tiene muy en cuenta y cualquier fallo técnico, humano, el acceso de un hacker al sistema, el extravío, o la destrucción de parte de esa información de negocio, podría traducirse en considerables pérdidas o en el paro de la actividad empresarial.

Integridad: la información se mantiene completa y libre de modificaciones no autorizadas.

Políticas de seguridad: es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma.

Las políticas de seguridad definen lo que está permitido y lo que está prohibido, permiten definir los procedimientos y herramientas necesarias, expresan el consenso de los “dueños” y permiten adoptar una buena actitud dentro de la organización[4].

Estas políticas deben ser divulgadas entre todos los empleados, de tal forma que genere la concienciación, entendimiento y compromiso de todos los involucrados. Las políticas deben contener claramente las prácticas que serán adoptadas por la compañía, y deben ser revisadas, y si es necesario actualizadas, periódicamente.

---

[3] THOMPSON, Iván. ¿Qué es información? {En línea}. {06 diciembre de 2014}. Disponible en: (http://www.promonegocios.net/mercadotecnia/que-es-informacion.html)

[4] UNAM. Esquemas de seguridad informática. {En línea}. {06 diciembre de 2014}. Disponible en: (http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/DefinicionPolitica.php)

Seguridad de los datos: es la protección contra la exposición accidental o intencional de los datos[5]. El precio de las infracciones de seguridad de datos, en términos monetarios y de credibilidad de las empresas es elevado. Todas las organizaciones necesitan aplicar seguridad a la información a fin de prevenir la divulgación de su información.

Seguridad informática: esta disciplina se encarga de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que articulados con prácticas de gobierno de tecnología de información, establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo[6].

Seguridad de la información: Es la disciplina que trata de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que nos exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información.

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.

SGSI: Es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. También llamado ISMS, por sus siglas en ingles de Information Security Management System[7].

El propósito de un Sistema de Gestión de la Seguridad 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.

---

[5] CISCO. Seguridad de datos. {En línea}. {06 diciembre de 2014}. Disponible en: (http://www.cisco.com/web/ES/solutions/es/information_security/index.html)

[6] GONZALES, Julián. ¿Seguridad Informática o Seguridad de la Información? {En línea}. {06 diciembre de 2014}. Disponible en: (http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html)

[7] ISO27000.ES. ¿Qué es un SGSI? {En línea}. {12 diciembre de 2014}. Disponible en: (http://www.iso27000.es/sgsi.html)

5.3 MARCO LEGAL

Ley 1273 de 2009 Protección de la Información y de los Datos en Colombia.

En la actualidad, e impulsada por el surgimiento de estándares, leyes y normativas, la seguridad se convierte en un requisito fundamental para cualquier tipo de organización. No sólo es un requerimiento de los bancos u organizaciones financieras, sino que se extiende a todo tipo y tamaño de organización.

Por medio de la Ley 1273 de 2009 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[8].

Esta ley tipificó como delitos una serie de conductas que tienen que ver con el manejo de datos personales, y que las empresas deben conocer para protegerse jurídicamente y evitar caer en alguno de estos delitos, los cuales pueden conducir a pagar grandes multas e incluso cárcel.

Es de esperar que los avances tecnológicos aporten grandes beneficios a la sociedad, pero estos algunas veces suelen ser mal utilizados por algunas personas que intentan apropiarse de información ilícitamente y de manera no autorizada, logrando divulgar, modificar, eliminar, obtener y denegar información, para así lograr obtener beneficios personales, económicos y/o de reconocimiento. Por este motivo y para tratar de controlar este tipo de conductas y que se continúe cometiendo este tipo de delitos informáticos, la Ley 1273 adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, el primero de ellos denominado: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y el segundo denominado “De los atentados informáticos y otras infracciones”, los cuales mediante una serie de artículos buscan evitar accesos abusivos a los sistemas informáticos, evitar obstaculizar un sistema informático, evitar la interceptación de datos, evitar daños informáticos, evitar el uso de software malicioso, la violación de datos personales, la suplantación de sitios web para capturar datos personales, evitar el hurto a través de medios informáticos y la trasferencia no consentida de activos.

[8] MINTIC. Ley 1273 de 2009. {En línea}. {14 febrero de 2015}. Disponible en: (http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf)

Ley 1266 de 2008 Habeas Data en Colombia

Esta Ley ha sido establecida por el gobierno nacional con el objeto de desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países[9].

Entre sus artículos, esta Ley busca que sea aplicable a todos los datos registrados en bancos de datos, sin importar si éstos son administrados por entidades públicas o privadas. Además contempla algunas definiciones tales como: Titular de la información, fuente de información, operador de información, dato personal, dato público, dato semiprivado, dato privado, lo que obliga a que cualquier persona u organización que maneje datos personales, está sujeta a cumplir esta ley, ofreciendo protección a la información y salvaguardando los derechos de los titulares de los datos.

De igual manera se establece que la información registrada en los bancos de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible y está prohibida la divulgación y registro de datos incompletos que induzcan a error. Así mismo se hace referencia a que los datos personales, salvo si se trata de información pública, no podrán ser accesibles desde Internet o por otros medios de comunicación masiva, a menos que se garantice un acceso restringido.

Esta ley también describe los derechos de los titulares de la información, los deberes de los operadores, las fuentes y los usuarios de la información, lo que permite entre otras cosas que el titular de la información conozca la información que sobre él exista en el banco de datos y solicite la actualización o corrección de los datos en caso de ser necesario.

Ley 1581 de 2012

[9] SIC. Ley Estatutaria No. 1266. {En línea}. {21 febrero de 2015}. Disponible en: (http://www.sic.gov.co/drupal/sites/default/files/files/ley1266_31_12_2008%281%29.pdf)

El 17 de octubre de 2012 el Gobierno Nacional expidió la Ley Estatutaria 1581 de 2012 mediante la cual se dictan disposiciones generales para la protección de datos personales.

Esta ley regula el derecho fundamental de hábeas data y a su vez busca proteger los datos personales registrados en cualquier base de datos que permita realizar operaciones de recolección, almacenamiento, uso, circulación o eliminación por parte de entidades de naturaleza pública y privada[10].

Esta ley permite a las personas tener acceso a la información que sobre ellas se ha venido recolectando y almacenando en bases de datos. Del mismo modo se podrá tener acceso a las bases de datos para incluir nuevos datos con el fin de ampliar la información del titular, actualizar la información para poner al día el contenido de dichas bases de datos, rectificar o corregir la información en caso de ser necesario, de tal manera que concuerde con la realidad, eliminar información de una base de datos, cuando se está haciendo un uso indebido de ella, o por simple voluntad del titular, salvo las excepciones previstas en la normativa.

La Ley obliga a todas las entidades públicas y empresas privadas a revisar el uso de los datos personales contenidos en sus sistemas de información y replantear sus políticas de manejo de información, fortaleciendo sus herramientas, ya que son ellas, las únicas responsables del tratamiento y administración de los datos y deberán garantizar los derechos de intimidad y hábeas data del titular de los datos.

Decreto 1377 de 2013

Este Decreto expedido el 27 de junio de 2013 tiene como objetivo facilitar la implementación y el cumplimiento de la ley 1581 reglamentando aspectos relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información, entre otros[11].

En síntesis este decreto plantea la exclusión del régimen general de protección de datos, a los datos personales o domésticos, haciendo referencia a aquellas actividades inscritas en la vida privada o familiar de las personas. También

[10] SECRETARIA GENERAL DEL SENADO. Ley Estatutaria 1581 de 2012. {En línea}. {28 febrero de 2015}. Disponible en: (http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html)

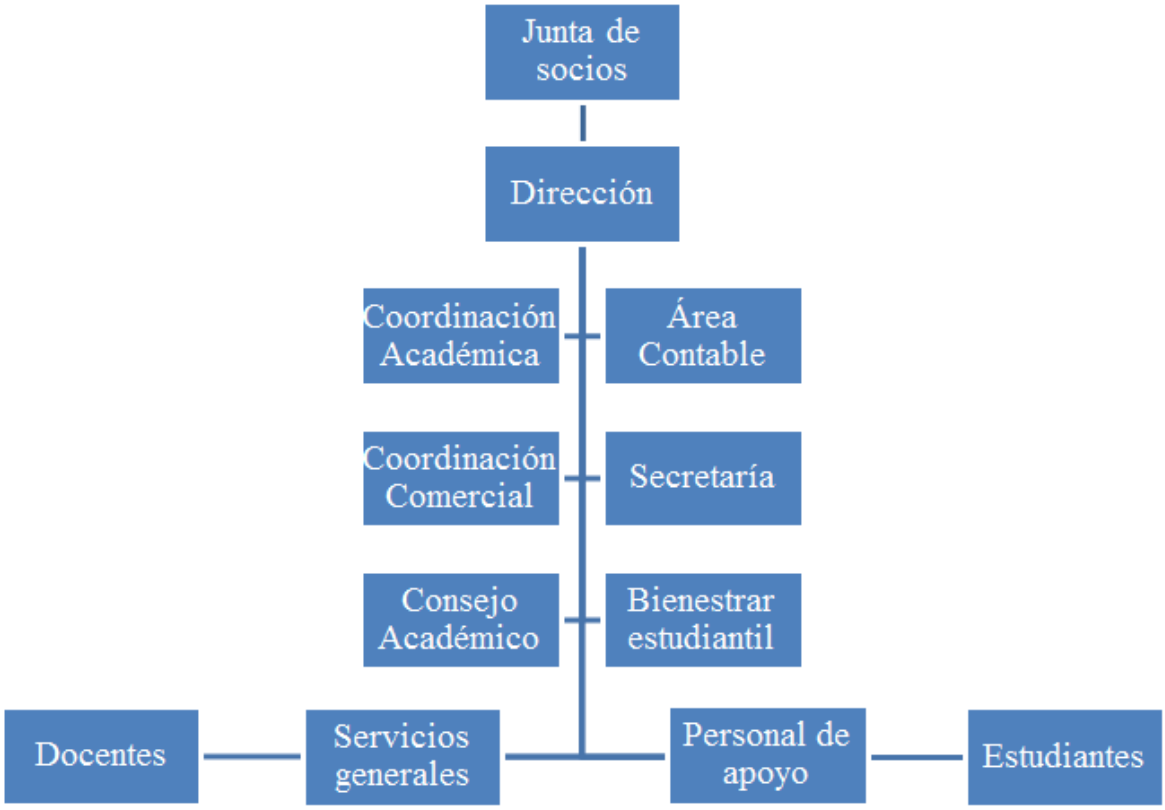
[11] MINTIC. Decreto 1377 de 2013. {En línea}. {21 febrero de 2015}. Disponible en: (http://www.mintic.gov.co/portal/604/articles-4274_documento.pdf)

describe la manera como se realiza la recolección de los datos personales y aclara que ésta no se podrá realizar sin autorización del Titular. Faculta al titular de revocar la autorización y solicitar mediante reclamo, la eliminación de los datos y se establecen sanciones en caso de incumplimiento. Igualmente se habla de los datos recolectados antes de la expedición del decreto e indica que los responsables de la información deberán solicitar a los titulares si desean que ellos continúen con el tratamiento de sus datos o si por el contrario desean ser borrados definitivamente, empleando para ello cualquier medio de comunicación para su divulgación. Además se aborda el tema de las políticas de tratamiento de la información e indica que los responsables del tratamiento deberán desarrollar sus políticas para el tratamiento de los datos personales y velar por su cumplimiento; asimismo se deberá informar de manera oportuna al Titular sobre la existencia de las políticas. También se describe el ejercicio de los derechos de los titulares, indicando que se debe establecer por parte de los encargados del tratamiento de la información personal, mecanismos que permitan a los titulares acceder a los datos y poder consultarlos. Para el caso de requerir actualización, rectificación y eliminación, deberán adaptarse medidas para asegurar que los datos personales estén acordes a los requerimientos de los Titulares.

5.4 MARCO CONTEXTUAL

La Institución SYSTEM PLUS PASTO LTDA, es una Institución de formación para el Trabajo y el Desarrollo Humano, que presta sus servicios de capacitación en carreras Técnicas desde hace 21 años en la ciudad de San Juan de Pasto. La Institución cuenta con más de 25 funcionarios entre administrativos, docentes y personal de apoyo y más de 300 estudiantes.

Figura 1. Organigrama Institución de Educación para el Trabajo y el Desarrollo Humano System Plus Pasto Ltda



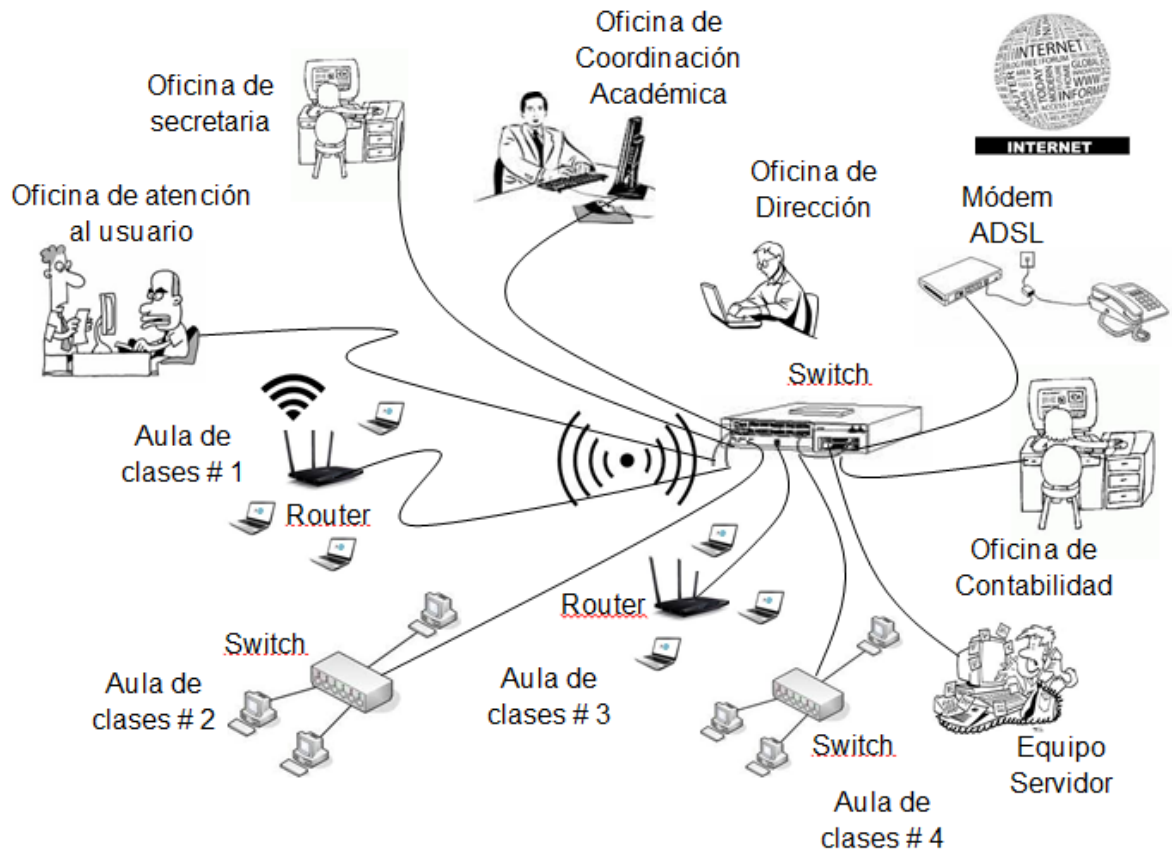
Fuente: Manual de Calidad System Plus Pasto.

Cada funcionario del área administrativa y el área académica de la Institución SYSTEM PLUS PASTO LTDA, realiza sus actividades diarias en su propia oficina o espacio de trabajo, el cual cuenta con un equipo o computador y acceso a internet para desarrollar sus actividades.

El área administrativa se encarga de la administración de personal, de la gestión administrativa organizacional, manejo de los recursos materiales, financieros y de servicios en general.

El área académica se encarga de manejar aspectos relacionados con admisiones de estudiantes, registro de calificaciones, información de egresados, constancias, certificaciones, pagos, convenios con Instituciones, información de contenidos de los programas, asignación académica de los docentes, entre otros.

Figura 2. Diagrama de red Institución de Educación para el Trabajo y el Desarrollo Humano System Plus Pasto Ltda



Fuente: Autor del Proyecto.

5.4.1 Descripción del croquis

El diseño de la red de la Institución SYSTEM PLUS PASTO LTDA, cuenta con el número de equipos que se detallan a continuación:

Oficina	Equipo	Sistema Operativo
Atención al usuario	1 Computador de escritorio	Windows 7 32 bits
Secretaria	1 Computador de escritorio	Windows 7 32 bits
Dirección	1 Computador portátil	Windows 7 32 bits
Coordinación Académica	1 Computador de escritorio	Windows 7 32 bits
Coordinación Comercial	1 Computador de escritorio	Windows 7 32 bits
Coordinación Tabletas Digitales	1 Computador de escritorio	Windows 7 32 bits
Servidor	1 Computador de escritorio	Windows 7 32 bits
Contabilidad	1 Computador de escritorio	Windows 7 32 bits
Aula de clases # 1	20 Computadores portátiles	Windows 7 32 bits
Aula de clases # 2	10 Computadores de escritorio	Windows 7 32 bits
Aula de clases # 3	18 Computadores portátiles	Windows 7 32 bits
Aula de clases # 4	15 Computadores portátiles	Windows 7 32 bits

Equipos de conexión	
Modem ADSL	2
Switch principal	1
Switch aulas de clase	2
Router inalámbrico	2

Software	
Sistema Operativo licenciado	71
Suite Office 2013 licenciado	71
Antivirus Kaspersky licenciado	70
Software contable SIIGO	2

6. METODOLOGÍA

Con el propósito de llevar un orden lógico y sistémico para la implantación del Sistema de Gestión de la Seguridad de la Información en las áreas administrativa y académica de la Institución SYSTEM PLUS PASTO LTDA, y tal como lo establece la norma ISO/IEC 27001, se usará el modelo PHVA, el cual es un modelo dividido en cuatro fases que permite Planificar, Hacer, Verificar y Actuar y éstos a su vez se repiten para alcanzar una mejora continua en base a los resultados obtenidos.

Dentro de la fase de Planificación lo que se pretende es lograr una idea más acertada en relación con la realidad y el estado actual de las áreas administrativa y académica de la Institución SYSTEM PLUS PASTO LTDA, por lo que se necesita verificar el estado actual, a través de la realización de un análisis diferencial, el cual se realizará mediante un chequeo de cada uno de los controles con sus respectivos objetivos de seguridad según lo dispuesto en la norma ISO/IEC 27001, y éste permitirá conocer el estado general de las áreas administrativa y académica de la Institución SYSTEM PLUS PASTO LTDA, entorno a la seguridad de la información, permitiendo la definición del alcance.

Para ello se hará uso de una tabla donde se relacionará cada una de las normas y se verificará el estado actual de las áreas de la Institución, en relación a la implementación de cada control y objetivo.

Posteriormente se define el alcance del SGSI y se establece el compromiso de la dirección. Así mismo se determinan las personas responsables y las responsabilidades o funciones que tendrá cada una de ellas y que harán parte del equipo de seguridad de la Institución, y se crea un documento específico para esta definición.

Luego se continúa con la definición de políticas de seguridad, las cuales son unas reglas generales de comportamiento definidas para una adecuada interacción entre los usuarios y los activos de la Institución. Éstas políticas y procedimientos deben estar hechos a la medida y por ello se realiza un proceso de validación en conjunto con la Institución con el fin de generar políticas y procedimientos que se ajusten a ésta. Como punto de partida para la definición de las políticas se tendrá como referencia el análisis de riesgo realizado y los controles de la norma ISO 27001.

Del mismo modo se definen los objetivos de la seguridad de la información entorno a las características de la Institución.

Así mismo se define una metodología de análisis de riesgos, la cual permitirá desarrollar análisis de amenazas y vulnerabilidades tanto de personas, de procesos, de recursos como de sistemas, con el fin de determinar el nivel de riesgo. También, se pretende realizar una serie de observaciones que se constituirán en la base para formular las acciones de prevención, mitigación y respuesta que contempla el plan de continuidad del negocio.

Dentro de la segunda fase denominada de Ejecución, se define el alcance y el tiempo estimado para implantar el SGSI en las áreas administrativa y académica de la Institución SYSTEM PLUS PASTO LTDA, es por eso que para este proyecto se ha establecido un tiempo de 6 meses para su implantación y una vez organizado, se debe presentar ante el comité de seguridad para su aprobación y puesta en marcha.

Se hace el análisis de riesgos de acuerdo a la metodología seleccionada para posteriormente implementar las medidas de seguridad y mitigar los riesgos a los que se encuentran expuestas las áreas administrativa y académica de la Institución SYSTEM PLUS PASTO LTDA.

También se elaboraran algunos documentos que son necesarios en caso que la Institución desee certificar el SGSI en las áreas descritas. Entre estos documentos figura el documento de las políticas de seguridad, el cual al no incluir detalles técnicos, es muy conveniente que todas las personas de la Institución lo conozcan para alcanzar los objetivos de la Institución. Igualmente se debe elaborar un documento de procedimientos, que desarrolla los objetivos marcados por las políticas y en él se detalla de forma más técnica como alcanzar los objetivos planteados en las políticas. A diferencia de las políticas, los procedimientos deben ser conocidos por las personas que lo requieran para el desarrollo de sus funciones. Posteriormente se debe elaborar el documento con las instrucciones que describa los comandos técnicos que se deben realizar para la ejecución de los Procedimientos y por último se debe elaborar un documento con los Registros que evidencian la efectiva implantación del sistema y el cumplimiento de los requisitos.

