REALIZAR UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA PARA CENTRO EDUCATIVO DE SISTEMAS UPARSISTEM DE ACUERDO A LA NORMATIVA ISO/IEC 27001.

RUBÉN DARÍO ACUÑA MONTES, Código 77090411

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
VALLEDUPAR
2017

REALIZAR UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA PARA EL CENTRO EDUCATIVO DE SISTEMAS UPARSISTEM DE ACUERDO A LA NORMATIVA ISO/IEC 27001.

RUBÉN DARÍO ACUÑA MONTES

Monografía para optar al título de:

ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director:
JHON FREDDY QUINTERO TAMAYO
Ms(c) Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
VALLEDUPAR
2017

Nota de aceptación:

_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Valledupar, Abril de 2017

INDICE

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

RESUMEN

La propuesta realizada sobre un sistema de gestión de seguridad informática de acuerdo a la normativa ISO/IEC 27001. Tiene como fin de implementar un SGSI en la Comunidad educativa del Centro Educativo de Sistemas “Uparsistem”.

Este sistema se basa en las directrices indicadas en la norma ISO/IEC 27001, y en el marco del mismo se generó un análisis de *GAP (*análisis de gap, permite comparar los procesos actuales que tiene la organización con los lineamientos de cumplimiento de la norma ISO/IEC 27001 y establecer en qué áreas o procesos se debe priorizar y enfocar el esfuerzo para permitir incrementar la seguridad de la información - Fuente: http://www.gapanalisis.com/), que permita evidenciar un nivel de brechas significativo en la mencionada Comunidad, con base en el cual se estableció políticas y controles de mejoramiento de los procesos de seguridad de la información y se definieron las declaraciones de aplicabilidad que fortalecerán todo el análisis de riesgos efectuado.

Palabras Claves: Sistema, informática, seguridad.

ABSTRACT

The proposal made on a system of information security management according to ISO / IEC 27001. Its regulations to implement a SGSI in educational Community Education Center Systems "Uparsistem".

This system is based on the guidelines in the ISO / IEC 27001, and under the same analysis GAP (gap analysis, generated for comparing the current processes that the organization has with the guidelines of compliance with the standard ISO / IEC 27001 and identify possible areas or processes should prioritize and focus the effort to allow increased information security - Source: http://www.gapanalisis.com/), which will uncover a level of significant gaps in said Community, based on which policies and controls to improve security processes information was established and applicability statements that will strengthen the entire risk analysis effected defined.

Keywords: system, computer security

1. INTRODUCCION

Cada vez vemos más la importancia que tiene la tecnología de la información en nuestro entorno y también en las empresas y organizaciones. Debido al volumen de información que se trata y maneja por su parte, el trabajo de protegerla es uno de los retos que implica un mayor esfuerzo en un empresa, por lo que un sistema de Gestión de Seguridad Informática (SGSI), de acuerdo a las normativa ISO, es uno de los pilares fundamentales para lograr todos esos objetivo que en primera instancia es salvaguardar los datos confidenciales dentro de una organización, y también ayuda a gestionar, conocer y minimizar los impactos ocasionados por los riegos a los que son expuestos, nos apoyaremos en la normativo ISO/IEC 27001:2013, la cual ofrece una guía para lograr los objetivo y así controlar los riegos.

Con base a lo anterior expuesto la propuesta planteada al Centro Educativo de Sistemas UPARSISTEM, tiene como objetivo principal Implementar un Sistema de Gestión de Seguridad Informática (SGSI), el cual es poder mostrar el paso a paso para la elaboración de un plan de acuerdo a la normativa ISO/IEC 27001:2013, acorde a las necesidades.

No importa el tipo de organización independiente de su tamaño y naturaleza, debe ser consciente que la diversidad de amenazas existentes que actualmente atentan contra la seguridad y privacidad de la información, representan un riesgo que al materializarse no solo les puede acarrear costos económicos, sanciónales legales, afectación de su imagen y reputación, sino que pueden afectar la continuidad y supervivencia del negocio.