Posteriormente se debe gestionar roles y responsabilidades mediante la selección de un grupo de personas del área con perfiles de gestión, experiencia y técnicos en el área de la informática y seguridad, ya que serán ellos los encargados de planear, crear, mantener, revisar, auditar y mejorar el sistema. Por lo tanto se debe especificar en un documento los compromisos y responsabilidades que asume el equipo de trabajo que se estipula como comité de seguridad. En dicho comité debemos involucrar a por lo menos una persona de dirección para tener el respaldo de las directivas institucionales en las decisiones que se requieran tomar.

Para medir la eficacia de cada uno de los controles de seguridad implantados se deberá gestionar indicadores, en donde cada indicador es la medida de referencia.

Uno de los aspectos que contempla la norma ISO/IEC 27001 es la revisión cada cierto tiempo de los aspectos más importantes que se han presentado con

relación al SGSI implantados. De esta manera la dirección puede verificar y/o monitorear el sistema y establecer compromisos para realizar las mejoras necesarias.

En cuanto al procedimiento de auditorías internas, se debe elaborar un documento donde se establezcan los requisitos que los auditores internos deben tener, las áreas a auditar en la Institución y se establece la forma como se presentará el informe de la auditoría ante los directivos y empleados de la Institución. Con esto se pretende hacer la revisión de cumplimiento de cada aspecto que involucra el estándar ISO/IEC 27001; por consiguiente, se considera necesario elaborar un documento que presente toda la planificación para la ejecución de las auditorías internas que la Institución debe realizar con el objetivo de verificar el cumplimiento de las condiciones de la normativa y poder certificarse o mantener la vigencia de certificación obtenida en la implantación del SGSI de la Institución.

Para la declaración de aplicabilidad es necesario un documento que especifique los controles de seguridad de acuerdo a la normativa que aplica a las áreas de la Institución. Ésta se puede representar a través de una tabla que especifique cada uno de los controles aplicables.

Dentro de la tercera fase denominada de Verificación, se deberá efectuar la revisión por parte de la dirección del cumplimiento de los objetivos propuestos, el alcance proyectado, las medidas de seguridad implementadas para mitigar los riesgos. El proceso de seguimiento y monitorización del SGSI se hace con base a los resultados que arroja los indicadores de la seguridad de la información propuestos para verificación de la eficacia y efectividad de los controles implementados.

En la última fase que conlleva a Actuar, se busca mantener y mejorar el sistema con la implantación de mejoras, acciones correctivas y preventivas en

relación a los resultados obtenidos de la revisión por dirección y las auditorías internas.

Para la obtención de dicha información se emplearán entrevistas, encuestas y observación directa, y de esta forma se obtendrán los requerimientos en cuanto a seguridad de las áreas escogidas para el proyecto. De esta manera todo lo que se aplicará, se basará directamente en la cotidianidad de las áreas administrativa y académica de la Institución SYSTEM PLUS PASTO LTDA.

Los funcionarios serán notificados y recibirán información sobre sus incidencias de seguridad.

En este sentido, la Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo.

La Gestión del Riesgo, en su forma general tiene cuatro fases:

- *Análisis:* Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.
- *Clasificación:* Determina si los riesgos encontrados y los riesgos restantes son aceptables.
- *Reducción:* Define e implementa las medidas de protección. Además sensibiliza y capacita los usuarios conforme a las medidas.

- *Control:* Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento.

Y como último paso se pretende concienciar al personal del área administrativa y área académica de la Institución SYSTEM PLUS PASTO LTDA, acerca de los problemas de seguridad existentes en dichas áreas, para que hagan un adecuado tratamiento frente a las amenazas y procedan de acuerdo a las reglas establecidas en las políticas de seguridad.

6.1 PERSONAS QUE PARTICIPAN EN EL PROCESO

Las personas que participarán en el desarrollo del proyecto son:

1 ingeniero en la ejecución del proyecto:

Ing. Carlos Arturo Pulido Rodríguez.

1 encargado del área Administrativa

Economista María Eugenia Benavides Cerón.

1 encargado del área Académica

Mg. Lilian Dayana Cruz Cruz.

7. RECURSOS DISPONIBLES

Para el desarrollo del proyecto se contará con la participación de los funcionarios de las áreas administrativa y académica de la Institución SYSTEM PLUS PASTO LTDA. Para la revisión bibliográfica se cuenta con todos los recursos de la Biblioteca de la Universidad UNAD, entre los que podemos mencionar revistas especializadas, artículos, tesis, monografías y demás trabajos de grado expuestos por egresados de la Universidad y otras Instituciones relacionadas con los temas objeto de estudio.

Para el desarrollo del proyecto, la Institución dispone de computadores de mesa y portátiles con discos duros de gran tamaño y procesadores CoreI3, I5 y I7 y memoria RAM de 4GB, equipos que proporcionan conectividad a nivel de red tales como routers alámbricos e inalámbricos, switches, y redes; además se dispone de acceso a internet y software libre y propietario con permiso de uso, como antivirus, antispywares, firewalls, Sistemas operativos, suites de oficina, navegadores, herramientas para la copia de seguridad, bloqueo y restricción, y herramientas más especializadas tales como Kali Linux, Caine, Clonezilla y por último se dispone de acceso a la información y bases de datos que se requiera para las actividades de identificación de vulnerabilidades y seguridad de la misma, hasta lograr un modelo de seguridad que proteja la información que se maneja en las áreas administrativa y académica de la Institución SYSTEM PLUS PASTO LTDA.

8. CRONOGRAMA

Tabla 1. Registro pormenorizado del plan de acción

Actividades	MES 1				MES 2				MES 3				MES 4				MES 5				MES 6			
	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4
Verificar el estado actual de las áreas de la Institución a través de un análisis diferencial																								
Establecer un chequeo de cada uno de los controles y los objetivos de seguridad según Anexo A, norma ISO 27001:2013.																								
Redefinir alcance del SGSI y establecer compromiso de la dirección																								
Definir responsabilidades y funciones a los miembros del equipo de seguridad.																								
Definir políticas de seguridad.																								
Definir objetivos de seguridad de la información entorno a las áreas de la Institución.																								
Definir la metodología de análisis de riesgo a utilizar.																								
Diseñar el plan de SGSI																								
Presentación del tiempo estimado para el diseño.																								
Presentación ante el comité de seguridad y puesta en marcha																								
Analizar los riesgos según la metodología seleccionada																								
Elaborar documentos que define la ISO 27001:2013 para certificar el SGSI																								
Especificar el documento con los compromisos y responsabilidades que asume el equipo de trabajo de seguridad.																								
Gestionar los indicadores																								
Medir la eficacia de cada uno de los controles de seguridad implantados.																								
Verificar y monitorear el sistema por parte de la dirección																								

Establecer compromisos para realizar las mejoras necesarias.																								
Planificar la ejecución de las auditorías internas																								
Elaborar el documento que permita establecer los requisitos para los auditores internos y las áreas a auditar.																								
Declarar la aplicabilidad de los controles																								
Elaborar el documento que especifique los controles de seguridad de acuerdo a la norma ISO 27001:2013.																								
Verificación y revisión por parte de la dirección																								
Verificar el cumplimiento de los objetivos propuestos.																								
Verificar el alcance proyectado.																								
Verificar las medidas de seguridad propuestas.																								
Verificar mediante las auditorías internas que los objetivos de control, controles, procesos y procedimientos del SGSI cumplen con la norma ISO 27001:2013.																								
Mantener y mejorar el sistema																								
Presentar mejoras, acciones correctivas y preventivas en base a los resultados obtenidos de la revisión por dirección y las auditorías internas.																								

Fuente: Autor del Proyecto.

9. DESARROLLO DEL PROYECTO

9.1 ACTIVOS DE INFORMACIÓN

Las áreas Administrativa y Académica de la Institución SYSTEM PLUS PASTO LTDA, actualmente cuentan con los siguientes activos de información:

Tabla 2. Capital Humano

Cargo	Cantidad
Directora	1
Contadora	1
Coordinadora Académica	1
Coordinadora Comercial	1
Volanteadores	2
Secretarias	2
Asesora psicológica	1
Coordinadora Proyecto Tabletas Digitales	1
Asesores Comerciales	2
Practicantes Empresariales	2
Personal de servicios generales aseo	1
Personal de servicios generales seguridad	1
Docentes	15

Fuente: Autor del Proyecto.

Tabla 3. Hardware

Oficina	Equipo
Dirección	1 PC portátil y 1 impresora
Coordinación Académica	1 PC de escritorio y 1 impresora
Coordinación Comercial	1 Computador de escritorio
Coordinación Tabletas Digitales	1 Computador de escritorio
Atención al usuario	1 Computador portátil
Secretaria	1 PC de escritorio y 1 impresora
Servidor	1 Computador de escritorio
Contabilidad	1 Computador de escritorio
Aula de clases # 1	20 Computadores portátiles

Tabla 3. (Continuación)

Oficina	Equipo
Aula de clases # 2	10 Computadores de escritorio
Aula de clases # 3	18 Computadores portátiles
Aula de clases # 4	15 Computadores portátiles

Equipos de conexión	
Modem ADSL	2
Switch principal	1
Switch aulas de clase	2
Router inalámbrico	2

Fuente: Autor del Proyecto.

Tabla 4. Software

Software	Tipo de Licencia	Cantidad
Sistema Operativo Windows 7 32 bits	Por volumen - 1 año	71
Office 2013 Word, Excel, PowerPoint, Access	Por volumen - 1 año	71
Antivirus Kaspersky Workstations	Comercial - 1 año	70
Software contable SIIGO v8.1	Comercial - 1 año	2
Servicio de web hosting http://www.systempluspasto.edu.co/	Comercial - 1 año	1

Fuente: Autor del Proyecto.

Tabla 5. Información

Área responsable de la información: Área Administrativa			
Nombre de la información	**Descripción**	**Uso**	**Soporte de información**
Control de pagos	Documento que se elabora cada trimestre. Incluye el nivel, estudiantes, horario, docente, cuotas/pagos, fecha de inicio/fin de nivel.	Privada	Documento físico, Digital

Tabla 5. (Continuación)

Nombre de la información	Descripción	Uso	Soporte de información
Venta interna	Documento que se elabora a partir de la información suministrada por el Control de pagos del trimestre anterior. Indica los módulos que a cursado el estudiante y los niveles que va a cursar el próximo trimestre.	Privada	Documento físico, Digital
Correspondencia interna enviada	Documentos que cursan entre las áreas de la Institución: Oficios, memorandos, circulares, citaciones, solicitudes, etc.	Privada	Documento físico
Resoluciones	Documento donde se plasman las decisiones a las que se llega, después de analizar las situaciones planteadas.	Privada	Documento físico
Archivos inactivos	Documentos guardados de los primeros 15 años de existencia de la Institución.	Confidencial	Documento físico
Cartas descriptivas del personal	Documento que describe las funciones de los cargos asignados al personal de la Institución.	Privada	Documento físico, Digital
Contrato servicio de internet banda ancha	Documento que pone de manifiesto las obligaciones acordadas entre la empresa prestadora del servicio de internet y la Institución.	Privada	Documento fíisico
CDTs paso a paso	Inversión de la Institución para obtener beneficios y realizar el pago de las prestaciones de los empleados.	Confidencial	Documento físico

Tabla 5. (Continuación)

Nombre de la información	Descripción	Uso	Soporte de información
Convenios	Acuerdos de la Institución con otras empresas o Instituciones para que mutuamente se colaboren.	Privada	Documento físico
Cronogramas	Documento donde se organiza el desarrollo de actividades de cada trimestre.	Pública	Documento físico, Digital
Cotizaciones y propuestas	Ofertas económicas que se envían a empresas, instituciones y/o personas independientes.	Pública	Documento físico
Contrato de arrendamiento	Documento que indica la entrega temporal de la edificación por parte del propietario y se autoriza el uso de las instalaciones físicas por parte de System Plus Pasto.	Confidencial	Documento físico
Comité Paritario de Salud Ocupacional-COPASO	Registro de las actividades relacionadas con las prácticas saludables, entorno a la adquisición de hábitos seguros en las distintas áreas de la Institución.	Privada	Documento físico
Certificados	Documento de tipo administrativo en el que la alcaldía, la gobernación, y otras instituciones certifican que la Institución está legalmente acreditada.	Confidencial	Documento físico
DIAN	Documentos que se deben reportar anualmente por la Institución System Plus Pasto a la DIAN.	Privada	Documento físico, Digital

Tabla 5. (Continuación)

Nombre de la información	Descripción	Uso	Soporte de información
Difusión de documentos	Formulario que especifica el acuse de recibo o justificante de recepción para certificar la entrega de documentos o participación en las reuniones.	Pública	Documento físico
Estados financieros	Informes financieros para dar a conocer la situación económica y financiera de la Institución y los cambios que experimenta en un periodo determinado.	Confidencial	Documento físico, Digital
Franquicia	Contrato mediante el cual se otorga por parte de System Plus a nivel Nacional, una licencia de uso a System Plus Pasto, para su aprovechamiento comercial.	Confidencial	Documento físico
Gestión de Calidad	Normas a partir de las cuales la Institución System Plus Pasto administra de manera organizada la calidad de sus operaciones.	Privada	Documento físico, Digital
Inventario	Lista ordenada de los bienes y demás recursos que posee la Institución.	Privada	Documento físico, Digital
Licencias de software	Contrato entre la Cooperativa de Promoción Integral Educativa COPIE y la Institución, donde se permite el uso de software, cumpliendo con términos legales de uso.	Confidencial	Documento físico, Digital

Tabla 5. (Continuación)

Nombre de la información	Descripción	Uso	Soporte de información
Nómina	Documento que relaciona los nombres y sueldos de los empleados vinculados a la Institución.	Confidencial	Documento físico
Normas y derechos	Decretos, artículos, leyes legales importantes para la Institución.	Confidencial	Documento físico
Practicantes	Personal que apoya las actividades de la Institución.	Privada	Documento físico
Presupuesto	Se realiza una vez al año y contiene la proyección de ingresos y egresos de la institución	Confidencial	Documento físico, Digital
Plan de mejoramiento	Documento correspondiente a la gestión de la calidad.	Privada	Documento físico, Digital
Publicidad	Propuestas publicitarias especialmente emisoras radiales.	Privada	Documento físico, Digital
Selección de Personal	Proceso encaminado a prever cuáles de los aspirantes tendrán éxito si se les contrata.	Privada	Documento físico
Reglamento interno de trabajo	Documento que regula las relaciones internas de System Plus con sus trabajadores	Privada	Documento físico, Digital
Secretaria de educación	Todas las licencias de funcionamiento de la Institución.	Confidencial	Documento físico
Siigo – Software Contable	Reportes de comprobantes, control de activos fijos, ventas, recaudos, cotizaciones, facturas y estados de cartera.	Confidencial	Documento físico
Seguros de vida	Cubrimiento en caso de un evento accidental, enfermedad/fallecimiento.	Confidencial	Documento físico

Tabla 5. (Continuación)

Nombre de la información	Descripción	Uso	Soporte de información
Solicitudes	Se adjuntan todos los requerimientos solicitados por los funcionarios de la Institución	Privada	Documento físico
Seminarios	Es la conformación de cursos de profundización, en las áreas técnicas ofrecidas por System Plus a sus estudiantes	Privada	Documento físico
Sensibilización de personal	Formación y sensibilización del personal	Privada	Documento físico
Talento digital	Listado estudiantes becados por el Ministerio de las Tics	Confidencial	Documento físico, Digital
Proyecto Educativo Institucional – PEI System Plus Pasto	Contienen la estructura del servicio que ofrece la institución	Confidencial	Documento físico, Digital
Dinero recogido por pagos	Ingresos	Privada	Documento físico, Digital

Área responsable de la información: Área Académica			
Nombre de la información	**Descripción**	**Uso**	**Soporte de información**
Asignación académica	Documento que se elabora cada trimestre e Indica los cursos a dictar por cada docente según su perfil profesional.	Privada	Documento físico, Digital
Cronograma planeación académica	Documento que incluye la lista de actividades académicas trimestrales.	Privada	Documento físico, Digital
Desarrollo curricular	Documento que muestra la estructura de los programas de formación Técnica que dicta la Institución.	Privada	Documento físico, Digital

Tabla 5. (Continuación)

Nombre de la información	Descripción	Uso	Soporte de información
Registro SIET	Registro de los programas Técnicos en el Sistema de Información de la Educación para el Trabajo y el Desarrollo Humano.	Pública	Digital
Control de asistencia de estudiantes	Permite controlar asistencia, llegadas tarde, permisos de los estudiantes a clases	Pública	Documento físico
Registro de notas	Servicio que permite a los docentes realizar el ingreso de notas de los estudiantes a través de internet	Privada	Documento físico, Digital
Respuesta a reclamos y sugerencias dispuestas en el buzón de sugerencias	Se establecen las manifestaciones de insatisfacción de los estudiantes con los servicios prestados por la Institución.	Privada	Documento físico, Digital
Evaluación docente	Permite asegurar y garantizar mejores resultados dentro del proceso formativo.	Privada	Digital
Comunicación con egresados	Sistema de información para lograr una mejor comunicación entre los egresados y la Institución.	Pública	Base de datos
Normas y procedimientos académicos	Documento que registra información relativa a los órganos administrativos, facilitando las labores de los docentes y estudiantes.	Privada	Documento físico, Digital
Reglamento interno académico	Garantiza el desarrollo del Proyecto Educativo Institucional.	Privada	Documento físico

Tabla 5. (Continuación)

Nombre de la información	Descripción	Uso	Soporte de información
Implementación de seminarios académicos	Listado de diplomados, cursos y demás oferta académica de formación.	Privada	Documento físico
Convenios desarrollo de prácticas empresariales	Acuerdo que se desarrolla en función de las actividades que se realizarán y el lugar donde se llevará a cabo dicha práctica.	Confidencial	Documento físico
Seguimiento plan de trabajo estudiantes	Permite evaluar la calidad y ejecución del trabajo de los estudiantes, en relación con el plan de acción.	Privada	Documento físico

Fuente: Autor del Proyecto.

En la siguiente tabla se clasifican los activos de las áreas Administrativa y Académica de la Institución SYSTEM PLUS PASTO LTDA, de una forma más detallada, tal como lo plantea MAGERIT[12] en su Libro 2, en la sección "2. Tipos de activos", con el propósito de identificar y valorar la relevancia de los activos determinantes para el proyecto.

Tabla 6. Clasificación según el tipo de activo

[ESSENTIAL] ACTIVOS ESENCIALES
La información que se maneja en la Institución es la siguiente: [nfo] información [vr] datos vitales (act1) Control de pagos (act2) Venta interna (act3) Convenios (act4) Estados financieros [per] datos de carácter personal [A] nivel alto

[12] MAGERIT. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. {En línea}. {11 julio de 2015}. Disponible en: (http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Vk-MKXYrLIV)

(act5) Licencias de software
(act6) Registro de notas
[M] nivel medio
(act7) Registro SIET
(act8) Nómina
[classified] datos clasificados
[R] difusión limitada
(act9) Correspondencia interna enviada
(act10) Resoluciones
(act11) Cartas descriptivas del personal
(act12) Certificados Cámara de Comercio
(act13) Reglamento interno de trabajo
(act14) Secretaria de educación
(act15) Proyecto Educativo Institucional – PEI System Plus Pasto

[D] DATOS / INFORMACIÓN

La Institución cuenta con los siguientes datos para prestar sus servicios:
[password] Credenciales
(act16) Contraseña de acceso a los computadores, Contraseña de acceso a los equipos de comunicación, Contraseña de acceso a la red Wi-Fi, Contraseña de acceso a programas y Contraseña de apertura de archivos.

[S] SERVICIOS

Para los usuarios internos como externos la Institución presta los siguientes servicios:
[www] World wide web
(act17) www.systempluspasto.edu.co

[SW] APLICACIONES (SOFTWARE)

Entre las aplicaciones que usa la Institución están:
[std] estándar
[browser] navegador web
(act18) Internet Explorer, Mozilla Firefox y Google Chrome
[office] ofimática
(act19) Microsoft Office 2013 (Excel, PowerPoint, Word)
[av] antivirus
(act20) kaspersky internet security
[os] sistema operativo
(act21) Microsoft Windows 7 Professional
[hypervisor] gestor de máquinas virtuales
(act22) VMware Workstation

Otros

- Siigo – Software Contable
- Moodle
- VLC media player
- Foxit Reader
- Winamp

- PhotoShop
- Corel Draw
- Winrar

[HW] EQUIPOS INFORMÁTICOS (HARDWARE)

Dentro de los equipos informáticos que posee la Institución están los siguientes:
[pc] informática personal
(act23) Computadores de escritorio y equipos portátiles
[mobile] informática móvil
(act24) smartphone
[peripheral] periféricos
[print] medios de impresión
(act25) Impresoras láser e Impresoras de chorro de tinta
HP Laser Jet 1020, Epson L555 y Epson WorkForce 325
[scan] escáneres
(act26) Escáner Genius ColorPage-Vivid Pro
[network] soporte de la red
[modem] modems
(act27) Modems
Modem Mitrastar DSL-2401HN-T1C, Modem ZTE W300 y Modem BHS Mini Mitrastar
[switch] conmutadores
(act28) Conmutadores
TP-LINK TL-SG1024D Gigabit switch, Switch D-Link DES1016A
[wap] punto de acceso inalámbrico
(act29) Punto de acceso inalámbrico
TP-LINK N750 TL-WDR4300

[COM] REDES DE COMUNICACIONES

Entre los medios de transporte de información que posee la Institución están:
[PSTN] red telefónica
(act30) Red telefónica
[pp] punto a punto
(act31) Punto a punto
[wifi] red inalámbrica
(act32) Red inalámbrica
[LAN] red local
(act33) Red local
[Internet] Internet
(act34) Internet

[MEDIA] SOPORTES DE INFORMACIÓN

La Institución utiliza los siguientes soportes de información electrónicos:
[electronic] electrónicos
[disk] discos
(act35) Discos
[cd] (CD-ROM)

(act36) cd's
[usb] memorias USB
(act37) Memorias USB
[dvd] DVD
(act38) dvd's
La Institución utiliza los siguientes soportes de información no electrónicos:
[non_electronic] no electrónicos
[printed] material impreso
(act39) Material impreso

[AUX] EQUIPAMIENTO AUXILIAR

La Institución cuenta con los siguientes equipos auxiliares:
[power] fuentes de alimentación
(act40) Fuentes de alimentación
[ups] sistemas de alimentación ininterrumpida
[cabling] cableado
(act41) cableado
[wire] cable eléctrico
(act42) cable eléctrico
[furniture] mobiliario
(act43) Armarios, escritorios, sillas, etc.
Otros

- Detector de movimiento
- Extintor de incendios
- CCTV Circuito Cerrado de Televisión

[L] INSTALACIONES

[site] recinto
(act44) La infraestructura donde se localiza los sistemas de información y comunicación, está situada en una edificación antigua, considerada patrimonio arquitectónico de la ciudad y está ubicada en la calle 18A # 25 – 55 Pasaje Corazón de Jesús, en pleno centro de la ciudad de San Juan de Pasto.

[P] PERSONAL

Dentro del personal de la Institución están:
(act45)
[ue] usuarios externos

- Todos los estudiantes

[ui] usuarios internos

- Administrativos
- Docentes

[sub] subcontratas

- Personal de vigilancia privada

[prov] proveedores

- Proveedores de partes y suministros

Fuente: Autor del Proyecto.

9.2 VALORACIÓN DE LOS ACTIVOS

La Metodología MAGERIT propone cinco dimensiones de valoración:

[D] Disponibilidad
[I] Integridad de los datos
[C] Confidencialidad de la información
[A] Autenticidad
[T] Trazabilidad

La valoración de los activos, se realiza teniendo en cuenta el impacto que causa la alteración, interrupción de los activos disponibles en las áreas Administrativa y Académica de la Institución SYSTEM PLUS PASTO LTDA, estimando cuales serían las pérdidas al no contar con el activo.

Para estimar el nivel de importancia de los activos, se emplea la escala cuantitativa de 0 a 10 propuesta por MAGERIT, en la que el valor 0 representa un riesgo muy bajo o despreciable y el valor 10 representa un riesgo extremadamente grave, tal como se muestra en la siguiente tabla:

Tabla 7. Criterios de valoración

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: MAGERIT – versión 3.0 Libro II – Catálogo de Elementos.

Una vez identificados los activos y la escala a utilizar, se procede a realizar la valoración de los mismos, teniendo en cuenta las dimensiones en las que el activo es relevante.

Tabla 8. Valoración de los activos

[ESSENTIAL] ACTIVOS ESENCIALES					
ACTIVO	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
(act1) Control de pagos	-	9	8	9	9
(act2) Venta interna	-	8	6	8	7
(act3) Convenios	-	8	9	9	8
(act4) Estados financieros	-	9	9	9	8
(act5) Licencias de software	-	8	9	9	8
(act6) Registro de notas	-	9	8	9	9
(act7) Registro SIET	-	9	8	9	8
(act8) Nómina	-	8	9	9	9
(act9) Correspondencia interna enviada	-	6	7	7	7
(act10) Resoluciones	-	7	7	6	7
(act11) Cartas descriptivas del personal	-	6	6	6	6
(act12) Certificados Cámara de Comercio	-	8	6	2	7
(act13) Reglamento interno de trabajo	-	7	6	5	6
(act14) Secretaria de educación	-	8	8	5	8
(act15) Proyecto Educativo Institucional – PEI	-	8	8	6	8
[D] DATOS / INFORMACIÓN					
ACTIVO	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
(act16) Contraseñas	8	8	9	9	8
[S] SERVICIOS					
ACTIVO	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
(act17) World wide web	8	7	6	6	5
[SW] APLICACIONES (SOFTWARE)					
ACTIVO	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
(act18) Navegador web	5	2	3	5	6
(act19) Ofimática	6	3	4	5	5
(act20) Antivirus	9	6	5	6	6
(act21) Sistema Operativo	9	6	5	8	8
(act22) Gestor de máquinas virtuales	5	2	2	3	2
[HW] EQUIPOS INFORMÁTICOS (HARDWARE)					
ACTIVO	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
(act23) Equipos de escritorio / Portátiles	9	8	8	8	7
(act24) Smartphone	7	6	7	7	5
(act25) Impresoras	8	8	5	7	3
(act26) Escáner	7	6	5	7	3
(act27) Módems	9	8	8	8	7
(act28) Conmutadores	8	8	8	8	7
(act29) Punto de acceso inalámbrico	7	8	8	8	7

Tabla 8. (Continuación)

[COM] REDES DE COMUNICACIONES					
ACTIVO	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
(act30) Red telefónica	9	3	8	8	5
(act31) Punto a punto	6	5	6	6	3
(act32) Red inalámbrica	8	5	9	7	4
(act33) Red local	8	5	8	8	4
(act34) Internet	9	6	9	9	6
[MEDIA] SOPORTES DE INFORMACIÓN					
ACTIVO	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
(act35) Discos	9	7	8	8	7
(act36) CD-ROM	5	5	7	7	5
(act37) Memorias USB	7	6	8	8	6
(act38) DVD	5	5	7	7	5
(act39) Material impreso	9	8	9	8	7
[AUX] EQUIPAMIENTO AUXILIAR					
ACTIVO	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
(act40) Fuentes de alimentación	7	6	5	2	2
(act41) Cableado	8	7	5	6	5
(act42) Cable electric	7	7	6	6	5
(act43) Mobiliario	5	2	2	3	3
[L] INSTALACIONES					
ACTIVO	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
(act44) Recinto	8	7	5	3	2
[P] PERSONAL					
ACTIVO	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
(act45) Personal	No suelen identificarse				

Fuente: Autor del Proyecto.

9.3 IDENTIFICACIÓN Y VALORACIÓN DE LAS AMENAZAS

MAGERIT contiene una lista extensa de amenazas que afectan a un activo en específico. Una vez determinadas las que se pueden materializar en las áreas Administrativa y Académica de la Institución SYSTEM PLUS PASTO LTDA, se procede a asignarles una valoración usando el sentido de Probabilidad, para lo cual se utilizará la siguiente tabla de frecuencias:

Tabla 9. Probabilidad de ocurrencia

Frecuencia	Rango	Valor
Muy alta	1 vez cada semana	100
Alta	1 vez cada mes	75
Media	1 vez cada trimestre	50
Baja	1 vez cada semestre	25
Muy baja	1 vez cada año	1

Fuente: Autor del Proyecto.

Para cada una de las dimensiones se establecerá un valor en escala porcentual, el cual medirá el impacto que causaría si se llegara a materializar cada una de las amenazas por activo.

Tabla 10. Escala porcentual de impactos

Porcentaje	Criterio
90%-100%	Muy alto
71%-89%	Alto
50%-70%	Medio
21%-49%	Bajo
0%-20%	Muy bajo

Fuente: Autor del Proyecto.

Tabla 11. Valoración de amenazas

AMENAZAS POR ACTIVO	FREQ	[D]	[I]	[C]	[A]	[T]
[ESSENTIAL] ACTIVOS ESENCIALES						
(act1) Control de pagos		90%	100%	90%	90%	
[E.1] Errores de los usuarios	100	90%	100%	70%		
[E.15] Alteración accidental de la información	100		100%			
[E.18] Destrucción de información	100	90%				

Tabla 11. (Continuación)

AMENAZAS POR ACTIVO	FREQ	[D]	[I]	[C]	[A]	[T]
[E.19] Fugas de información	100			70%		
[A.5] Suplantación de la identidad del usuario	1		100%	90%	90%	
[A.15] Modificación deliberada de la información	75		100%			
[A.18] Destrucción de información	50	90%				
[A.19] Divulgación de información	50			90%		
(act2) Venta interna		90%	100%	70%		
[E.1] Errores de los usuarios	50	70%	100%	70%		
[E.15] Alteración accidental de la información	75		100%			
[E.18] Destrucción de información	50	90%				
[E.19] Fugas de información	50			40%		
(act3) Convenios		70%	100%	80%		
[E.1] Errores de los usuarios	1	40%	80%	50%		
[E.15] Alteración accidental de la información	50		100%			
[E.18] Destrucción de información	50	70%				
[E.19] Fugas de información	50			80%		
[A.19] Divulgación de información	50			80%		
(act4) Estados financieros		100%	100%	90%	90%	
[E.1] Errores de los usuarios	75	100%	100%	90%		
[E.15] Alteración accidental de la información	100		100%			
[E.18] Destrucción de información	75	100%				
[E.19] Fugas de información	100			90%		
[A.5] Suplantación de la identidad del usuario	1		100%	90%	90%	
[A.6] Abuso de privilegios de acceso	75	70%	100%	90%		
[A.15] Modificación deliberada de la información	50		100%			
[A.19] Divulgación de información	25			80%		
(act5) Licencias de software		50%	50%	70%		
[E.1] Errores de los usuarios	1	40%	20%	50%		
[E.2] Errores del administrador	1	50%	50%	70%		
[E.18] Destrucción de información	1	50%				
[E.19] Fugas de información	25			40%		
[A.6] Abuso de privilegios de acceso	50	40%	40%	70%		
(act6) Registro de notas		100%	100%	100%	100%	
[E.1] Errores de los usuarios	50	90%	100%	70%		
[E.15] Alteración accidental de la información	50		100%			
[E.18] Destrucción de información	50	100%				
[E.19] Fugas de información	50			70%		
[A.5] Suplantación de la identidad del usuario	50		100%	100%	100%	
[A.6] Abuso de privilegios de acceso	50	100%	100%	100%		
[A.11] acceso no autorizado	50		100%	80%		
[A.15] Modificación deliberada de la información	50		100%			
[A.18] Destrucción de información	50	100%				
[A.19] Divulgación de información	50			80%		
(act7) Registro SIET		80%	100%	90%		
[E.1] Errores de los usuarios	25	70%	100%	40%		
[E.15] Alteración accidental de la información	25		100%			

Tabla 11. (Continuación)

AMENAZAS POR ACTIVO	FREQ	[D]	[I]	[C]	[A]	[T]
[E.18] Destrucción de información	25	80%				
[E.19] Fugas de información	25			70%		
[A.6] Abuso de privilegios de acceso	25	70%	90%	90%		
(act8) Nómina		100%	100%	90%		
[E.1] Errores de los usuarios	75	100%	90%	80%		
[E.15] Alteración accidental de la información	75		100%			
[E.18] Destrucción de información	75	90%				
[E.19] Fugas de información	75			90%		
[A.6] Abuso de privilegios de acceso	75	90%	100%	80%		
[A.11] acceso no autorizado	50		100%	80%		
[A.18] Destrucción de información	50	100%				
[A.19] Divulgación de información	50			80%		
(act9) Correspondencia interna enviada		70%	100%	100%		
[E.1] Errores de los usuarios	100	70%	80%	100%		
[E.15] Alteración accidental de la información	100		100%			
[E.18] Destrucción de información	100	70%				
[E.19] Fugas de información	100			80%		
(act10) Resoluciones		70%	100%	70%		
[E.1] Errores de los usuarios	75	70%	80%	70%		
[E.15] Alteración accidental de la información	50		100%			
[E.18] Destrucción de información	50	40%				
[E.19] Fugas de información	50			40%		
(act11) Cartas descriptivas del personal		40%	100%	40%		
[E.1] Errores de los usuarios	50	20%	70%	40%		
[E.15] Alteración accidental de la información	1		100%			
[E.18] Destrucción de información	1	40%				
[E.19] Fugas de información	1			40%		
(act12) Certificados Cámara de Comercio		20%				
[E.18] Destrucción de información	1	20%				
(act13) Reglamento interno de trabajo		40%	100%	40%		
[E.1] Errores de los usuarios	1	20%	50%	40%		
[E.15] Alteración accidental de la información	1		100%			
[E.18] Destrucción de información	25	40%				
[E.19] Fugas de información	1			40%		
(act14) Secretaria de educación		70%	80%	70%		
[E.1] Errores de los usuarios	1	40%	70%	50%		
[E.15] Alteración accidental de la información	1		80%			
[E.18] Destrucción de información	1	70%				
[E.19] Fugas de información	1			70%		
(act15) Proyecto Educativo Institucional – PEI		80%	100%	80%		
[E.1] Errores de los usuarios	1	40%	70%	20%		
[E.15] Alteración accidental de la información	1		100%			
[E.18] Destrucción de información	1	80%				
[E.19] Fugas de información	1			80%		
[D] DATOS / INFORMACIÓN						
(act16) Contraseñas		100%	100%	100%	100%	
[E.1] Errores de los usuarios	100	100%	100%	100%		
[E.2] Errores del administrador	50	100%	100%	100%		

Tabla 11. (Continuación)

AMENAZAS POR ACTIVO	FREQ	[D]	[I]	[C]	[A]	[T]
[E.15] Alteración accidental de la información	100		100%			
[E.18] Destrucción de información	100	100%				
[E.19] Fugas de información	100			100%		
[A.5] Suplantación de la identidad del usuario	100		100%	100%	100%	
[A.6] Abuso de privilegios de acceso	75	90%	80%	100%		
[A.11] acceso no autorizado	100		100%	90%		
[A.15] Modificación deliberada de la información	75		90%			
[A.18] Destrucción de información	25	80%				
[A.19] Divulgación de información	75			90%		
[S] SERVICIOS						
(act17) World wide web		90%	90%	90%	80%	
[E.1] Errores de los usuarios	100	80%	20%	80%		
[E.2] Errores del administrador	75	70%	40%	50%		
[E.9] Errores de [re-]encaminamiento	100			90%		
[E.15] Alteración accidental de la información	75		80%			
[E.18] Destrucción de información	100	80%				
[E.19] Fugas de información	100			70%		
[A.5] Suplantación de la identidad del usuario	100		70%	80%	80%	
[A.7] Uso no previsto	100	80%	70%	80%		
[A.9] [Re-]encaminamiento de mensajes	75			80%		
[A.11] acceso no autorizado	100		80%	70%		
[A.13] Repudio	100		90%			
[A.24] Denegación de servicio	25	90%				
[SW] APLICACIONES (SOFTWARE)						
(act18) Navegador web		100%	70%	90%		
[I.5] Avería de origen físico o lógico	75	50%				
[E.1] Errores de los usuarios	100	70%	50%	80%		
[E.2] Errores del administrador	50	50%	40%	70%		
[E.8] Difusión de software dañino	100	90%	70%	90%		
[E.9] Errores de [re-]encaminamiento	75			80%		
[E.19] Fugas de información	100			70%		
[E.20] Vulnerabilidades de los programas	100	80%	50%	80%		
[E.21] Errores de mantenimiento / actualización de programas	100	80%	40%			
[A.7] Uso no previsto	100	80%	70%	80%		
[A.8] Difusión de software dañino	100	100%	50%	90%		
[A.19] Divulgación de información	75			70%		
[A.22] Manipulación de programas	25	80%	20%	80%		
(act19) Ofimática		100%	80%	80%		
[I.5] Avería de origen físico o lógico	75	70%				
[E.1] Errores de los usuarios	100	90%	80%	80%		
[E.2] Errores del administrador	50	70%	40%	70%		
[E.8] Difusión de software dañino	75	100%	50%	80%		
[E.18] Destrucción de información	1	80%				
[E.19] Fugas de información	50			80%		
[E.20] Vulnerabilidades de los programas	75	80%	50%	80%		

Tabla 11. (Continuación)

AMENAZAS POR ACTIVO	FREQ	[D]	[I]	[C]	[A]	[T]
[E.21] Errores de mantenimiento / actualización de programas	75	80%	40%			
[A.7] Uso no previsto	100	50%	40%	50%		
[A.8] Difusión de software dañino	25	70%	50%	70%		
[A.18] Destrucción de información	1	70%				
(act20) Antivirus		100%	80%	90%	80%	
[I.5] Avería de origen físico o lógico	50	80%				
[E.1] Errores de los usuarios	25	90%	40%	40%		
[E.2] Errores del administrador	50	80%	50%	70%		
[E.8] Difusión de software dañino	50	80%	50%	80%		
[E.18] Destrucción de información	100	100%				
[E.19] Fugas de información	50			80%		
[E.20] Vulnerabilidades de los programas	75	80%	50%	80%		
[E.21] Errores de mantenimiento / actualización de programas	75	80%	40%			
[A.5] Suplantación de la identidad del usuario	75		50%	80%	80%	
[A.7] Uso no previsto	100	90%	70%	80%		
[A.8] Difusión de software dañino	50	100%	80%	90%		
(act21) Sistema Operativo		100%	100%	90%	90%	
[I.5] Avería de origen físico o lógico	75	80%				
[E.1] Errores de los usuarios	100	90%	70%	70%		
[E.2] Errores del administrador	75	90%	70%	80%		
[E.8] Difusión de software dañino	75	100%	50%	90%		
[E.18] Destrucción de información	75	90%				
[E.19] Fugas de información	75			90%		
[E.20] Vulnerabilidades de los programas	75	80%	50%	80%		
[E.21] Errores de mantenimiento / actualización de programas	75	80%	70%			
[A.5] Suplantación de la identidad del usuario	75		80%	90%	90%	
[A.6] Abuso de privilegios de acceso	75	100%	70%	80%		
[A.7] Uso no previsto	100	80%	70%	70%		
[A.8] Difusión de software dañino	75	90%	80%	90%		
[A.11] acceso no autorizado	100		100%	90%		
[A.15] Modificación deliberada de la información	75		80%			
[A.22] Manipulación de programas	25	80%	20%	80%		
(act22) Gestor de máquinas virtuales		100%	40%	70%		
[I.5] Avería de origen físico o lógico	25	40%				
[E.1] Errores de los usuarios	1	50%	20%	20%		
[E.2] Errores del administrador	50	70%	40%	50%		
[E.8] Difusión de software dañino	75	100%	40%	70%		
[E.19] Fugas de información	50			70%		
[E.20] Vulnerabilidades de los programas	50	50%	20%	50%		
[E.21] Errores de mantenimiento / actualización de programas	50	50%	20%			
[A.7] Uso no previsto	75	70%	40%	40%		
[HW] EQUIPOS INFORMÁTICOS (HARDWARE)						

Tabla 11. (Continuación)

AMENAZAS POR ACTIVO	FREQ	[D]	[I]	[C]	[A]	[T]
(act23) Equipos de escritorio / Portátiles		100%	100%	100%		
[N.1] Fuego	1	100%				
[N.2] Daños por agua	1	100%				
[I.1] Fuego	25	90%				
[I.2] Daños por agua	50	80%				
[I.5] Avería de origen físico o lógico	75	90%				
[I.6] Corte del suministro eléctrico	75	40%				
[E.2] Errores del administrador	50	70%	60%	70%		
[E.23] Errores de mantenimiento / actualización de equipos	50	100%				
[E.24] Caída del sistema por agotamiento de recursos	50	100%				
[E.25] Pérdida de equipos	50	100%		100%		
[A.6] Abuso de privilegios de acceso	75	100%	70%	70%		
[A.7] Uso no previsto	100	90%	80%	80%		
[A.11] acceso no autorizado	75		100%	90%		
[A.23] Manipulación de los equipos	75	90%		80%		
[A.24] Denegación de servicio	25	80%				
[A.25] Robo	1	100%		100%		
(act24) Smartphone		80%	90%	100%		
[N.1] Fuego	1	50%				
[N.2] Daños por agua	1	50%				
[I.1] Fuego	25	50%				
[I.2] Daños por agua	50	40%				
[I.5] Avería de origen físico o lógico	50	50%				
[I.6] Corte del suministro eléctrico	75	20%				
[E.2] Errores del administrador	75	70%	70%	80%		
[E.23] Errores de mantenimiento / actualización de equipos	50	50%				
[E.24] Caída del sistema por agotamiento de recursos	75	70%				
[E.25] Pérdida de equipos	75	50%		100%		
[A.6] Abuso de privilegios de acceso	75	80%	50%	80%		
[A.7] Uso no previsto	100	80%	70%	80%		
[A.11] acceso no autorizado	75		90%	90%		
[A.23] Manipulación de los equipos	75	70%		80%		
[A.24] Denegación de servicio	1	70%				
[A.25] Robo	50	80%		90%		
(act25) Impresoras		90%	50%	80%		
[N.1] Fuego	1	70%				
[N.2] Daños por agua	1	70%				
[I.1] Fuego	25	70%				
[I.2] Daños por agua	25	60%				
[I.5] Avería de origen físico o lógico	75	70%				
[I.6] Corte del suministro eléctrico	75	60%				
[E.2] Errores del administrador	50	80%	20%	50%		
[E.23] Errores de mantenimiento / actualización de equipos	50	80%				

Tabla 11. (Continuación)