Por lo anterior la responsabilidad e importancia del manejo de información posee muchos aspectos entre ellos los archivos, documentos, mensajería, Sistemas de Información internos y externos.

Las instituciones educativas y especialmente para este proyecto “Uparsistem”, es reconocida en toda la región, en Valledupar, es líder y lleva la vanguardia, de instituciones técnicas con énfasis en sistemas, por lo que amerita, esta investigación. Esta institución trata información, primeramente, académica y personal, así como la información de docentes y comunidad educativa; la dificultad es sobre la falta de control en posible riesgo y la pérdida de información o acceso excesivo, lo cual pueda generar un daño en el sistema informático.

Por lo que se hace necesario implementar en la comunidad educativa de “Uparsistem” un sistema de gestión de seguridad de la información o medidas informáticas que permita prevenir y controlar estas insolvencias.

Además, y conforme a sus demás políticas de crecimiento, “Uparsistem”, tiene como principio natural de su objeto social, la inclusión de las Tics y por consiguiente el desarrollo, de buenas prácticas en cuanto a seguridad de la información.

2. PLANTEAMIENTO DEL PROBLEMA

“Uparsistem”, posee sistemas informáticos, muy básicos, que le ayuda a manejar con muchos riesgos sus actividades diarias. Actualmente no se evidencia la importancia que debe dársele a la seguridad informática para proteger los activos de información existentes, por lo cual se está dando continuidad a los problemas actuales sobre algunas vulneraciones a sus sistemas informáticos, y lo peor, aquellos que podrían a futuro, perjudicar su tranquilidad informática.

No proteger la información es exponer a la institución en general porque tiene el valor y activo más importante para la institución, una ruptura en la seguridad puede dar el caso que un estudiante cambie sus calificaciones y a la vez los reportes o un caso más relevante, se pierda la información.

Por lo antes mencionado, es que surge la necesidad de realizar un plan para implementar un Sistema de Gestión de Seguridad Informática (SGSI) para el área administrativa del Centro Educativo de Sistemas UPARSISTEM, ya que el flujo de información es bastante alto y no cuenta con adecuado manejo de este activo tan importante como lo es la información.

Por lo que se plantea una propuesta para realizar un sistema de Gestión de seguridad informática (SGSI) para el Centro Educativo de Sistemas UPARSISTEM de acuerdo a la normativa ISO/IEC 27001, el cual brinda una guía paso a paso para salvaguardar los datos de la institución.

Los riesgos en el control de información a través de las plataformas implementadas siempre deben reevaluarse, auditarse y aplicarse políticas de control, la institución educativa objeto del presente trabajo aún no cuenta con un sistema que le permita mantener seguro su principal activo, la información,

apegándose únicamente a sistemas de seguridad comunes que no siempre garantizan los resultados, sin que existan una responsabilidad a cargo de un profesional, de igual manera los usuarios no cuentan con la capacitación, conocimiento y responsabilidad al momento de interactuar con la base de datos, permitiendo accesos a personal ajeno a la institución y no autorizado, divulgación de contraseñas, sistema de autenticación débil, entre otros problemas.

Por lo expuesto anteriormente, es que la institución “Uparsistem”, ha tenido a bien aceptar la propuesta en mención, ya que se ve con mucha preocupación que la información tenga cierto riesgo tanto la que está en la nube como la que se encuentra localmente, pero que tiene acceso remoto y se espera alguna solución para mejorar la seguridad de los servicios instalados a través del proyecto TIC de la institución, con el fin de darle continuidad al mismo; hasta el momento no se cuenta con políticas de seguridad ni con alguna capacitación a los docentes para el manejo de contraseñas, igualmente no se ha hecho auditoría ni seguimiento a todos los sistemas para ver qué tan seguros son ante cualquier ataque, la página web no cuenta con ningún sistema de protección o seguridad, sólo los básicos ofrecidos por el operador Hosting donde se aloja la página, la autenticación funciona de manera normal, sin tener mínimos requerimientos.

Finalmente cabe resaltar que de acuerdo a las políticas de la institución se proyecta ampliar las plataformas informáticas vía web para otros servicios, lo que implica mayores riesgos y vulnerabilidades por atender.