AMENAZAS POR ACTIVO	FREQ	[D]	[I]	[C]	[A]	[T]
[E.24] Caída del sistema por agotamiento de recursos	75	80%				
[E.25] Pérdida de equipos	25	90%		40%		
[A.6] Abuso de privilegios de acceso	75	40%	50%	80%		
[A.7] Uso no previsto	100	80%	20%	80%		
[A.23] Manipulación de los equipos	75	80%		40%		
[A.24] Denegación de servicio	25	80%				
[A.25] Robo	25	80%		20%		
(act26) Escáner		70%	50%	80%		
[N.1] Fuego	1	50%				
[N.2] Daños por agua	1	50%				
[I.1] Fuego	25	50%				
[I.2] Daños por agua	25	40%				
[I.5] Avería de origen físico o lógico	25	50%				
[I.6] Corte del suministro eléctrico	75	40%				
[E.23] Errores de mantenimiento / actualización de equipos	50	70%				
[E.25] Pérdida de equipos	25	50%		20%		
[A.6] Abuso de privilegios de acceso	75	40%	50%	80%		
[A.7] Uso no previsto	50	70%	40%	50%		
[A.23] Manipulación de los equipos	50	70%		40%		
[A.25] Robo	25	70%		20%		
(act27) Módems		100%	70%	80%		
[N.1] Fuego	1	90%				
[N.2] Daños por agua	1	80%				
[I.1] Fuego	25	90%				
[I.2] Daños por agua	25	80%				
[I.5] Avería de origen físico o lógico	50	80%				
[I.6] Corte del suministro eléctrico	75	90%				
[E.2] Errores del administrador	50	90%	40%	80%		
[E.23] Errores de mantenimiento / actualización de equipos	50	100%				
[E.24] Caída del sistema por agotamiento de recursos	50	100%				
[E.25] Pérdida de equipos	25	100%		40%		
[A.6] Abuso de privilegios de acceso	75	100%	20%	80%		
[A.7] Uso no previsto	25	100%	20%	70%		
[A.11] acceso no autorizado	50		70%	80%		
[A.23] Manipulación de los equipos	50	90%		80%		
[A.24] Denegación de servicio	25	90%				
[A.25] Robo	25	80%		20%		
(act28) Conmutadores		80%	40%	80%		
[N.1] Fuego	1	80%				
[N.2] Daños por agua	1	80%				
[I.1] Fuego	25	80%				
[I.2] Daños por agua	1	70%				
[I.5] Avería de origen físico o lógico	1	50%				
[I.6] Corte del suministro eléctrico	75	70%				

Tabla 11. (Continuación)

AMENAZAS POR ACTIVO	FREQ	[D]	[I]	[C]	[A]	[T]
[E.23] Errores de mantenimiento / actualización de equipos	50	70%				
[E.25] Pérdida de equipos	25	80%		20%		
[A.7] Uso no previsto	75	70%	40%	80%		
[A.25] Robo	1	50%		20%		
(act29) Punto de acceso inalámbrico		90%	70%	90%		
[N.1] Fuego	1	80%				
[N.2] Daños por agua	1	70%				
[I.1] Fuego	25	80%				
[I.2] Daños por agua	25	70%				
[I.5] Avería de origen físico o lógico	75	70%				
[I.6] Corte del suministro eléctrico	75	60%				
[E.2] Errores del administrador	50	90%	40%	80%		
[E.23] Errores de mantenimiento / actualización de equipos	50	90%				
[E.24] Caída del sistema por agotamiento de recursos	75	80%				
[E.25] Pérdida de equipos	25	90%		20%		
[A.6] Abuso de privilegios de acceso	75	90%	20%	80%		
[A.7] Uso no previsto	50	80%	20%	80%		
[A.11] acceso no autorizado	50		70%	80%		
[A.23] Manipulación de los equipos	75	80%		90%		
[A.24] Denegación de servicio	25	80%				
[A.25] Robo	25	90%		20%		
[COM] REDES DE COMUNICACIONES						
(act30) Red telefónica		70%	50%	100%	100%	
[E.2] Errores del administrador	1	70%	40%	70%		
[E.19] Fugas de información	100			100%		
[A.5] Suplantación de la identidad del usuario	75		50%	90%	100%	
[A.7] Uso no previsto	100	70%	40%	80%		
[A.9] [Re-]encaminamiento de mensajes	50			80%		
[A.14] Interceptación de información	75			100%		
[A.19] Divulgación de información	75			80%		
(act31) Punto a punto		100%	100%	100%	80%	
[E.2] Errores del administrador	50	80%	50%	70%		
[E.18] Destrucción de información	75	80%				
[E.19] Fugas de información	100			80%		
[A.5] Suplantación de la identidad del usuario	75		70%	80%	80%	
[A.6] Abuso de privilegios de acceso	75	100%	100%	100%		
[A.7] Uso no previsto	75	80%	80%	80%		
(act32) Red inalámbrica		100%	80%	100%	90%	
[E.2] Errores del administrador	75	80%	70%	90%		
[E.15] Alteración accidental de la información	75		70%			
[E.18] Destrucción de información	100	100%				
[E.19] Fugas de información	100			100%		
[E.24] Caída del sistema por agotamiento de recursos	75	80%				
[A.5] Suplantación de la identidad del usuario	100		70%	90%	90%	

Tabla 11. (Continuación)

AMENAZAS POR ACTIVO	FREQ	[D]	[I]	[C]	[A]	[T]
[A.6] Abuso de privilegios de acceso	75	100%	20%	90%		
[A.7] Uso no previsto	100	100%	80%	90%		
[A.9] [Re-]encaminamiento de mensajes	75			90%		
[A.11] acceso no autorizado	75		80%	90%		
[A.12] Análisis de tráfico	75			100%		
[A.14] Interceptación de información	75			100%		
[A.15] Modificación deliberada de la información	75		80%			
[A.19] Divulgación de información	75			80%		
[A.24] Denegación de servicio	25	80%				
(act33) Red local		100%	90%	100%	90%	
[E.2] Errores del administrador	75	80%	50%	90%		
[E.15] Alteración accidental de la información	75		80%			
[E.18] Destrucción de información	100	80%				
[E.19] Fugas de información	100			90%		
[E.24] Caída del sistema por agotamiento de recursos	75	80%				
[A.5] Suplantación de la identidad del usuario	75		80%	100%	90%	
[A.6] Abuso de privilegios de acceso	75	100%	80%	90%		
[A.7] Uso no previsto	100	90%	80%	80%		
[A.9] [Re-]encaminamiento de mensajes	75			80%		
[A.11] acceso no autorizado	75		90%	90%		
[A.12] Análisis de tráfico	75			90%		
[A.14] Interceptación de información	75			100%		
[A.15] Modificación deliberada de la información	75		90%			
[A.19] Divulgación de información	75			70%		
[A.24] Denegación de servicio	25	80%				
(act34) Internet		100%	100%	100%	100%	
[E.2] Errores del administrador	100	100%	70%	90%		
[E.15] Alteración accidental de la información	100		100%			
[E.18] Destrucción de información	100	90%				
[E.19] Fugas de información	100			100%		
[E.24] Caída del sistema por agotamiento de recursos	75	90%				
[A.5] Suplantación de la identidad del usuario	100		80%	90%	100%	
[A.6] Abuso de privilegios de acceso	50	90%	90%	90%		
[A.7] Uso no previsto	100	80%	70%	80%		
[A.9] [Re-]encaminamiento de mensajes	75			80%		
[A.11] acceso no autorizado	75		80%	90%		
[A.12] Análisis de tráfico	50			80%		
[A.14] Interceptación de información	75			90%		
[A.15] Modificación deliberada de la información	75		80%			
[A.19] Divulgación de información	75			80%		
[MEDIA] SOPORTES DE INFORMACIÓN						
(act35) Discos		100%	100%	100%		
[N.1] Fuego	1	100%				

Tabla 11. (Continuación)

AMENAZAS POR ACTIVO	FREQ	[D]	[I]	[C]	[A]	[T]
[N.2] Daños por agua	1	100%				
[I.1] Fuego	25	100%				
[I.2] Daños por agua	50	90%				
[I.5] Avería de origen físico o lógico	50	80%				
[I.6] Corte del suministro eléctrico	75	70%				
[I.10] Degradación de los soportes de almacenamiento de la información	1	100%				
[E.1] Errores de los usuarios	50	80%	100%	100%		
[E.2] Errores del administrador	50	100%	90%	90%		
[E.15] Alteración accidental de la información	100		100%			
[E.18] Destrucción de información	100	100%				
[E.19] Fugas de información	75			100%		
[E.23] Errores de mantenimiento / actualización de equipos	75	100%				
[E.25] Pérdida de equipos	50	100%		100%		
[A.7] Uso no previsto	100	80%	80%	90%		
[A.11] acceso no autorizado	50		100%	100%		
[A.15] Modificación deliberada de la información	50		100%			
[A.18] Destrucción de información	50	100%				
[A.19] Divulgación de información	75			100%		
[A.23] Manipulación de los equipos	1	80%		100%		
[A.25] Robo	25	100%		100%		
(act36) CD-ROM		100%	70%	100%		
[N.1] Fuego	1	70%				
[N.2] Daños por agua	25	70%				
[I.1] Fuego	25	70%				
[I.2] Daños por agua	50	50%				
[I.5] Avería de origen físico o lógico	75	50%				
[I.10] Degradación de los soportes de almacenamiento de la información	1	100%				
[E.18] Destrucción de información	100	80%				
[E.19] Fugas de información	100			100%		
[E.25] Pérdida de equipos	75	80%		100%		
[A.11] acceso no autorizado	75		70%	90%		
[A.18] Destrucción de información	75	80%				
[A.19] Divulgación de información	75			90%		
[A.25] Robo	75	80%		90%		
(act37) Memorias USB		100%	100%	100%		
[N.1] Fuego	1	80%				
[N.2] Daños por agua	25	80%				
[I.1] Fuego	25	80%				
[I.2] Daños por agua	50	80%				
[I.5] Avería de origen físico o lógico	75	80%				
[I.10] Degradación de los soportes de almacenamiento de la información	25	100%				
[E.1] Errores de los usuarios	100	100%	100%	90%		
[E.2] Errores del administrador	75	50%	80%	90%		

Tabla 11. (Continuación)

AMENAZAS POR ACTIVO	FREQ	[D]	[I]	[C]	[A]	[T]
[E.15] Alteración accidental de la información	100		100%			
[E.18] Destrucción de información	100	100%				
[E.19] Fugas de información	100			100%		
[E.23] Errores de mantenimiento / actualización de equipos	50	80%				
[E.25] Pérdida de equipos	75	90%		100%		
[A.7] Uso no previsto	100	80%	90%	90%		
[A.11] acceso no autorizado	75		100%	100%		
[A.15] Modificación deliberada de la información	75		100%			
[A.18] Destrucción de información	75	90%				
[A.19] Divulgación de información	100			100%		
[A.23] Manipulación de los equipos	75	80%		90%		
[A.25] Robo	75	90%		90%		
(act38) DVD		100%	70%	100%		
[N.1] Fuego	1	70%				
[N.2] Daños por agua	25	70%				
[I.1] Fuego	25	70%				
[I.2] Daños por agua	25	50%				
[I.5] Avería de origen físico o lógico	75	50%				
[I.10] Degradación de los soportes de almacenamiento de la información	1	100%				
[E.18] Destrucción de información	100	80%				
[E.19] Fugas de información	100			100%		
[E.25] Pérdida de equipos	75	80%		100%		
[A.11] acceso no autorizado	75		70%	90%		
[A.18] Destrucción de información	75	80%				
[A.19] Divulgación de información	75			80%		
[A.25] Robo	75	80%		90%		
(act39) Material impreso		100%	100%	100%		
[N.1] Fuego	1	100%				
[N.2] Daños por agua	50	100%				
[I.1] Fuego	50	100%				
[I.2] Daños por agua	75	100%				
[E.1] Errores de los usuarios	100	100%	100%	100%		
[E.15] Alteración accidental de la información	100		100%			
[E.18] Destrucción de información	100	100%				
[E.19] Fugas de información	100			100%		
[A.11] acceso no autorizado	75		90%	100%		
[A.18] Destrucción de información	75	100%				
[A.19] Divulgación de información	75			90%		
[A.25] Robo	1	100%		100%		
[AUX] EQUIPAMIENTO AUXILIAR						
(act40) Fuentes de alimentación		70%		20%		
[N.1] Fuego	25	70%				
[N.2] Daños por agua	50	70%				
[I.1] Fuego	75	70%				
[I.2] Daños por agua	25	70%				

Tabla 11. (Continuación)

AMENAZAS POR ACTIVO	FREQ	[D]	[I]	[C]	[A]	[T]
[I.5] Avería de origen físico o lógico	25	50%				
[I.6] Corte del suministro eléctrico	75	20%				
[E.23] Errores de mantenimiento / actualización de equipos	50	70%				
[E.25] Pérdida de equipos	75	50%		20%		
[A.25] Robo	1	50%		20%		
(act41) Cableado		90%		20%		
[N.1] Fuego	25	90%				
[N.2] Daños por agua	1	90%				
[I.1] Fuego	25	90%				
[I.2] Daños por agua	25	20%				
[I.5] Avería de origen físico o lógico	1	20%				
[E.23] Errores de mantenimiento / actualización de equipos	1	80%				
[E.25] Pérdida de equipos	1	80%		20%		
[A.25] Robo	1	80%		20%		
(act42) Cable electric		100%		20%		
[N.1] Fuego	25	90%				
[N.2] Daños por agua	1	100%				
[I.1] Fuego	25	100%				
[I.2] Daños por agua	25	20%				
[I.5] Avería de origen físico o lógico	1	80%				
[E.23] Errores de mantenimiento / actualización de equipos	1	80%				
[E.25] Pérdida de equipos	1	90%		20%		
[A.25] Robo	1	90%		20%		
(act43) Mobiliario		50%		20%		
[N.1] Fuego	1	40%				
[N.2] Daños por agua	25	40%				
[I.1] Fuego	50	50%				
[I.2] Daños por agua	1	20%				
[I.5] Avería de origen físico o lógico	1	20%				
[A.25] Robo	25	40%		20%		
[L] INSTALACIONES						
(act44) Recinto		80%	70%	90%		
[N.1] Fuego	1	40%				
[N.2] Daños por agua	25	40%				
[I.1] Fuego	1	60%				
[I.2] Daños por agua	50	20%				
[E.18] Destrucción de información	1	80%				
[E.19] Fugas de información	1			90%		
[A.11] acceso no autorizado	25		70%	80%		
[P] PERSONAL						
(act45) Personal		90%	80%	100%		
[E.7] Deficiencias en la organización	75	80%				
[E.19] Fugas de información	100			100%		
[E.28] Indisponibilidad del personal	75	80%				
[A.28] Indisponibilidad del personal	1	80%				

Tabla 11. (Continuación)

AMENAZAS POR ACTIVO	FREQ	[D]	[I]	[C]	[A]	[T]
[A.29] Extorsión	1	90%	70%	90%		
[A.30] Ingeniería social	100	90%	80%	90%		

Fuente: Autor del Proyecto.

Tabla 12. Resumen valoración de amenazas por activo

AMENAZAS POR ACTIVO	FREQ	[D]	[I]	[C]	[A]	[T]
[ESSENTIAL] ACTIVOS ESENCIALES						
(act1) Control de pagos		90%	100%	90%	90%	
(act2) Venta interna		90%	100%	70%		
(act3) Convenios		70%	100%	80%		
(act4) Estados financieros		100%	100%	90%	90%	
(act5) Licencias de software		50%	50%	70%		
(act6) Registro de notas		100%	100%	100%	100%	
(act7) Registro SIET		80%	100%	90%		
(act8) Nómina		100%	100%	90%		
(act9) Correspondencia interna enviada		70%	100%	100%		
(act10) Resoluciones		70%	100%	70%		
(act11) Cartas descriptivas del personal		40%	100%	40%		
(act12) Certificados Cámara de Comercio		20%				
(act13) Reglamento interno de trabajo		40%	100%	40%		
(act14) Secretaria de educación		70%	80%	70%		
(act15) Proyecto Educativo Institucional – PEI		80%	100%	80%		
[D] DATOS / INFORMACIÓN						
(act16) Contraseñas		100%	100%	100%	100%	
[S] SERVICIOS						
(act17) World wide web		90%	90%	90%	80%	
[SW] APLICACIONES (SOFTWARE)						
(act18) Navegador web		100%	70%	90%		
(act19) Ofimática		100%	80%	80%		
(act20) Antivirus		100%	80%	90%	80%	
(act21) Sistema Operativo		100%	100%	90%	90%	
(act22) Gestor de máquinas virtuales		100%	40%	70%		
[HW] EQUIPOS INFORMÁTICOS (HARDWARE)						
(act23) Equipos de escritorio / Portátiles		100%	100%	100%		
(act24) Smartphone		80%	90%	100%		
(act25) Impresoras		90%	50%	80%		
(act26) Escáner		70%	50%	80%		
(act27) Módems		100%	70%	80%		
(act28) Conmutadores		80%	40%	80%		
(act29) Punto de acceso inalámbrico		90%	70%	90%		

Tabla 12. (Continuación)

AMENAZAS POR ACTIVO	FREQ	[D]	[I]	[C]	[A]	[T]
[COM] REDES DE COMUNICACIONES						
(act30) Red telefónica		70%	50%	100%	100%	
(act31) Punto a punto		100%	100%	100%	80%	
(act32) Red inalámbrica		100%	80%	100%	90%	
(act33) Red local		100%	90%	100%	90%	
(act34) Internet		100%	100%	100%	100%	
[MEDIA] SOPORTES DE INFORMACIÓN						
(act35) Discos		100%	100%	100%		
(act36) CD-ROM		100%	70%	100%		
(act37) Memorias USB		100%	100%	100%		
(act38) DVD		100%	70%	100%		
(act39) Material impreso		100%	100%	100%		
(act40) Fuentes de alimentación		70%		20%		
[MEDIA] SOPORTES DE INFORMACIÓN						
(act41) Cableado		90%		20%		
(act42) Cable electric		100%		20%		
(act43) Mobiliario		50%		20%		
(act44) Recinto		80%	70%	90%		
(act45) Personal		90%	80%	100%		

Fuente: Autor del Proyecto.

9.4 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

9.4.1 Política de seguridad de la red

Código: P01	**POLÍTICA SEGURIDAD DE LA RED SYSTEM PLUS PASTO LTDA**	
Versión: 01		
Elaborado:	Ing. Carlos Arturo Pulido Rodríguez	
Revisado:	María Eugenia Benavides Cerón	
Fecha:	30 de noviembre de 2015	

NOTA DE CONFIDENCIALIDAD

Este documento es de propiedad exclusiva de la Institución SYSTEM PLUS PASTO LTDA y su uso y distribución sólo está autorizado al interior de la Institución y por parte del personal debidamente habilitado, quedando prohibida la divulgación y/o reproducción total o parcial del contenido de éste sin la debida autorización por parte del responsable de la Seguridad de la Información de la Institución.

Descripción de la política:

La política de seguridad de la red precisa los controles de acceso a la red y los recursos de red, presentes en la Institución SYSTEM PLUS PASTO LTDA, propendiendo porque ésta red sea debidamente protegida contra accesos no autorizados.

Alcance:

Esta política se aplica a todos los usuarios de la Institución SYSTEM PLUS PASTO LTDA, ya sean administrativos, docentes, personal de apoyo, estudiantes, practicantes, proveedores y personal externo.

Aplicable

La Institución SYSTEM PLUS PASTO LTDA en su interés por proteger su información y los recursos de procesamiento de la misma demostrará el compromiso de la Dirección en este esfuerzo, promoviendo que el personal cuente con el nivel deseado de conciencia en seguridad de la información para la correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan las Políticas de seguridad de la información de la Institución.

Todos los funcionarios de la Institución deben tener especial cuidado de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad y el buen nombre de la Institución SYSTEM PLUS PASTO LTDA.

Esta política es aplicable durante el empleo y aún después de terminado el empleo.

Responsabilidades de la Dirección:

Autorizar los mecanismos de control para los dominios de seguridad definidos.

Demostrar su compromiso con la seguridad de la información por medio de su aprobación de las políticas y demás lineamientos que desee establecer la Institución.

Promover la importancia de la seguridad de la información entre los funcionarios de la Institución SYSTEM PLUS PASTO LTDA, así como también del personal externo; motivando el entendimiento, la toma de conciencia y el cumplimiento de las políticas establecidas para la seguridad de la información.

Incluir en el proceso disciplinario existente en la Institución, el tratamiento de las faltas de cumplimiento a las políticas de seguridad o los incidentes de seguridad que lo ameriten.

Responsabilidades del encargado de la Seguridad de la Información:

Establecer revisiones periódicas de cumplimiento de los controles definidos, con el fin de proteger el acceso a la red de personas no autorizadas.

Asegurar que las aplicaciones limiten el número de intentos errados de conexión a la red, además de llevar un sistema de registro de dichos eventos.

Velar por que cada uno de los usuarios que acceden a la red cuente con una única identificación.

Definir los dominios de seguridad y de la implementación, activación y mantenimiento de los mecanismos de protección de los recursos y la información con que cuenta la red.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Los empleados de la Institución SYSTEM PLUS PASTO LTDA deberán permanecer atentos, y en caso de detectar actividades sospechosas, deberán reportarlas al Encargado de la Seguridad Informática.

El personal externo a la Institución SYSTEM PLUS PASTO LTDA, que por sus funciones haga uso de la red de la Institución SYSTEM PLUS PASTO LTDA, deberá dar cumplimiento a ésta y todas las demás políticas de seguridad de la información establecidas, con el propósito de proteger la seguridad de la red.

CONSIDERACIONES GENERALES

Controles de acceso

El acceso de los usuarios a la red de la Institución SYSTEM PLUS PASTO LTDA, se encuentra establecido por la Política de Control de acceso.

Todo acceso a servicios de la red de la Institución SYSTEM PLUS PASTO LTDA debe ser validado, y todo intento exitoso o incorrecto debe ser registrado para su análisis.

Dominios de seguridad

Se deben establecer niveles de confianza asociados a los dominios de seguridad y las conexiones asociadas a niveles no confiables, deben ser controladas por el firewall.

Se deben determinar mecanismos de protección de la red que permitan realizar conexiones autorizadas entre los funcionarios de la Institución SYSTEM PLUS PASTO LTDA y los dominios definidos como confiables.

No se permitirán establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo a través de la red de la Institución. Las excepciones deben ser autorizadas por el encargado de la Seguridad de la Información, el que debe establecer control, registro y revisión de esta excepción.

Manejo de conexiones externas

Toda solicitud de conexión externa (tales como Web Service, VPNs, FTP, otros) a dominios confiables de la Institución SYSTEM PLUS PASTO LTDA, debe ser formalizada y debidamente autorizada por el responsable de la Seguridad de la Información, especificando motivo, sistemas que accederá, usuarios autorizados, periodo de conexión, e incluir firma de acuerdo de no divulgación. Si la conexión es a sistemas de otras instituciones, se deben establecer convenios de colaboración, aprobados por los encargados de servicios respectivos.

Toda conexión a entidades externas debe ser monitoreada mediante procesos definidos por el responsable de la Seguridad de la Información.

Se deben programar revisiones a todos los dispositivos de conexión con entidades externas. Las conexiones no vigentes deben ser deshabilitadas en forma inmediata por el responsable de la Seguridad de la Información.

Ante cualquier evento sospechoso se debe informar al encargado de la Seguridad de la Información, quien gestionará la evaluación del evento.

Administración de redes inalámbricas

No se debe permitir la configuración de router a través de conexiones inalámbricas.

Se debe mantener un listado de accesos inalámbricos (router) identificados con sus claves, ubicación, alcances, responsables, usuarios con perfiles restringidos, etc.

Cada uno de los dispositivos de red (router, firewall, switch, etc) deben tener una contraseña única. Las contraseñas de los router no deben tener encriptación WEP o WAP, debe utilizarse WPA2 o superior.

Las redes inalámbricas no deben permitir el acceso al equipo servidor ni a los equipos de las áreas administrativa y académica de la Institución SYSTEM PLUS PASTO LTDA.

No se permite incorporar ningún tipo de dispositivo personal tales como Router, Switch o Access Point a la red de la Institución SYSTEM PLUS PASTO LTDA.

Acceso a los puertos de comunicación

Se deben proteger los puertos de diagnóstico de dispositivos de control de red de comunicaciones de la Institución SYSTEM PLUS PASTO LTDA, así como los puertos lógicos asociados, con el objeto de evitar el acceso de personas no autorizadas.

NOTA:

Las personas que no estén dispuestas a acatar la normativa de la Institución SYSTEM PLUS PASTO LTDA no podrán formar parte de la Institución, dado que estos documentos enuncian sus responsabilidades.

9.4.2 Política de seguridad de control de acceso

Código: P02	**POLÍTICA CONTROL DE ACCESO SYSTEM PLUS PASTO LTDA**	
Versión: 01		
Elaborado:	Ing. Carlos Arturo Pulido Rodríguez	
Revisado:	María Eugenia Benavides Cerón	
Fecha:	30 de noviembre de 2015	

NOTA DE CONFIDENCIALIDAD

Este documento es de propiedad exclusiva de la Institución SYSTEM PLUS PASTO LTDA y su uso y distribución sólo está autorizado al interior de la Institución y por parte del personal debidamente habilitado, quedando prohibida la divulgación y/o reproducción total o parcial del contenido de éste sin la debida autorización por parte del responsable de la Seguridad de la Información de la Institución.

Descripción de la política:

La política de seguridad para el control de acceso, tiene por objeto proporcionar seguridad a los accesos de los recursos de la Institución SYSTEM PLUS PASTO LTDA.

Todo el personal es responsable del mecanismo de control de acceso que se le sea proporcionado, por lo cual deberá mantenerlo de forma confidencial.

El control de acceso a la información que se encuentra en la Institución SYSTEM PLUS PASTO LTDA, debe ser proporcionado por el dueño de la información, otorgándole únicamente los permisos mínimos necesarios para el desempeño de sus funciones.

Cualquier intento de violación de seguridad de la información, ejecutada por personal autorizado o no, será considerado como una falta a las políticas de seguridad de la información independiente de la motivación.

Alcance:

Esta política se aplica a todos los usuarios de la Institución SYSTEM PLUS PASTO LTDA, ya sean administrativos, docentes, personal de apoyo, estudiantes, practicantes, proveedores y personal externo.

Aplicable

La Institución SYSTEM PLUS PASTO LTDA en su interés por proteger su información y los recursos de procesamiento de la misma demostrará el compromiso de la Dirección en este esfuerzo, promoviendo que el personal cuente con el nivel deseado de conciencia en seguridad de la información para la correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan las Políticas de seguridad de la información de la Institución.

Todos los funcionarios de la Institución SYSTEM PLUS PASTO LTDA y en específico los de las áreas administrativa y académica, deben tener especial cuidado de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad y el buen nombre de la Institución.

Esta política es aplicable durante el empleo y aún después de terminado el empleo.

Responsabilidades de la Dirección:

Autorizar los mecanismos de control para los dominios de seguridad definidos.

Demostrar su compromiso con la seguridad de la información por medio de su aprobación de las políticas y demás lineamientos que desee establecer la Institución.

Promover la importancia de la seguridad de la información entre los funcionarios de la Institución SYSTEM PLUS PASTO LTDA y el personal provisto por terceras partes, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas establecidas para la seguridad de la información.

Definir y establecer el proceso disciplinario o incluir en el proceso disciplinario existente en la Institución, el tratamiento de las faltas de cumplimiento a las políticas de seguridad o los incidentes de seguridad que lo ameriten.

Responsabilidades del encargado de la Seguridad de la Información:

Generar las condiciones que permitan el intercambio y manejo seguro de la información en la Institución SYSTEM PLUS PASTO LTDA.

Habilitar mecanismos tecnológicos de tal manera que se pueda prevenir el uso de técnicas de ataque a los sistemas informáticos de la Institución SYSTEM PLUS PASTO LTDA.

Velar por la disponibilidad de los servicios de las distintas áreas de la Institución SYSTEM PLUS PASTO LTDA.

Responsabilidades de los empleados, y demás incluidos en el alcance:

El personal de la Institución SYSTEM PLUS PASTO LTDA, deberá permanecer atento y en caso de detectar actividades sospechosas, deberá seguir los procedimientos de seguridad y reportarlas.

Los funcionarios y personal externo que por sus funciones hagan uso de la información de la Institución SYSTEM PLUS PASTO LTDA, deben dar cumplimiento a las políticas de seguridad de la información, así como asistir a las capacitaciones que sean referentes a la seguridad de la información.

Requerimientos de seguridad para las aplicaciones.

El encargado de la Seguridad de la Información debe conocer qué aplicaciones de las instaladas en los equipos de la Institución SYSTEM PLUS PASTO LTDA utilizan internet, para identificar los destinos específicos a los que necesitan acceder.

Divulgación y autorización de la información.

La divulgación de la información se debe realizar con la autorización del propietario de la misma.

Control de acceso

A la información.

El acceso a la información se controla a través de autorizaciones y permisos para su uso, conocimiento y difusión.

A las redes.

El acceso de los usuarios a las redes y a los servicios de red, no debería comprometer la seguridad de los servicios de red ya que se exige control de acceso de los usuarios a los servicios de información.

Al sistema operativo.

Registrar intentos exitosos y fallidos de ingreso al sistema.

Emitir alarma cuando se violan las políticas de seguridad del sistema.

A las aplicaciones.

Las aplicaciones deben suministrar protección contra acceso no autorizado, evitando poner en peligro otros sistemas con los que se comparten los recursos de información.

Requerimientos para la autorización formal de las solicitudes de acceso.

Se debe establecer un procedimiento formal para el registro y eliminación del usuario para otorgar y revocar el acceso a todos los sistemas y servicios de información, el procedimiento debe considerar al menos lo siguiente:

Utilizar Identificadores de usuario únicos que permitan a los usuarios vincularse y ser responsables de sus acciones.

Verificar que el usuario tenga la autorización dada por el propietario del sistema para el uso del sistema o de los servicios de información.

Comprobar que el nivel de acceso otorgado sea apropiado para el propósito de los funcionarios de la Institución SYSTEM PLUS PASTO LTDA.

Proporcionar a los usuarios un enunciado escrito de sus derechos de acceso.

Mantener un registro formal de todas las personas registradas para usar el servicio.

Eliminar y bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de puesto de trabajo o han dejado la Institución.

Chequeo periódico para eliminar o bloquear los Identificadores de usuarios y cuentas redundantes.

Requerimientos para la revisión periódica de los controles de acceso.

Se establece una revisión de los controles en un periodo trimestral (3 meses), con el fin de asegurar que no se hayan obtenido privilegios no autorizados.

Cuando existan cambios de funciones o terminación de empleo, se deben revisar los controles de acceso del usuario afectado.

Revocación de los derechos de acceso

Los derechos de acceso de todos los usuarios a la información y los medios de procesamiento de información son removidos como consecuencia de su desvinculación, o ajustados si sus funciones cambian.

NOTA:

Las personas que no estén dispuestas a acatar la normativa de la Institución SYSTEM PLUS PASTO LTDA no podrán formar parte de la Institución, dado que estos documentos enuncian sus responsabilidades.

9.4.3 Política de seguridad de gestión de los medios removibles

Código: P03	**POLÍTICA GESTIÓN DE LOS MEDIOS REMOVIBLES SYSTEM PLUS PASTO LTDA**	
Versión: 01		
Elaborado:	Ing. Carlos Arturo Pulido Rodríguez	
Revisado:	María Eugenia Benavides Cerón	
Fecha:	30 de noviembre de 2015	

NOTA DE CONFIDENCIALIDAD

Este documento es de propiedad exclusiva de la Institución SYSTEM PLUS PASTO LTDA y su uso y distribución sólo está autorizado al interior de la Institución y por parte del personal debidamente habilitado, quedando prohibida la divulgación y/o reproducción total o parcial del contenido de éste sin la debida autorización por parte del responsable de la Seguridad de la Información de la Institución.

Descripción de la política:

La política de seguridad para la gestión de los medios removibles define las reglas para la protección de datos en diferentes medios de almacenamiento y evita la divulgación no autorizada, modificación, borrado o destrucción de los activos e interrupción de las actividades de la Institución SYSTEM PLUS PASTO LTDA.

Alcance:

Esta política se aplica a todos los usuarios de la Institución SYSTEM PLUS PASTO LTDA, ya sean administrativos, docentes, personal de apoyo, estudiantes, practicantes, proveedores y personal externo.

Aplica para todos los medios de almacenamiento removibles incluyendo memorias, discos externos, pendrive, CD’s y DVD’s e incluso equipos que se conectan a través de Bluetooth u otro medio como los teléfonos celulares y tablets.

Aplicable

La Institución SYSTEM PLUS PASTO LTDA en su interés por proteger su información y los recursos de procesamiento de la misma demostrará el compromiso de la Dirección en este esfuerzo, promoviendo que el personal cuente con el nivel deseado de conciencia en seguridad de la información para la correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan las Políticas de seguridad de la información de la Institución.

Todos los funcionarios de la Institución SYSTEM PLUS PASTO LTDA deben tener especial cuidado de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad y el buen nombre de la Institución.

Esta política es aplicable durante el empleo y aún después de terminado el empleo.

Responsabilidades de la Dirección:

Autorizar los mecanismos de control para los dominios de seguridad definidos.

Demostrar su compromiso con la seguridad de la información por medio de su aprobación de las políticas y demás lineamientos que desee establecer la Institución.

Promover la importancia de la seguridad de la información entre los funcionarios de la Institución SYSTEM PLUS PASTO LTDA y el personal provisto por terceras partes, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas establecidas para la seguridad de la información.

Definir y establecer el proceso disciplinario o incluir en el proceso disciplinario existente en la Institución, el tratamiento de las faltas de cumplimiento a las políticas de seguridad o los incidentes de seguridad que lo ameriten.

Responsabilidades del encargado de la Seguridad de la Información:

Proponer configuraciones de seguridad para los medios removibles.

Aplicar las medidas de protección en la utilización de estos.

Formatear medio externo y pendrive a solicitud del usuario.

Responsabilidades de los empleados, y demás incluidos en el alcance:

El personal de la Institución SYSTEM PLUS PASTO LTDA, deberá mantener protegida la información contenida en el medio removible que le fue asignado. Utilizar los medios removibles asignados, de acuerdo a lo establecido en esta política, informando en forma oportuna de cualquier deterioro. Además de gestionar el medio removible, ocupándose de su uso, utilización, eliminación de los datos, almacenamiento y eliminación del mismo cuando corresponda.

El personal que requiera un medio removible para el ejercicio de sus actividades, deberá solicitarlo al encargado de la Seguridad de la Información quien evaluará y autorizará su uso.

Es de exclusiva responsabilidad de cada funcionario tomar las medidas adecuadas para el almacenamiento y protección de los medios removibles, para evitar accesos no autorizados, daños, pérdida de información o extravío del medio.

En caso de ocurrir alguna situación con el medio removible, se debe inmediatamente informar al encargado de la Seguridad de la Información.

Consideraciones generales

Los medios removibles no son alternativa de respaldo de información de la Institución SYSTEM PLUS PASTO LTDA, siendo responsabilidad de los usuarios mantener la información en el servidor o equipos destinados para ello.

Los medios de almacenamiento removibles (CD, DVD, pendrive, Disco duro externo, etc.) deben ser utilizados únicamente como medio de transporte de información; es responsabilidad de los usuarios mantener la información que manipulan en los equipos asignados.

Todo medio removible debe ser escaneado mediante antivirus cada vez que sea conectado a un equipo de la red de la Institución SYSTEM PLUS PASTO LTDA.

Toda vez que se requiera almacenar información sensible en medios removibles, debe ser mediante herramientas de cifrado. Las claves de cifrado asociadas

deben protegerse de acuerdo a lo descrito en la política de seguridad en el manejo de contraseñas.

Cuando la información almacenada en un medio removible pierda vigencia, se debe formatear.

Todos los medios removibles deben almacenarse en un ambiente seguro, de acuerdo a las especificaciones del fabricante.

La información almacenada en medios removibles que requiera estar disponible después del tiempo de vida del medio, debe ser almacenada en cualquier otro medio de manera de garantizar que no exista pérdida de información.

Asignación y manejo del medio removible

La utilización de un medio removible requiere previamente de una revisión de cumplimiento del estándar asignado para este tipo de medio, revisión que es de responsabilidad del encargado de la Seguridad de la Información.

El uso del medio removible debe ser solicitado formalmente al responsable de la Seguridad de la Información, el que una vez autorizado, entrega el medio removible, registrando la asignación.

Manejo de los medios removibles

Debe formatearse el medio removible cuando la información pierda vigencia; de no ser posible este formateo, el medio debe ser destruido. El desecho, borrado, limpieza o destrucción de los medios removibles debe ser realizado por el Responsable de la Seguridad Informática.

NOTA:

Las personas que no estén dispuestas a acatar la normativa de la Institución SYSTEM PLUS PASTO LTDA no podrán formar parte de la Institución, dado que estos documentos enuncian sus responsabilidades.

9.4.4 Política de seguridad de manejo de contraseñas

Código: P04	**POLÍTICA MANEJO DE CONTRASEÑAS SYSTEM PLUS PASTO LTDA**	
Versión: 01		
Elaborado:	Ing. Carlos Arturo Pulido Rodríguez	
Revisado:	María Eugenia Benavides Cerón	
Fecha:	30 de noviembre de 2015	

NOTA DE CONFIDENCIALIDAD

Este documento es de propiedad exclusiva de la Institución SYSTEM PLUS PASTO LTDA y su uso y distribución sólo está autorizado al interior de la Institución y por parte del personal debidamente habilitado, quedando prohibida la divulgación y/o reproducción total o parcial del contenido de éste sin la debida autorización por parte del responsable de la Seguridad de la Información de la Institución.

Descripción de la política:

La política de seguridad en el manejo de contraseñas define los parámetros para mantener y mejorar la creación, administración y uso de las contraseñas de la Institución SYSTEM PLUS PASTO LTDA, evitando así que personas internas o externas a la Institución tengan acceso a recursos tales como documentos, equipos, aplicaciones, bases de datos que normalmente no deberían tener.

Alcance:

Esta política se aplica a todos los usuarios de la Institución SYSTEM PLUS PASTO LTDA, ya sean administrativos, docentes, personal de apoyo, estudiantes, practicantes, proveedores y personal externo que desee acceder a algún recurso de la Institución.

Aplicable

La Institución SYSTEM PLUS PASTO LTDA en su interés por proteger su información y los recursos de procesamiento de la misma demostrará el compromiso de la Dirección en este esfuerzo, promoviendo que el personal cuente con el nivel deseado de conciencia en seguridad de la información para la correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan las Políticas de seguridad de la información de la Institución.

Todos los funcionarios de la Institución SYSTEM PLUS PASTO LTDA deben tener especial cuidado de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad y el buen nombre de la Institución.

Esta política es aplicable durante el empleo y aún después de terminado el empleo.

Responsabilidades de la Dirección:

Autorizar los estándares para la selección, uso y gestión de contraseñas.

Demostrar su compromiso con la seguridad de la información por medio de su aprobación de las políticas y demás lineamientos que desee establecer la Institución.

Promover la importancia de la seguridad de la información entre los funcionarios de la Institución SYSTEM PLUS PASTO LTDA y el personal provisto por terceras partes, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas establecidas para la seguridad de la información.

Definir y establecer el proceso disciplinario o incluir en el proceso disciplinario existente en la Institución, el tratamiento de las faltas de cumplimiento a las políticas de seguridad o los incidentes de seguridad que lo ameriten.

Actuar de forma coordinada con el encargado de la Seguridad de la Información, para notificar de las altas, bajas y traslados de miembros de la Institución SYSTEM PLUS PASTO LTDA, de modo tal que se puedan mantener actualizadas las correspondientes cuentas de usuarios.

Responsabilidades del encargado de la Seguridad de la Información:

Actuar de forma coordinada con la Dirección y el personal encargado de la Institución SYSTEM PLUS PASTO LTDA, para la oportuna creación, modificación y eliminación de cuentas de usuario, y así mismo velar por el adecuado registro de la información asociada a dichas cuentas.

Responsabilidades de los empleados, y demás incluidos en el alcance:

El personal de la Institución SYSTEM PLUS PASTO LTDA deberá permanecer atento y en caso de detectar actividades sospechosas, deberá seguir los procedimientos de seguridad y reportarlas.

Solicitar formalmente al encargado de la Seguridad de la Información, cada vez que se requiera realizar algún cambio en el perfil de privilegios de acceso para una cuenta de usuario.

Los funcionarios y personal externo que por sus funciones hagan uso de contraseñas, deberán solicitar al encargado de la Seguridad de la Información, autorización para que se les asigne un usuario y una contraseña cuando corresponda.

Cada miembro de la Institución SYSTEM PLUS PASTO LTDA, debe tener asignada una cuenta de usuario con su correspondiente contraseña, para acceder a los recursos y activos de información de la red institucional, y asumirá la responsabilidad de la correcta utilización de esta credencial, teniendo presente que los datos de su cuenta de usuario son personales e individuales.

El personal puede hacer la solicitud de cambio de contraseña al encargado de la seguridad de la información, cuando crea que su contraseña la conocen otras personas o cuando la haya olvidado y requiera una contraseña nueva, o cuando considere que lleva tiempo suficiente y que necesita ser cambiada.

El encargado de cada área de la Institución SYSTEM PLUS PASTO LTDA debe ser la fuente oficial que suministre los datos de identidad, cargo y demás información que se requiera de todo el personal que trabaja en éstas áreas de la Institución.

Los funcionarios de la Institución SYSTEM PLUS PASTO LTDA, deberán informar cualquier evento anómalo o vulnerabilidad que detecten durante la operación de los sistemas al encargado de la Seguridad de la Información.

Identificación y Contraseñas requeridas

Antes de tener acceso a cualquier recurso de la red de la Institución SYSTEM PLUS PASTO LTDA, todos los usuarios deben ser identificados mediante un usuario y su contraseña.

El usuario y la contraseña deben ser individuales.

Está prohibido el uso de un nombre de usuario ajeno o facilitar el usuario y su contraseña personal a un tercero.

Protección de los Equipos de Trabajo

Todos los equipos de trabajo de la Institución SYSTEM PLUS PASTO LTDA, deben tener una contraseña de ingreso y un protector de pantalla con contraseña y activación máxima definida como estándar.

Todas las aplicaciones corporativas deben tener tiempo de expiración de sesión.

Longitud y contenido de la contraseña

La longitud y configuración de la contraseña debe verificarse al momento de crearla o modificarla.

Las contraseñas de acceso a los recursos de la Institución SYSTEM PLUS PASTO LTDA deben cumplir con los siguientes requisitos:

Debe contener mínimo 8 caracteres.

No debe contener el nombre de usuario, el nombre real del usuario, nombre de la Institución o nombre del área al que pertenece el equipo.

No debe contener palabras completas.

No deben ser consecutivas (ej.: Sy5t3mP14s2014, Sy5t3mP14s2015)

Debe incluir una combinación de letras mayúsculas, letras minúsculas, números y caracteres especiales.

Cambio periódico de las Contraseñas

Cualquier archivo de contraseñas históricas debe mantenerse siempre encriptado, en aquellas plataformas donde sea factible.

Se establece un tiempo límite de 3 meses para renovar la contraseña actual, con este cambio periódico se pretende aumentar el nivel de dificultad de las contraseñas, forzando a los usuarios de la Institución SYSTEM PLUS PASTO LTDA a cambiar sus claves, evitando que pueda ser descubierta fácilmente.