¿El Centro Educativo de Sistemas – Uparsistem-, está preparada en la actualidad, para contrarrestar, a hackers maliciosos, que ingresen al sistema?

3. JUSTIFICACIÓN.

El Centro Educativo de Sistemas –Uparsistem- es una institución de Educación técnico para el desarrollo y el trabajo aprobado por la secretaria de educación municipal ubicado en la ciudad de Valledupar, al paso de los años se ha convertido en una institución de alto prestigio en la ciudad, brindando excelentes escenarios de capacitación para aquellas personas que quieren realizar una carrera técnica.

Por el gran volumen de estudiantes esta cuenta con una base de datos muy grande e información confidencial de todos sus usuarios, clientes, proveedores, estudiantes, docentes e información financiera de la institución, por lo que se hace necesario implementar un plan para asegurar dicha información, y proponer un Sistema de gestión de Seguridad Informática, es el soporte base para lograr el objetivo principal que es salvaguardar el activo más preciado que tiene cualquier organización o institución.

Es precisamente por el crecimiento de la Institución y además por los avances significativos que tiene las tecnologías y el desarrollo de la internet, que nos lleva a la reflexión de preocuparnos por toda la información que posee Uparsistem en la red, ya que lastimosamente se encuentra vulnerada la seguridad, lo que originaría ataques para acceder a la información privada para aprovecharse de ella y muy posiblemente cometer actos delincuenciales e ilícitos.

La existencia de un sistema de seguridad de la información en las organizaciones genera sentido de pertenencia y apropiación en temas de seguridad en las personas, de tal forma, que se logra la participación activa de toda la organización en la planeación, definición, identificación e implementación de

medidas orientadas a salvaguardar la seguridad de la información de la organización.

La implementación de un Sistema de Gestión de Seguridad de la Información, requiere que inicialmente se realicé un proceso ineludible de clasificar los activos de información en términos de su valor, requerimientos legales, sensibilidad y criticidad para la organización, con el propósito de identificar los riesgos de seguridad asociados con la información y de esta forma realizar un análisis para definir y establecer los mecanismos más convenientes para protegerla.

Para llevar a cabo el presente proyecto es necesario contar con normativas y estándares internacionales como es la ISO, que ofrece una guía de paso a paso, para la propuesta de implementar un sistema de gestión de seguridad informática en la institución educativa.

Uparsistem, requiere diseñar, implementar y mantener un Sistema de Gestión de Seguridad de la Información mediante un conjunto coherente de procesos para la gestión eficaz de acceso a la información. Se requiere como conocer el estado actual de sus activos de información, clasificarlos, priorizarlos y determinar su valor en caso de pérdida de información, lo que implica que es necesario que se conozcan los posibles riesgos que afectan la seguridad de la información y se establecen los mecanismos para minimizar el impacto en caso de presentarse la materialización de una vulnerabilidad.

4. OBJETIVOS.

4.1. Objetivo general.

Implantar un Sistema de Gestión de Seguridad Informática para la Institución Uparsistem, basado en los requisitos de la norma 27001, para incrementar la confianza en los Sistemas de Información, reducir los riesgos y garantizar la confidencialidad, integridad y disponibilidad de la información en todos sus niveles.

4.2. Objetivos específicos.

- Identificar las amenazas y posibles riesgos informáticos a los que se enfrenta el centro educativo de sistemas Uparsistem.

- Analizar las amenazas y vulnerabilidades, y establecer controles para minimizar los riesgos encontrados.

- Sugerir medidas de seguridad para preservar los activos informáticos del centro educativo de sistemas Uparsistem, con base a la confidencialidad, integridad y disponibilidad.

- Divulgar sistema de gestión de seguridad de la información (SGSI), en toda la Institución, y capacitar el personal.