Asignación de Contraseñas expiradas y Reasignación de Contraseñas

La contraseña asignada a una nueva cuenta obligará al usuario a cambiarla durante su primera conexión. La solicitud de cambio de contraseña por olvido, debe ser efectuada al encargado de la Seguridad de la Información, previa identificación del usuario que lo solicita.

Toda reasignación de contraseñas será registrada en la bitácora del sistema y deberá notificarse al usuario de la cuenta.

Almacenamiento de contraseñas

No se deben mantener listados de contraseñas en archivos de texto plano. Los archivos con listas de usuarios y contraseñas deben mantenerse encriptados en todo momento.

Las contraseñas de cuentas de administración, deben ser guardadas en sobres cerrados por cada área, en un lugar protegido.

Contraseñas en dispositivos de Red

Cada uno de los dispositivos de red (routers, switches, Access Point, módems) debe tener una contraseña única.

Toda contraseña provista por el fabricante de los dispositivos de red de cualquier sistema, debe ser reemplazada de acuerdo a lo establecido en el apartado “Longitud y contenido de la contraseña” de esta política.

Se debe evitar que los dispositivos de red conserven las claves por defecto.

Si un dispositivo no posee contraseña de acceso, se debe impedir su administración remota, permitiendo la intervención sólo al personal autorizado y en forma directa (conexión local).

Límite de intentos fallidos de ingreso

Para prevenir ingresos mediante la prueba de varias posibles contraseñas, se limita la aceptación de tres intentos consecutivos de ingreso. Después de los intentos fallidos, la cuenta de usuario debe quedar deshabilitada. El usuario debe notificar al encargado de la Seguridad de la Información, quien habilitará la cuenta, previa verificación de la identidad del usuario y generando el informe de atención respectivo.

En caso de usuarios externos sólo podrá ser reactivado el acceso por consentimiento del contacto establecido al momento de crear la cuenta del usuario.

Recordatorios de Contraseñas

Queda absolutamente prohibido escribir las contraseñas de acceso en lugares públicos.

Cualquier contraseña encontrada en estos medios, será informada y podrá ser motivo de sanción.

En el caso de control de acceso a información, se deben emplear contraseñas robustas o seguras, según lo establecido en el apartado “Longitud y contenido de la contraseña” de esta política.

NOTA:

Las personas que no estén dispuestas a acatar la normativa de la Institución SYSTEM PLUS PASTO LTDA no podrán formar parte de la Institución, dado que estos documentos enuncian sus responsabilidades.

9.4.5 Política de seguridad de uso de Internet

Código: P05	**POLÍTICA USO DE INTERNET SYSTEM PLUS PASTO LTDA**	
Versión: 01		
Elaborado:	Ing. Carlos Arturo Pulido Rodríguez	
Revisado:	María Eugenia Benavides Cerón	
Fecha:	30 de noviembre de 2015	

NOTA DE CONFIDENCIALIDAD

Este documento es de propiedad exclusiva de la Institución SYSTEM PLUS PASTO LTDA y su uso y distribución sólo está autorizado al interior de la Institución y por parte del personal debidamente habilitado, quedando prohibida la divulgación y/o reproducción total o parcial del contenido de éste sin la debida autorización por parte del responsable de la Seguridad de la Información de la Institución.

Descripción de la política:

La política de seguridad de uso de Internet establece los criterios para regular el uso y navegación de Internet en la Institución SYSTEM PLUS PASTO LTDA. Dichas políticas pretenden sensibilizar y formar al personal sobre las amenazas que pueden presentarse a través de internet y busca fomentar el uso correcto y eficaz de sus recursos, como también regular la conexión de las aplicaciones y sitios externos.

Se define Internet como un servicio provisto para los usuarios y aplicaciones que lo requieran como apoyo a sus funciones o funcionamiento de sus aplicaciones. Se les permite el uso siempre y cuando cumplan con las directrices sobre el uso adecuado de este recurso de información, indicadas en esta política.

Los usuarios o sistemas que violen las disposiciones establecidas en este documento están sujetos a acciones disciplinarias según lo establezca la Dirección.

Las disposiciones contenidas en esta Política tienen por objeto maximizar el uso de los recursos de la Institución SYSTEM PLUS PASTO LTDA, protegiendo el ancho de banda con que se cuenta y la integridad de la información.

Alcance:

Esta política se aplica a todos los usuarios de la Institución SYSTEM PLUS PASTO LTDA, con acceso a Internet y servicios relacionados, ya sean estos administrativos, docentes, personal de apoyo, estudiantes, practicantes, proveedores y personal externo.

Aplicable

La Institución SYSTEM PLUS PASTO LTDA en su interés por proteger su información y los recursos de procesamiento de la misma demostrará el compromiso de la Dirección en este esfuerzo, promoviendo que el personal cuente con el nivel deseado de conciencia en seguridad de la información para la correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan las Políticas de seguridad de la información de la Institución.

Todos los funcionarios de la Institución SYSTEM PLUS PASTO LTDA, deben tener especial cuidado de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad y el buen nombre de la Institución.

Esta política es aplicable durante el empleo y aún después de terminado el empleo.

Responsabilidades de la Dirección:

Autorizar los mecanismos de control para los dominios de seguridad definidos.

Demostrar su compromiso con la seguridad de la información por medio de su aprobación de las políticas y demás lineamientos que desee establecer la Institución.

Promover la importancia de la seguridad de la información entre los funcionarios de la Institución SYSTEM PLUS PASTO LTDA, así como la del personal externo,

motivando el entendimiento, la toma de conciencia y el cumplimiento de las políticas establecidas para la seguridad de la información.

Incluir en el proceso disciplinario existente en la Institución, el tratamiento de las faltas de cumplimiento a las políticas de seguridad o los incidentes de seguridad que lo ameriten.

Responsabilidades del encargado de Seguridad de la Información:

Revisar las categorías de navegación y las excepciones a las mismas.

Auditar la integridad de las categorías de permiso de navegación.

Controlar la navegación de Internet.

Informar a la Dirección las situaciones anómalas presentadas.

Enviar avisos por violación a las políticas de seguridad establecidas.

Generar reportes mensuales que incluyan el rendimiento de la conexión a Internet, las velocidades de subida y de descarga, tiempos de respuesta, tráfico, situaciones anómalas, y en base a estos datos analizar los indicadores del servicio.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Cada usuario de la Institución SYSTEM PLUS PASTO LTDA debe ser responsable del acceso permitido para el uso de Internet.

El personal de la Institución SYSTEM PLUS PASTO LTDA, deberá permanecer atento y en caso de detectar actividades sospechosas, deberá seguir los procedimientos de seguridad y reportarlas.

Los funcionarios de la Institución SYSTEM PLUS PASTO LTDA y personal externo que por sus funciones hagan uso de Internet, deben dar cumplimiento a las políticas de seguridad de uso de Internet.

Consideraciones generales

El uso correcto de Internet desde el usuario:

Gestión de perfiles

Los permisos para el uso de Internet estarán limitados por la necesidad de acceso que requiera el desarrollo de la función de cada usuario.

El servicio de internet se encuentra disponible para todos los usuarios que prestan servicios a la Institución, su uso es según el perfil asignado.

La asignación de perfiles es realizada por el encargado de la Seguridad de la Información a través de las IPs asignadas a los equipos.

Uso de internet

Los usuarios de la Institución SYSTEM PLUS PASTO LTDA, deben utilizar como primera opción para conectarse a Internet los medios dispuestos por la Institución. De existir problemas con la conexión principal, los usuarios pueden acceder a través de otros canales de proveedores de servicios de Internet externos. Cuando se use la conexión alternativa, esta debe ser resguardada con medidas de seguridad tales como firewall entre la Institución y la salida a Internet, equipos de escritorio y portátiles actualizados con software antivirus, firewall, antimalware y parches de seguridad.

Se permitirá el uso ocasional o eventual de este servicio en tanto no interfiera con las funciones de los usuarios y no cause conflictos con las actividades de la Institución SYSTEM PLUS PASTO LTDA.

Para las personas visitantes que deseen tener acceso a Internet, sólo podrán disponer de una conexión a Internet en un ambiente limitado en cuanto a opciones de navegación y uso de aplicaciones, es decir que su navegación se hará de forma controlada, asegurando que la red de las áreas administrativa y académica de la Institución se mantenga aislada de los mismos.

El uso de las redes sociales, chats, foros, blogs, sitios de entretenimiento y el uso del servicio streaming, utilizado para emisiones de audio/video en directo a través de Internet, sólo serán permitidos con la debida autorización formal del encargado de Seguridad de la Información.

No se deben almacenar contraseñas en los navegadores.

Restricciones al uso de Internet

No está permitido descargar desde Internet, material que infrinja la normativa establecida por la Institución.

El ingreso a páginas web con contenido pornográfico, abuso de alcohol y otras drogas, discriminación, violencia explícita, grupos terroristas, plagio, abuso de menores, matoneo, ocultismo, aborto, nudismo, venta de armas, maltrato, sitios de descarga de programas, sitios de almacenamiento y compartición de archivos, uso de software P2P, radio y televisión por Internet, telefonía por Internet y sitios reconocidos como inseguros tales como hacking, phishing y navegación de forma anónima, entre otros, no están permitidos. Cualquier excepción deberá ser estudiada por el encargado de la Seguridad de la Información.

El usuario no debe infringir la propiedad intelectual, el secreto comercial, las patentes, regulaciones u otra propiedad intelectual, y debe limitarse únicamente a la instalación o distribución de software, que está licenciado para el uso de la Institución SYSTEM PLUS PASTO LTDA.

El usuario no puede interferir o denegar cualquier servicio informático, utilizando programas, scripts, comandos o cualquier otro método, siendo realizados de forma interna o externa a la Institución.

Los usuarios no podrán publicar ningún tipo de información perteneciente a la Institución en sitios personales u otros, sin la autorización correspondiente del propietario de dicha información.

El uso correcto de Internet desde las aplicaciones:

Aplicaciones propias y de terceros

El encargado de la Seguridad de la Información, debe identificar las aplicaciones tanto internas como externas de la Institución SYSTEM PLUS PASTO LTDA, que necesitan ser accedidas, a fin de asegurar su acceso. Para este propósito se debe conocer la Ip interna, puertos a utilizar, Ip pública asignada, Ip pública que accederá (si corresponde), URL, persona que autoriza, email y teléfono.

Todas aquellas aplicaciones, sistemas o equipos que funcionan internamente pero que son soportadas por terceros que necesitan acceso desde internet, se les asignarán acceso vía VPN.

Para el flujo de información generado desde las aplicaciones internas y/o externas, se debe utilizar el protocolo SSL.

NOTA:

Las personas que no estén dispuestas a acatar la normativa de la Institución SYSTEM PLUS PASTO LTDA no podrán formar parte de la Institución, dado que estos documentos enuncian sus responsabilidades.

9.5 PLAN DE CONCIENTIZACIÓN DE POLÍTICAS DE SEGURIDAD

Una vez presentadas las políticas de seguridad de la información resultado de este proyecto para la Institución SYSTEM PLUS PASTO LTDA, y éstas sean aprobadas por la Dirección, es necesario realizar el plan de divulgación y concientización de las mismas, con el fin de que los funcionarios de la Institución las conozcan, sepan utilizarlas y de esta forma se apropien de conceptos de seguridad de la información y buenas prácticas para proteger la información de la Institución.

El propósito general de la concientización del personal de la Institución SYSTEM PLUS PASTO LTDA, es cambiar esa creencia que tienen muchos empleados de que la seguridad de la información es exclusiva de las áreas de Tecnología de Información, buscando el compromiso de todos los miembros de la Institución.

Para el logro de este propósito se pretende dar a conocer a cada empleado de la Institución SYSTEM PLUS PASTO LTDA, que se han establecido una serie de políticas de seguridad de la información, que buscan regular la gestión de la seguridad de la información al interior de la Institución y mantener seguros sus activos, siendo muy importante su participación para el logro de éste propósito, y que es responsabilidad de todos cuidar porque no se realicen actividades que vayan en contra de cada una de estas políticas.

Se debe enfatizar que la mayoría de los usuarios de la Institución SYSTEM PLUS PASTO LTDA, han ido desarrollando conductas que en general contribuyen a la inseguridad de la información. Este plan de concientización busca educar a los funcionarios de la Institución y conseguir un adecuado nivel de protección de la información mediante comportamientos tales como evitar usar el internet para actividades personales tales como escuchar música, ver videos, descargar archivos o programas, abstenerse de abrir archivos adjuntos provenientes de algunos contractos de correo, evitar suministrar datos personales por teléfono o

por sitios web, evitar utilizar la misma contraseña en diferentes páginas, realizar copias de la información con cierta periodicidad, evitar dejar contraseñas escritas en papeles, vacunar cualquier medio removible inmediatamente después de conectarlo al equipo y antes de entrar a ver su contenido, etc.

Con estas y muchas otras conductas se pretende darles a entender al personal de la Institución SYSTEM PLUS PASTO LTDA, que la seguridad de los activos informáticos no sólo depende de los especialistas en el tema, sino que cada persona hace parte de ello y que son piezas fundamentales en la protección de la información de la Institución.

Un punto que se debe dejar muy claro en las capacitaciones que se realicen con el personal de la Institución SYSTEMPLUS PASTO LTDA, son los procesos disciplinarios para los usuarios que no tienen sentido de pertenencia hacia la Institución y no acaten las políticas.

Las sanciones y su cumplimiento serán establecidas por la Dirección.

De igual forma, se recomienda establecer incentivos, ya sean por áreas o de forma personal, premiando de esta forma al personal que se encuentra comprometido con el desarrollo y crecimiento de las políticas de seguridad, ya que así se incentiva y motiva al funcionario, cambiando para bien las costumbres con las que vienen laborando desde hace muchos años.

Al igual que el manual de las políticas de seguridad, la Institución SYSTEM PLUS PASTO LTDA debe aprobar y destinar recursos para el desarrollo del programa de concientización.

Diseño del Plan de Concientización

Para este plan, se propone realizar las siguientes actividades:

- ✓ Definir un diseño para la campaña de concientización

Con este diseño se busca que tanto el personal interno como externo de la Institución SYSTEM PLUS PASTO LTDA, inmediatamente observen el afiche, recuerden que deben hacer uso de las políticas de seguridad definidas y en caso de detectar actividades sospechosas, deberán reportarlas al encargado de la Seguridad de la Información.

- ✓ Definir un lema para la campaña de concientización

Con esta frase breve se busca que todo aquel que la lea o la escuche, recuerde que no puede hacerse el de la vista gorda o en otras palabras que no puede pasar por alto ciertos detalles de seguridad internos de la Institución, y en caso de hallar o realizar alguna actividad que afecte la seguridad de los activos de la Institución, lo piense dos veces antes de hacerlo.

- ✓ Para la definición de medios y estrategias se determina que los soportes de los mensajes a transmitir se harán de forma impresa y audiovisual, y se impartirán charlas y conferencias. Todo esto se sugiere para que la campaña tenga mayor impacto.

En cuanto a la parte impresa se elaborarán unos pendones o afiches que incluyan algunas políticas de seguridad para que permanezcan siempre en la mente de los funcionarios. Dichos afiches serán ubicados en las principales carteleras de la Institución y lugares estratégicamente dispuestos para que todo el personal los observe y los tenga en cuenta.

Por otro lado para la parte audiovisual se publicarán presentaciones y videos que les permitan recordar a los funcionarios algunas políticas de seguridad y qué hacer y a quién dirigirse en caso de presentarse algún incidente de seguridad de la información. Dichos videos estarán publicados en la página web de la Institución www.systempluspasto.edu.co y se proyectarán en las salas dotadas con televisores tres veces a la semana y también cuando se programen reuniones institucionales.

Se dispondrá también de los fondos de pantalla de los equipos de las oficinas, los cuales tendrán el diseño de la campaña con el fin de que sea visible y accesible para todos.

Para ayudar al propósito de esta campaña se podrían elaborar lapiceros, llaveros, vasos u otros objetos que tengan el diseño de la campaña de tal forma que logremos estar en la mente del personal interno como externo de la Institución.

Como medida extrema se intentará que los desprendibles de pago de la Institución lleven impreso en marca de agua el diseño de la campaña, así lograremos ubicarnos en la mente de todos los funcionarios.

Para conocer el impacto de la campaña se realizarán concursos de preguntas respecto a las políticas de seguridad, qué hacer en caso de presentarse un incidente de seguridad y a dónde reportar anomalías.

Puesta en ejecución del plan

- ✓ Definir un diseño para la campaña de concientización

Para cumplir con este propósito se ha elaborado el siguiente diseño:

Figura 3. Diseño de la campaña de concientización Institución System Plus Pasto Ltda

Fuente: Autor del proyecto

Lo que se pretende con este diseño

El diseño incorpora como elemento central el logo de la Institución SYSTEM PLUS PASTO LTDA desintegrándose, y al fondo de la imagen se encuentra un equipo portátil, del cual sale desde la pantalla una persona que está intentando apoderarse de algo que pertenece a la Institución.

Con este diseño se pretende dar a conocer al personal de la Institución que si no se compromete con la seguridad de la información, puede llegar a producir daños importantes y destruir la Institución, y por supuesto esto causaría angustia e intranquilidad en los funcionarios que laboran en la Institución. El significado que se quiere lograr con el logo de la Institución desintegrándose, es precisamente que si cada una de las personas no adquiere compromisos de seguridad en su puesto de trabajo, podría ver que todo lo que existe en la Institución se pierda y dejaría de existir.

Es de vital importancia que todos ayuden a proteger los activos de la Institución con el simple hecho de informar cualquier actividad sospechosa, cualquier incidente de seguridad y sobre todo informando oportunamente al encargado de la seguridad de la información.

✓ Definir un lema para la campaña de concientización

Como lema para el plan de concientización se propone el siguiente:

"¡La seguridad hace parte de ti!"

Lo que se pretende con el lema

El lema es una sentencia que busca explicar de forma sencilla la propuesta de valor de la campaña. Es una frase breve que sirve para reforzar y concretar aún más el mensaje que se quiere transmitir, conjuntamente con el diseño propuesto anteriormente, de modo que la campaña sea percibida de la forma esperada.

Al aportar mayor claridad y contundencia al mensaje, el lema se convierte en una pieza clave dentro de la campaña, ya que se asocia directamente al argumento o atributo que servirá para concientizar a los funcionarios de la Institución SYSTEM PLUS PASTO LTDA.

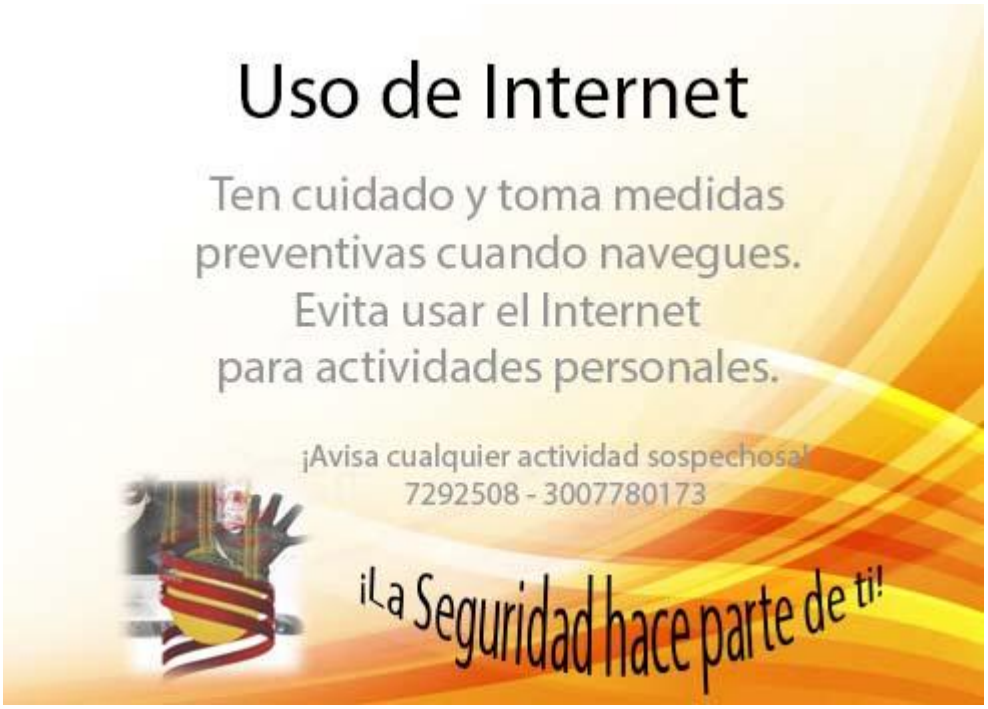
Figura 4. Lema acompañado del diseño de la campaña de concientización Institución System Plus Pasto Ltda

Fuente: Autor del proyecto

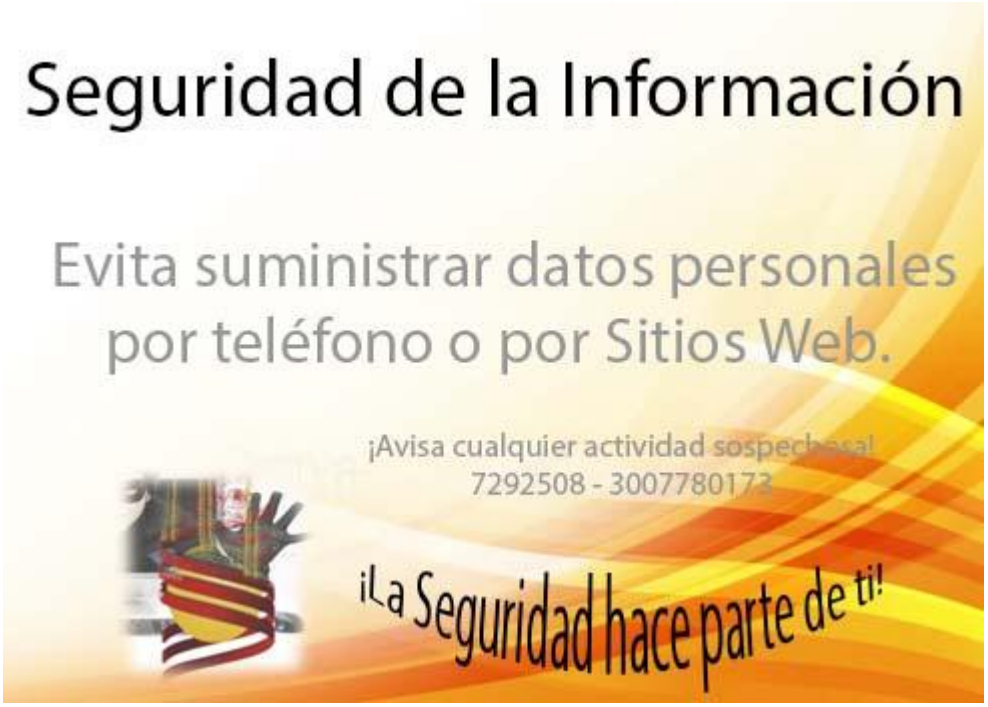
Medios impresos

Los pendones o afiches que se publicarán en las carteleras principales de la Institución y en lugares estratégicos para que puedan ser vistos por el personal de la Institución SYSTEM PLUS PASTO LTDA, son:

Figura 5. Pendones o afiches para la campaña de concientización Institución System Plus Pasto Ltda




Correo electrónico
¡Si no has solicitado nada, no hagas clic!
Hay correos electrónicos que pueden
infectar, secuestrar tu PC, robar información.
Abstenerse de abrir archivos adjuntos.
¡Avisa cualquier actividad sospechosa!
7292508 - 3007780173
¡La Seguridad hace parte de ti!


Seguridad de la Información
Evita suministrar datos personales
por teléfono o por Sitios Web.
¡Avisa cualquier actividad sospechosa!
7292508 - 3007780173
¡La Seguridad hace parte de ti!

Fuente: Autor del proyecto

Estos diseños pueden ser utilizados también como fondos o protectores de pantalla de los equipos de la Institución e incluso para ayudar al propósito de esta campaña se podrían elaborar lapiceros, llaveros, vasos u otros objetos que tengan el diseño de la campaña de tal forma que logremos estar en la mente del personal interno como externo de la Institución.

10. ANÁLISIS DETALLADO DEL ANEXO A ISO 27001:2013

DOMINIO	CUMPLE	NO CUMPLE
POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN	0%	100%
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	14%	86%
SEGURIDAD DE LOS RECURSOS HUMANOS	17%	83%
GESTIÓN DE ACTIVOS	10%	90%
CONTROL DE ACCESO	0%	100%
CRIPTOGRAFÍA	0%	100%
SEGURIDAD FÍSICA Y DEL ENTORNO	13%	87%
SEGURIDAD DE LAS OPERACIONES	14%	86%
SEGURIDAD DE LAS COMUNICACIONES	0%	100%
ADQUISICIÓN, DESARROLLO Y MENTENIMIENTO DE SISTEMAS	0%	100%
RELACIONES CON LOS PROVEEDORES	20%	80%
GESTIÓN DE INCIDENCIAS DE SEGURIDAD DE LA INFORMACIÓN	0%	100%
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	0%	100%
CUMPLIMIENTO	12,5%	87,5%

11. RECOMENDACIONES A IMPLEMENTAR SEGÚN EL ANÁLISIS DE LA ISO 27001:2013

ANEXO A (OBJETIVOS DE CONTROL Y CONTROLES)					
DOMINIO A.5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN**				
A.5.1	Orientación de la dirección para la gestión de la seguridad de la información				
Objetivo	Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.				
Numeral	**Controles**	**Cumple**	**no cumple**	**que se tiene**	**Recomendaciones a implementar**
A.5.1.1	Políticas para la seguridad de la información		X		Tener en cuenta las políticas propuestas para mejorar la seguridad de la información en la Institución SYSTEM PLUS PASTO LTDA.
A.5.1.2	Revisión de las políticas para la seguridad de la información		X		Revisar cada tres meses las políticas para saber cuáles deben ser cambiadas y eliminadas.
DOMINIO A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**				
A.6.1	Organización interna				
Objetivo	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.				

Numeral	Controles	Cumple	no cumple	que se tiene	Recomendaciones a implementar
A.6.1.1	Roles y responsabilidades para la seguridad de la información		X		Se debe trabajar en equipo con los encargados de las áreas y el responsable de la seguridad de la información.
A.6.1.2	Separación de deberes		X		Cada funcionario deberá realizar sólo las funciones que le fueron asignadas.
A.6.1.3	Contacto con las autoridades	X			
A.6.1.4	Contacto con grupos de interés especial		X		Mantener el contacto con grupos o foros de seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos		X		Adquirir buenas prácticas relacionadas con la gestión de proyectos.
A.6.2	Dispositivos móviles y teletrabajo				
Objetivo	Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.				
Numeral	**Controles**				
A.6.2.1	Política para dispositivos móviles		X		Establecer políticas de seguridad en el uso de dispositivos móviles.
A.6.2.2	Teletrabajo		X		Actualmente no aplica en la Institución. En tal caso se deben establecer recomendaciones de la Dirección.
DOMINIO	**SEGURIDAD DE LOS RECURSOS HUMANOS**				

A.7					
A.7.1	Antes de asumir el empleo				
Objetivo	Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.				
Numeral	**Controles**				
A.7.1.1	Selección		X		Un buen proceso de selección de personal contribuye a la elección adecuada y evita costos.
A.7.1.2	Términos y condiciones del empleo		X		Si el nuevo empleado no acepta los términos y condiciones establecidas, no puede ser vinculado.
A.7.2	Durante la ejecución del empleo				
Objetivo	Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.				
Numeral	**Controles**				
A.7.2.1	Responsabilidades de la dirección		X		La Dirección deberá apoyar y desarrollar la implementación del SGSI y su mejora continua.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	X			Tener en cuenta la campaña de concientización.
A.7.2.3	Proceso disciplinario		X		El proceso disciplinario busca garantizar la efectividad de las políticas de seguridad propuestas.
A.7.3	Terminación y cambio de empleo				

Objetivo	Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.				
Numeral	**Controles**				
A.7.3.1	Terminación o cambio de responsabilidades de empleo		X		Las responsabilidades de seguridad de la información que permanecen validas durante y después de la terminación o cambio de empleo se deberían definir, comunicar y hacer cumplir.
DOMINIO A.8	**GESTIÓN DE ACTIVOS**				
A.8.1	Responsabilidad por los activos				
Objetivo	Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas				
Numeral	**Controles**				
A.8.1.1	Inventario de activos		X		Listar todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, etc.), que tengan valor para la Institución y necesiten por tanto ser protegidos.
A.8.1.2	Propiedad de los activos		X		Los activos mantenidos en el inventario deberían tener un propietario.
A.8.1.3	Uso aceptable de los activos		X		Definir reglas claras para el uso de los activos.

A.8.1.4	Devolución de activos		X		Los empleados y usuarios deberían devolver los activos de la Institución que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2	Clasificación de la información				
Objetivo	Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.				
Numeral	**Controles**				
A.8.2.1	Clasificación de la información		X		La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2	Etiquetado de la información	X			Desarrollar e implementar procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la Institución.
A.8.2.3	Manejo de activos		X		Desarrollar e implementar procedimientos para el manejo de activos, asegurando la

					protección de los datos de carácter personal así como confidencial de la Institución.
A.8.3	Manejo de medios				
Objetivo	Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.				
Numeral	**Controles**				
A.8.3.1	Gestión de medios removibles		X		Definir el procedimiento de reutilización y eliminación de medios removibles, con el fin de garantizar que la información se proteja adecuadamente.
A.8.3.2	Disposición de los medios		X		Disponer en forma segura de los medios cuando se requieran y prescindir de ellos cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos		X		Proteger los medios que contienen información de accesos no autorizados o uso indebido durante la trasmisión.
DOMINIO A.9	**CONTROL DE ACCESO**				
A.9.1	Requisitos del negocio para control de acceso				

Objetivo	Limitar el acceso a información y a instalaciones de procesamiento de información.				
Numeral	**Controles**				
A.9.1.1	Política de control de acceso		X		Aplicar las políticas de control de acceso propuestas y establecer normas para garantizar un adecuado control de acceso a los sistemas de información de la Institución.
A.9.1.2	Acceso a redes y a servicios en red		X		Verificar los servicios de acceso a la red así como la identidad del usuario para determinar cuáles son los recursos a los que accede.
A.9.2	Gestión de acceso de usuarios				
Objetivo	Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.				
Numeral	**Controles**				
A.9.2.1	Registro y cancelación del registro de usuarios		X		Implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2	Suministro de acceso de usuarios		X		Realizar un proceso de suministro de acceso formal de usuarios para fijar o suprimir los derechos de

					acceso.
A.9.2.3	Gestión de derechos de acceso privilegiado		X		Restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios		X		Controlar la asignación de la información secreta por medio de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuarios		X		Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.
A.9.2.6	Retiro o ajuste de los derechos de acceso		X		Los derechos de acceso del personal de la Institución se deberían quitar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.
A.9.3	Responsabilidades de los usuarios				
Objetivo	Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.				
Numeral	**Controles**				
A.9.3.1	Uso de información de autenticación secreta		X		Controlar el acceso por medio de restricciones y excepciones con base en la autenticación de

					los usuarios.
A.9.4	Control de acceso a sistemas y aplicaciones				
Objetivo	Evitar el acceso no autorizado a sistemas y aplicaciones				
Numeral	**Controles**				
A.9.4.1	Restricción de acceso a la información		X		Negar o permitir el acceso a la información en relación a la política de control de accesos definida.
A.9.4.2	Procedimiento de ingreso seguro		X		El acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro siempre y cuando la política así lo indique.
A.9.4.3	Sistema de gestión de contraseñas		X		Tener en cuenta la política de seguridad para el manejo de contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados		X		Restringir y/o controlar el uso de programas utilitarios que pudieran tener la capacidad de anular los controles de seguridad establecidos.
A.9.4.5	Control de acceso a códigos fuente de programas		X		Restringir el acceso al código fuente de los programas, con el fin de prevenir la introducción de códigos no

					autorizados y para evitar cambios accidentales.
DOMINIO A.10	**CRIPTOGRAFÍA**				
A.10.1	Controles criptográficos				
Objetivo	Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.				
Numeral	**Controles**				
A.10.1.1	Política sobre el uso de controles criptográficos		X		Desarrollar e implementar una política de uso de las medidas Criptográficas para proteger la información.
A.10.1.2	Gestión de llaves		X		Precisar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
DOMINIO A.11	**SEGURIDAD FÍSICA Y DEL ENTORNO**				
A.11.1	Áreas seguras				
Objetivo	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.				
Numeral	**Controles**				
A.11.1.1	Perímetro de seguridad física		X		Definir y usar perímetros de seguridad para proteger las áreas que contengan información y recursos

					para su procesamiento.
A.11.1.2	Controles de acceso físicos		X		Implementar medidas de seguridad en áreas críticas de la Institución para prevenir el acceso no autorizado a material confidencial.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	X			Desarrollar una política para garantizar la integridad física de los recursos y resguardar los activos de la Institución.
A.11.1.4	Protección contra amenazas externas y ambientales		X		Asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, daños ocasionados por terceros y otras formas de desastres naturales.
A.11.1.5	Trabajo en áreas seguras		X		Establecer procedimientos para el trabajo en áreas seguras, que permitan identificar y controlar los riesgos en el desarrollo de actividades.
A.11.1.6	Áreas de despacho y carga		X		Controlar los puntos de acceso como las

					áreas de despacho y de carga y en lo posible aislarlas de las áreas de procesamiento de información para evitar accesos no autorizados.
A.11.2	Equipos				
Objetivo	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.				
Numeral	**Controles**				
A.11.2.1	Ubicación y protección de los equipos		X		Ubicar y asegurar los equipos de forma tal que no puedan ser manipulados o movidos del área de trabajo.
A.11.2.2	Servicios de suministro		X		Proteger los equipos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.11.2.3	Seguridad de cableado		X		Proteger contra interceptación, interferencia o daño el cableado eléctrico y de datos que soporta servicios de energía e información.
A.11.2.4	Mantenimiento de equipos	X			Mantener en buen estado los equipos para

					asegurar su disponibilidad y funcionamiento continuo.
A.11.2.5	Retiro de activos		X		Retirar los activos de manera formal y previa autorización.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones		X		Aplicar la seguridad a los activos requeridos para actividades fuera de la Institución y teniendo en cuenta los distintos riesgos.
A.11.2.7	Disposición segura o reutilización de equipos		X		Verificar los medios de almacenamiento de los equipos para garantizar que cualquier tipo de dato o software con licencia, se haya extraído o sobrescrito de manera segura antes de su reutilización.
A.11.2.8	Equipos de usuario desatendido		X		Los usuarios se deben asegurar de que los equipos no supervisados cuentan con la protección adecuada.
A.11.2.9	Política de escritorio limpio y pantalla limpia		X		Adoptar una política de puesto de trabajo despejado para documentación en papel y para medios

					de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información.
DOMINIO A.12	**SEGURIDAD DE LAS OPERACIONES**				
A.12.1	Procedimientos operacionales y responsabilidades				
Objetivo	Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.				
Numeral	**Controles**				
A.12.1.1	Procedimientos de operación documentados		X		Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
A.12.1.2	Gestión de cambios		X		Evaluar y planificar el proceso de cambio para asegurar que, si éste se lleva a cabo, se haga de la forma más eficiente, siguiendo los procedimientos establecidos y asegurando la continuidad del servicio.
A.12.1.3	Gestión de capacidad		X		Ajustar el uso de los recursos y garantizar que se cubren las necesidades tanto presentes como

					futuras que certifiquen el servicio.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación		X		Los entornos de desarrollo, pruebas y operación deberían permanecer separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional.
A.12.2	Protección contra códigos maliciosos				
Objetivo	Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.				
Numeral	**Controles**				
A.12.2.1	Controles contra códigos maliciosos		X		Implementar aplicaciones para el análisis de archivos, en busca de amenazas tales como malware, virus y demás código malicioso, seguido de un manejo responsable de los usuarios en cuanto al tratamiento de la información y los medios.
A.12.3	Copias de respaldo				
Objetivo	Proteger contra la pérdida de datos.				
Numeral	**Controles**				
A.12.3.1	Respaldo de la información		X		Programar copias de respaldo de la información, de las aplicaciones y del

					sistema, tratando de ponerlas a prueba regularmente de acuerdo con las políticas de seguridad de respaldo.
A.12.4	Registro y seguimiento				
Objetivo	Registrar eventos y generar evidencia.				
Numeral	**Controles**				
A.12.4.1	Registro de eventos		X		Elaborar, analizar y recopilar los registros acerca de actividades de los usuarios, que incluyan las excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de la información de registro		X		Proteger contra, pérdida, modificación y acceso no autorizado la información de registro al igual que las instalaciones donde reposa.
A.12.4.3	Registro del administrador y del operador		X		Registrar las actividades del administrador y del operador del sistema al igual que proteger sus registros y revisarlos con periodicidad.
A.12.4.4	Sincronización de relojes		X		Sincronizar los relojes

					de todos los sistemas de procesamiento de información pertinentes dentro de la Institución y en relación a una fuente de sincronización única de referencia.
A.12.5	Control de software operacional				
Objetivo	Asegurarse de la integridad de los sistemas operacionales.				
Numeral	**Controles**				
A.12.5.1	Instalación de software en sistemas operativos	X			Implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.12.6	Gestión de la vulnerabilidad técnica				
Objetivo	Prevenir el aprovechamiento de las vulnerabilidades técnicas.				
Numeral	**Controles**				
A.12.6.1	Gestión de las vulnerabilidades técnicas		X		Evaluar el grado de exposición de la Institución en base a la información registrada sobre las vulnerabilidades técnicas de los sistemas de información, y tomar las medidas necesarias para tratar los riesgos asociados.
A.12.6.2	Restricciones sobre la instalación de software	X			Establecer e implementar reglas que controlan la instalación de

					software por parte de los usuarios.
A.12.7	Consideraciones sobre auditorías de sistemas de información				
Objetivo	Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.				
Numeral	**Controles**				
A.12.7.1	Controles de auditorías de sistemas de información		X		Planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas de información para minimizar las interrupciones en los procesos relacionados con el servicio.
DOMINIO A.13	**SEGURIDAD DE LAS COMUNICACIONES**				
A.13.1	Gestión de la seguridad de las redes				
Objetivo	Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.				
Numeral	**Controles**				
A.13.1.1	Controles de redes		X		Administrar y controlar las redes para proteger la información en sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red		X		Identificar e incluir en un acuerdo de servicio de red, los mecanismos de seguridad, los niveles de servicio y los

					requisitos de administración, sin importar si son internos o externos.
A.13.1.3	Separación en las redes		X		Separar las redes en función de los grupos de servicios, usuarios y sistemas de información.
A.13.2	Transferencia de información				
Objetivo	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.				
Numeral	**Controles**				
A.13.2.1	Políticas y procedimientos de transferencia de información		X		Deberían existir políticas y procedimientos formales de transferencia para proteger la información que viaja a través de la red de la institución y fuera de ella.
A.13.2.2	Acuerdos sobre transferencia de información		X		Los acuerdos deberían abordar la transferencia segura de información entre la Institución y las instituciones externas con las que tiene comunicación.
A.13.2.3	Mensajería electrónica		X		Proteger adecuadamente la información publicada en la mensajería

					electrónica.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación		X		Identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la Institución para la protección de la información.
DOMINIO A.14	**Adquisición, desarrollo y mantenimiento de sistemas**				
A.14.1	Requisitos de seguridad de los sistemas de información				
Objetivo	Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.				
Numeral	**Controles**				
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información		X		Los requisitos relacionados con la seguridad de la información se deberían incluir en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas		X		La información de los servicios de aplicación que pasan a través de redes públicas se

					debería proteger contra modificación o acceso no autorizado.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones		X		La información en transacciones de servicios de aplicación se debería proteger para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o reproducción no autorizada.
A.14.2	Seguridad en los procesos de desarrollo y de soporte				
Objetivo	Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.				
Numeral	**Controles**				
A.14.2.1	Política de desarrollo seguro		X		Establecer y aplicar reglas para el desarrollo de software y sistemas dentro de la Institución.
A.14.2.2	Procedimientos de control de cambios en sistemas		X		Hacer uso de procedimientos formales de control de cambios en el ciclo de vida de desarrollo.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación		X		Las aplicaciones críticas para el negocio se deberían revisar y probar para garantizar que no se han generado impactos opuestos en

					las operaciones o en la seguridad de la Institución.
A.14.2.4	Restricciones en los cambios a los paquetes de software		X		Evitar modificaciones en los paquetes de software suministrados por terceros, limitándose a cambios realmente necesarios. Todos los cambios se deberían controlar formalmente.
A.14.2.5	Principios de construcción de los sistemas seguros		X		Establecer, documentar, mantener y aplicar los principios de seguridad en los sistemas para cualquier labor de implementación en el sistema de información.
A.14.2.6	Ambiente de desarrollo seguro		X		Establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.
A.14.2.7	Desarrollo contratado externamente		X		Supervisar y monitorear las actividades de

					desarrollo del sistema que se hayan contratado externamente.
A.14.2.8	Pruebas de seguridad de sistemas		X		Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2.9	Prueba de aceptación de sistemas		X		Establecer programas de prueba y criterios de aceptación para los sistemas de información nuevos, actualizaciones y nuevas versiones.
A.14.3	Datos de prueba				
Objetivo	Asegurar la protección de los datos usados para pruebas.				
Numeral	**Controles**				
A.14.3.1	Protección de datos de prueba		X		Los datos de pruebas se deberían seleccionar, proteger y controlar cuidadosamente.
DOMINIO A.15	**RELACIONES CON LOS PROVEEDORES**				
A.15.1	Seguridad de la información en las relaciones con los proveedores				
Objetivo	Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.				
Numeral	**Controles**				
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores		X		Los requisitos de seguridad de la información para mitigar los riesgos asociados con

					el acceso de proveedores a los activos de la Institución se deberían acordar con éstos y se deberían documentar.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores		X		Establecer y acordar los requisitos de seguridad de la información adecuados a cada proveedor para acceder, procesar, almacenar, comunicar o proporcionar soporte a la información de la Institución.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación		X		Los acuerdos con los proveedores deberían incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicación.
A.15.2	Gestión de la prestación de servicios de proveedores				
Objetivo	Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.				

Numeral	Controles				
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	X			Monitorear, revisar y auditar la presentación de servicios del proveedor regularmente.
A.15.2.2	Gestión de cambios en los servicios de los proveedores		X		Administrar los cambios en el suministro de servicios que realizan los proveedores teniendo en cuenta las políticas de seguridad de la información y los procedimientos.
DOMINIO A.16	**Gestión de incidencias de seguridad de la información**				
A.16.1	Gestión de incidencias y mejoras en la seguridad de la información				
Objetivo	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.				
Numeral	**Controles**				
A.16.1.1	Responsabilidades y procedimientos		X		Establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información		X		Los eventos de seguridad de la información se

					deberían informar lo antes posible utilizando los canales de comunicación disponibles.
A.16.1.3	Reporte de debilidades de seguridad de la información		X		Exigir a los empleados y contratistas que usan los servicios y sistemas de información de la Institución, que informen sobre cualquier debilidad de seguridad vista en los sistemas o servicios.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.		X		Evaluar los eventos de seguridad de la información y decidir si serán tratados como incidentes.
A.16.1.5	Respuesta a incidentes de seguridad de la información		X		Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo a los procedimientos documentados.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información		X		El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad

					o el impacto de incidentes futuros.
A.16.1.7	Recolección de evidencia		X		Definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir como evidencia.
DOMINIO A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO**				
A.17.1	Continuidad de seguridad de la información				
Objetivo	La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.				
Numeral	**Controles**				
A.17.1.1	Planificación de la continuidad de la seguridad de la información		X		La Institución debería determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información		X		La Institución debería establecer, documentar, implementar y mantener los procesos y procedimientos para garantizar el nivel de seguridad de la

					información durante situaciones adversas.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información		X		La Institución debería verificar con regularidad los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2	Redundancias				
Objetivo	Asegurar la disponibilidad de instalaciones de procesamiento de información.				
Numeral	**Controles**				
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.		X		Las instalaciones de procesamiento de información se deberían implementar lo suficiente para cumplir los requisitos de disponibilidad.
DOMINIO A.18	**CUMPLIMIENTO**				
A.18.1	Cumplimiento de requisitos legales y contractuales				
Objetivo	Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.				
Numeral	**Controles**				
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales		X		Todos los requisitos estatutarios,

					reglamentarios y contractuales pertinentes, y el enfoque de la Institución para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información.
A.18.1.2	Derechos de propiedad intelectual	X			Implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados.
A.18.1.3	Protección de registros		X		Los registros se deberían proteger contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada, de

					acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.4	Privacidad y protección de información de datos personales		X		Garantizar la privacidad y la protección de la información personal según lo establece la legislación y las normativas pertinentes.
A.18.1.5	Reglamentación de controles criptográficos		X		Usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A.18.2	Revisiones de seguridad de la información				
Objetivo	Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.				
Numeral	**Controles**				
A.18.2.1	Revisión independiente de la seguridad de la información		X		El enfoque de la Institución para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos

					para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad		X		El encargado de la seguridad de la información junto con la Dirección, deberán revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de las áreas de la Institución, con las políticas y normas de seguridad correspondiente.
A.18.2.3	Revisión del cumplimiento técnico		X		Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

12. CONCLUSIONES

Tal como lo expresa la norma ISO 27001, garantizar un nivel de protección total es casi que imposible, pero se pueden asumir compromisos y comportamientos frente a los riesgos de seguridad, que permiten reducir las amenazas y vulnerabilidades. Con el desarrollo del presente trabajo de grado se logró identificar los activos más críticos de las áreas administrativa y académica de la Institución SYSTEM PLUS PASTO LTDA, utilizando para ello la metodología MAGERIT v 3.0, la cual permitió clasificar los activos y obtener un total de 45 activos que se someterán al SGSI.

La valoración de los activos se realizó teniendo en cuenta las dimensiones propuestas por la metodología MAGERIT v 3.0, logrando obtener valores comprendidos entre 0 y 10 lo que permitió establecer que hay un promedio de impacto alto en los activos esenciales, activos de información, servicios, software y hardware, redes de comunicación soportes de información y una tendencia un poco más baja pero no menos importante en equipamiento auxiliar, instalaciones y personal.

Para la identificación de amenazas, vulnerabilidades y riesgos, y basados en el modelo propuesto por la metodología MAGERIT v 3.0, se logró determinar que la lista de amenazas que pueden materializarse y que afectan a los activos específicos de las áreas administrativa y académica de la Institución SYSTEM PLUS PASTO LTDA es bastante grande. El análisis de estos resultados indica que los activos se encuentran en un porcentaje de probabilidad de ocurrencia muy alto, siendo urgente la implementación de controles que disminuyan el impacto que causaría si se llegara a materializar alguna de esas amenazas.

La campaña de concientización es muy importante ya que no sólo busca concientizar sino también educar y capacitar en prevención a los miembros de la Institución SYSTEM PLUS PASTO LTDA y principalmente a los de las áreas administrativa y académica, para que puedan implementar estrategias de seguridad y buenas prácticas, frente a los riesgos a los que se encuentran expuestos en Internet, accesos no autorizados, errores de los usuarios, alteración accidental o intencional de la información, fugas de información, suplantación, abuso de privilegios de acceso, denegación de servicio, vulnerabilidades de los programas, entre otros.

BIBLIOGRAFÍA

MINTIC. Ley 1273 de 2009. {En línea}. {07 marzo de 2015}. Disponible en: (http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf)

27001ACADEMY. ¿Qué es norma ISO 27001?. {En línea}. {23 agosto de 2014}. Disponible en: (http://www.iso27001standard.com/es/que-es-iso-27001/)

ALMANZA, Andrés. Encuesta. Seguridad Informática en Colombia Tendencias 2012-2013. {En línea}. {20 junio de 2013}. Disponible en: (http://52.0.140.184/revsistemas1/index.php/ediciones-revista-sistemas/edicion-no127/item/132-seguridad-inform%C3%A1tica-en-colombia-tendencias-2012-2013)

CISCO. Seguridad de datos. {En línea}. {07 marzo de 2015}. Disponible en: (http://www.cisco.com/web/ES/solutions/es/information_security/index.html)

SUCAPUCA, Ckarens. El valor de la información. {En línea}. {07 marzo de 2015}. Disponible en: (http://www.academia.edu/5624135/EL_VALOR_DE_LA_INFORMACION)

DUSSAN CLAVIJO, Ciro. Políticas de seguridad informática. {En línea}. {03 mayo de 2014}. Disponible en: (http://www.unilibrecali.edu.co/entramado/images/stories/pdf_articulos/volumen2/Politicas_de_seguridad_informtica.pdf)

ISO 27000.ES. El portal de ISO 27001 en español. {En línea}. {07 marzo de 2015}. Disponible en: (http://www.iso27000.es/sgsi.html)

MIFSUD, Elvira. Introducción a la seguridad informática - Políticas de seguridad. {En línea}. {07 marzo de 2015}. Disponible en: (http://recursostic.educacion.es/observatorio/web/en/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=4)

INTECO. Sistema de Gestión de Seguridad de la Información. {En línea}. {25 agosto de 2014}. Disponible en: (http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/index.html)

MIFSUD, Elvira. Introducción a la seguridad informática – Vulnerabilidades de un sistema informático. {En línea}. {06 septiembre de 2014}. Disponible en: (http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=3)

CANO, Jeimy. La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes. {En línea}. {07 marzo de 2015}. Disponible en: (http://www.isaca.org/Journal/archives/2011/Volume-5/Documents/jolv5-11-LaGerencia.pdf)

PEÑA IBARRA, José. Metodología de Análisis y Gestión de Riesgos de TI. {En línea}. {30 agosto de 2014}. Disponible en: (http://www.isaca.org/chapters7/Monterrey/Events/Documents/20100302%20Metodolog%C3%ADas%20de%20Riesgos%20TI.pdf)

SEMANA. Los tres peores ataques informáticos del 2014. {En línea}. {27 septiembre de 2014}. Disponible en: (http://www.semana.com/tecnologia/novedades/articulo/los-peores-ataques-informaticos-de-2014/391376-3)

VILLALÓN HUERTA, Antonio. Seguridad en Unix y redes. {En línea}. {27 septiembre de 2014}. Disponible en: (https://www.rediris.es/cert/doc/unixsec/unixsec.pdf)

PAE. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. {En línea}. {10 noviembre de 2015}. Disponible en: (http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VkuLCnYrLIW)

GLOSARIO

ACTIVOS**:** en contabilidad, un activo es un bien tangible o intangible que posee una empresa o persona natural. Actualmente se considera “activo” a aquellos bienes o derechos que tienen un beneficio económico a futuro. Los activos son un recurso o bien económico con el cual se obtienen beneficios. Los activos de las empresas varían de acuerdo con la naturaleza de la actividad desarrollada.

Desde hace unos años, la información ha llegado a ser considerada como el activo más valioso dentro de las empresas ya que juega un papel muy importante a la hora de la toma de decisiones y definición de nuevas estrategias de negocios, pues la información como fuente del conocimiento otorga un bien a quien la posee, incluso en la actualidad es común escuchar acerca del espionaje, tráfico y/o robo de información como delito grave, puesto que la información se ha convertido punto clave para el crecimiento, desarrollo o éxito personal, profesional y empresarial, ya que, entre mayor sea el conocimiento adquirido a través de la información mayor será el beneficio obtenido.

AMENAZA**:** es la probabilidad de ocurrencia de un suceso potencialmente desastroso durante cierto periodo de tiempo, en un sitio dado.

En general el concepto de amenaza se refiere a un peligro latente o factor de riesgo externo, de un sistema o de un sujeto expuesto, expresada matemáticamente como la probabilidad de exceder un nivel de ocurrencia de un suceso con una cierta intensidad, en un sitio específico y durante un tiempo de exposición determinado.

Una amenaza informática es un posible peligro del sistema. Puede ser una persona (cracker), un programa (virus, caballo de Troya, etc.), o un suceso natural o de otra índole (fuego, inundación, etc.). Representan los posibles atacantes o factores que aprovechan las debilidades del sistema.

CONFIDENCIALIDAD**:** es la propiedad que impide la divulgación de información a personas o sistemas no autorizados, asegurando el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla, cuando se publica información privada, cuando un equipo con información sensible sobre una empresa es robado, cuando se divulga

información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad.

DISPONIBILIDAD**:** es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran. La información se debe encontrar a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente, además debe estar disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

ESTÁNDAR**:** es la definición clara de un modelo, criterio, regla de medida o de los requisitos mínimos aceptables para la operación de procesos específicos, con el fin asegurar la calidad en la prestación de los servicios.

Los estándares señalan claramente el comportamiento esperado y deseado en las personas o procesos y son utilizados como guías para evaluar su funcionamiento y lograr el mejoramiento continuo de los servicios.

Requieren ser establecidos con el fin de contar con una referencia que permita identificar oportunamente las variaciones presentadas en el desarrollo de los procesos y aplicar las medidas correctivas necesarias.

Es necesario considerar que las fallas de los procesos pueden ser imputables por un lado a problemas propios del sistema que condiciona la necesidad de revisar su estructura y funcionamiento y por otro lado a errores cometidos por las personas.

INTEGRIDAD**:** es la propiedad que busca mantener los datos libres de modificaciones no autorizadas, logrando que la información este exacta y completa. En otras palabras la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

La violación de integridad se presenta cuando una persona, programa o proceso de forma accidental o intencional, modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado

a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad.

RIESGO**:** es el grado de pérdidas esperadas, debido a la ocurrencia de un suceso particular y como una función de la amenaza y la vulnerabilidad.

El riesgo corresponde al potencial de pérdidas que pueden ocurrirle al sujeto o sistema expuesto, resultado de la relación de la amenaza y la vulnerabilidad, este concepto puede expresarse como la probabilidad de exceder un nivel de consecuencias económicas, sociales o ambientales en un cierto sitio y durante un cierto periodo de tiempo.

SGSI**:** es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita sea de forma escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.

El propósito de un sistema de gestión de la seguridad de la información es, por tanto, 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.

TIC**:** las tecnologías de la información y la comunicación (TIC) son todas aquellas herramientas y programas que tratan, administran, transmiten y comparten la información mediante soportes tecnológicos. La informática, Internet y las telecomunicaciones son las TIC más extendidas, aunque su crecimiento y evolución están haciendo que cada vez surjan más modelos.

En La actualidad las TIC han tomado un papel importantísimo en nuestra sociedad y se utilizan en multitud de actividades. Las TIC forman ya parte de la mayoría de sectores: educación, robótica, Administración pública, empleo, empresas, salud, etc.

VULNERABILIDAD**:** es el grado de pérdida de un elemento o grupo de elementos bajo riesgo, resultado de la probable ocurrencia de un suceso desastroso expresada en una escala.

La vulnerabilidad se entiende como un factor de riesgo interno, expresado como la factibilidad de que el sujeto o sistema expuesto sea afectado por el fenómeno que caracteriza la amenaza.

En el campo de la informática, la vulnerabilidad es el punto o aspecto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo.

Representan las debilidades o aspectos falibles o atacables en el sistema informático.

ANEXO

Tabla 13. Lista de chequeo anteproyecto de grado

DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LAS ÁREAS ADMINISTRATIVA Y ACADÉMICA DE LA INSTITUCIÓN SYSTEM PLUS PASTO LTDA, BASADO EN EL ESTÁNDAR INTERNACIONAL ISO/IEC 27001

Elemento	Criterio / elementos	cumple SI/NO	Argumento
Título	Abarca el qué, el cómo y el dónde del tema de investigación de forma clara y concisa	SI	Se busca implementar un SGSI en áreas específicas de la Institución basado en el estándar ISO/IEC 27001.
	Mayúscula sostenida, en negrilla, sin punto al final	SI	Se hace uso del conjunto de normas y reglas de la gramática y la ortografía.
Listas e índices	Índice o Contenido	SI	Incorpora la estructura con el contenido de los títulos de los temas y subtemas que forman el documento y ayudan al lector a encontrar lo que está buscando
	Lista de Tablas	SI	Lista de tablas ordenadas utilizadas secuencialmente en las páginas.
	Lista de Figuras	SI	Lista de figuras ordenadas utilizadas secuencialmente en las páginas.
Introducción	El texto introduce al lector del proyecto en su finalidad	SI	Introducción general al anteproyecto.
Resumen	Resumen documental en español	SI	Se redacta en tercera persona, responde a las preguntas ¿para qué? ¿Qué se busca con este estudio? Se usan abreviaturas

			necesarias y comprensibles, escribe 250 palabras o menos.
	Resumen documental en inglés (Abstract)	SI	Resumen claro, conciso y breve en el idioma Inglés, además de las palabras claves (keywords). (No se usa un software o herramienta de traducción automática).
Forma del documento	Espaciado, numeración y sangría.	SI	El anteproyecto presenta un espaciado apropiado (Interlineado 1,5).
	Tipo y tamaño de fuente	SI	El anteproyecto presenta el tipo, fuente y tamaño apropiado para su presentación (Arial, 12pt).
	Tamaño de la hoja y Márgenes	SI	El anteproyecto presenta el tamaño de hoja y márgenes apropiados para su presentación (Tamaño Carta).
	Alineación del Texto	SI	El texto está justificado.
Delimitación del tema de estudio	Pertinencia y relevancia del tema de estudio en el área en el que se desarrolla	SI	En lo que respecta a la seguridad de la información, uno de los aspectos más importantes es comprender que la información debe ser gestionada.
	La realización de la investigación no implica riesgos para la seguridad del investigador, o el investigador es plenamente consciente de ellos y decide asumirlos	SI	La realización de la investigación no implica riesgos para la seguridad del investigador, ya que el ambiente donde se desarrolla es conocido y apropiado para lo que se desea investigar.
Disponibilidad de la información	Es posible encontrar la suficiente información y asesoría respecto al tema en cuestión	SI	La cantidad de información digital que podemos encontrar del tema supera a la física, pero a pesar de ello existe suficiente material basado en otras

			investigaciones, artículos, tesis, libros y revistas electrónicas que garantizan un éxito en la investigación.
Redacción	Adecuación textual	SI	Se utilizan términos técnicos pero empleando un lenguaje sencillo que se ajusta al tema que se desea investigar y se considera adecuado para aquellos que ya poseen un nivel de conocimientos en el tema.
	Coherencia textual	SI	De principio a fin se expresa de manera clara y precisa lo que se desea investigar, dando a conocer claramente los objetivos que se pretenden alcanzar con la investigación.
	Cohesión textual	SI	Cada párrafo utilizada frases que siguen una secuencia lógica y se usan sinónimos de palabras para evitar repeticiones de términos que de una forma ordenada, facilitan la interpretación de lo que se desea investigar.
	Corrección gramatical	SI	Se realizó una corrección íntegra, que demandó un alto grado de concentración, además de un consistente conocimiento de las normas que rigen la lengua española.
Ortografía	No se presentan errores ortográficos	SI	No se presentan errores según las normas de ortografía.
Formulación del problema	Se hace una formulación clara y sin ambigüedades	SI	El problema está formulado de manera clara y no se incluyen términos que puedan tener doble significado.
	Evidencia la relación entre variables en un contexto temporal	SI	El problema pretende dar una solución a los problemas presentados hoy en la Institución e indica el espacio

	y espacial		donde se va a desarrollar.
	Se hace formalmente la pregunta de investigación	SI	Se formula la pregunta de investigación expresando con claridad qué se pretende resolver.
	La pregunta de investigación responde al objetivo general	SI	La pregunta formulada responde claramente al objetivo general del anteproyecto eliminando cualquier ambigüedad.
Justificación	Argumenta las razones por las cuales se escogió el tema de estudio y evidencia su importancia	SI	Se establecen argumentos basados en las situaciones reales observadas en las áreas administrativas y académica de la Institución y se demuestra la importancia de implementar un SGSI.
	Describe y argumenta claramente los beneficios al realizar el proyecto	SI	Se describen no sólo una sino varios beneficios que se alcanzarán al realizar este proyecto de investigación basado en la implementación de un SGSI.
	Grado de innovación del proyecto, su valor científico, académico o técnico.	SI	Para la región de Colombia y más exactamente la región Sur del país, el desarrollo de este tipo de proyectos es algo innovador ya que las empresas aún no han comenzado a ver la necesidad de certificarse para ofrecer mayor confianza y un mejor servicio a sus usuarios.
Objetivo general	El objetivo general es coherente con la pregunta de investigación	SI	Considero pertinente el objetivo general ya que da respuesta a la formulación del problema e indica además la manera como llevarla a cabo.
Objetivos específicos	Representan metas parciales que llevan al cumplimiento del objetivo general	SI	En cierta forma todos los objetivos específicos planteados son metas que llevan al cumplimiento del objetivo general ya que todos ellos buscan hacer una buena

			gestión de la información basado en estándares establecidos.
	Son realistas, no deben ser muy difíciles de cumplir.	SI	Desde el punto de vista de lo aprendido en la especialización, considero que todos los objetivos específicos son realistas y factibles de cumplir.
	Redactados en orden cronológico (orden de cumplimiento)	SI	Estoy convencido que los objetivos específicos siguen un orden para alcanzar el SGSI, ya que inicio por delimitar los activos, continuo con la identificación de las amenazas, diseño y definición de políticas de seguridad, elección de controles y metodología de análisis y culmino con la concientización del personal.
	Ayudan a cumplir el objetivo general	SI	Los objetivos específicos se desarrollan en forma sucesiva y ayudan a cumplir el objetivo general.
Marco referencial	Estado actual	SI	Se buscó profundizar en la situación actual de las empresas que han sido víctimas de ataques, conocer nuevos incidentes y fallos presentados en el tratamiento de la información, errores en los programas y vulnerabilidades en los sistemas y redes. También se buscó información respecto a empresas que alcanzaron certificaciones en los últimos años.
	Marco teórico	SI	Se realizó una revisión de la literatura sobre el tema. Esto permitió conocer algunos comportamientos éticos de personas que tienen acceso a

			información. Además permitió estar al tanto de las últimas revisiones de las normas internacionales que describen cómo gestionar la seguridad de la información en una empresa.
	Marco conceptual	SI	A través de la revisión de opiniones de varios expertos y publicaciones de organizaciones internacionales se intentó definir todos aquellos términos que intervienen en el proceso de la investigación.
Diseño metodológico preliminar	Tipo de investigación	SI	El presente anteproyecto se inscribe dentro del área de formación de sistemas, específicamente en la línea gestión de sistemas.
	Universo investigativo: Población, muestra, variables	SI	Se establecen dos áreas de la Institución con las cuales se piensa desarrollar el proceso de investigación.
	Técnicas de recolección de información e instrumentos	SI	Aunque no se detallan de manera específica cada técnica, si se hace mención de la manera como se desarrollará la recolección de información. Esto se hará mediante entrevistas, encuestas y observación directa.
Recursos	Talento Humano	SI	El anteproyecto relaciona los nombres de los profesionales del área específica de la Institución que apoyarán el proceso investigativo. Se espera contar además con la asesoría permanente del director del proyecto quién aún no ha sido asignado y estamos a la espera de la

			respuesta por parte del comité.
	Materiales y equipos	SI	Los equipos con que cuenta la Institución son suficientes para desarrollar la actividad investigativa. Además la Universidad y algunos sitios especializados en internet brindan un excelente apoyo con material bibliográfico tales como revistas y artículos científicos que apoyan los procesos de investigación.
Cronograma	Establece los plazos de ejecución de las fases y actividades más relevantes del proyecto.	SI	Las actividades están acordes con los objetivos específicos que pretenden alcanzar el cumplimiento del objetivo general.
Bibliografía	Cantidad, calidad y relevancia de las fuentes	SI	Se procuró ir directamente a las fuentes primarias y secundarias con contenido de alta confiabilidad disponible en la red, basados en Tesis, revistas especializadas, investigaciones, artículos científicos, etc.
	Normatividad APA o ICONTEC	SI	El documento presenta una estructura basada en el uso de las normas APA, esto incluye los márgenes, el tamaño y tipo de fuente y las referencias a citas en todo el documento y la bibliografía.
	Organizada en orden alfabético	SI	La lista de páginas, libros, tesis y demás fuentes consultadas y que permiten servir de guía en el proceso de investigación, fueron listadas en orden alfabético según las normas APA.
	Funcionalidad de los enlaces, si los	NO	No se presentan enlaces en este documento.

	hay.		
	Fuentes, Referencias, notas textuales y notal al pie.	SI	Se referencia las fuentes, referencias y notas al pie de forma clara ayudando a la comprensión del texto.
Glosario	Se incluye un glosario con mínimo 10 términos relacionados con el tema de estudio	SI	Se muestra un glosario de términos ordenado alfabéticamente que ayuda a la comprensión del texto.