5. MARCO REFERENCIAL

Este proyecto está centralizado en realizar una propuesta para implementar un Sistema de Gestión de Seguridad Informática (SGSI) en una institución académica del nivel técnico en la ciudad de Valledupar. Debido al alto crecimiento de la ciudad en lo comercial, por el auge de las construcciones de varias urbanizaciones, edificios y centro comerciales, son muchas las personas del departamento del cesar y sus alrededores que tiene como referencia a la ciudad para educar a sus hijos ya sea a nivel Profesional, tecnológico y técnico.

Por esta razón tan importante es que instituciones como UPARSISTEM, realizan una gran laborar comercial en ofrecer carreras técnicas en Diseño Gráfico, Secretaria Sistematizado, Mantenimiento y Reparación de equipos de cómputo, Contabilidad sistematizadas, bachillerato por módulos, Criminalística, operador de maquinaria pesada entre otras; al público en general y por esta razón es vital contar con un Sistema de Gestión de Seguridad Informática.

5.1. MARCO TEORICO

Para este proyecto, tenemos como base la norma ISO/IEC 27001, que contiene los lineamientos necesarios para implementar el SGSI, también sirve de referencia la Norma Técnica Colombiana NTC-ISO/IEC 27001, que es la misma norma anterior pero adaptada a procesos en nuestro país por ICONTEC.

Existen casos de éxito de universidades y entidades colombianas y europeas principalmente que han realizado implementaciones de Sistemas de Gestión de Seguridad de la Información y recomiendan algunos tips como: documentar el SGSI, exigir el debido cumplimiento de los procesos y procedimientos establecidos,

realizar revisiones periódicas del mismo y sensibilizar al personal de la importancia de la seguridad de la información y demás temas relacionados.

Debido a la evolución permanente de las tecnologías de la información y las comunicaciones que demandan un mayor esfuerzo para garantizar la seguridad, a las constantes amenazas que hoy en día atentan contra la seguridad de la información que cada vez son más especializadas, complejas y avanzadas, y a la normatividad vigente que regula y exige una mayor protección y privacidad de los datos sensibles, personales, comerciales y financieros de las personas, la organizaciones deben contar con un modelo o Sistema de Gestión de Seguridad de la Información basado en estándares de seguridad reconocidos a nivel mundial, con el propósito de poder establecer y mantener un gobierno de seguridad alineado a las necesidades y objetivos estratégicos del negocio, compuesto por una estructura organizacional con roles y responsabilidades y un conjunto coherente de políticas, procesos y procedimientos, que le permiten gestionar de manera adecuada los riesgos que puedan atentar contra la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y no repudio de la seguridad de la información.

Para lograr una adecuada gestión de la información es indispensable que las organizaciones establezcan una metodología estructurada, clara y rigurosa para la valoración y tratamiento de los riesgos de seguridad, con el objetivo de (i) conocer el estado real de la seguridad de los activos de información a través de los cuales se gestiona la información del negocio, (ii) identificar y valorar las amenazas que puedan comprometer la seguridad de la información y (iii) determinar los mecanismos y medidas de seguridad a implementar para minimizar el impacto en caso de las posibles pérdidas de confiabilidad, integridad y disponibilidad de la información.

5.1.1. Seguridad de la información.

La Seguridad de la Información, de acuerdo a la norma ISO 27000:20146, se define como la preservación de la confidencialidad, integridad y disponibilidad de la información. De acuerdo a la Asociación Española para la Calidad[1], la Seguridad de la Información tiene como propósito la protección de la información y de los sistemas de la información contra las amenazas y eventos que atenten con el acceso, uso, divulgación, interrupción y destrucción de forma no autorizada[2].

La información representa uno de los activos más valioso de las organizaciones, lo que implica que es indispensable asegurar su protección contra amenazas y eventos que puedan llegar comprometer su confidencialidad, integridad y disponibilidad.

La información puede existir en diferentes medios tanto físicos como electrónicos, pero independientemente del medio, es necesario que las organizaciones garanticen y aseguren la debida protección de la información durante su recolección, almacenamiento, tratamiento y uso.

La seguridad de la información busca preservar la confidencialidad, integridad y disponibilidad de la información mediante el establecimiento de un conjunto coherente de procesos, normas y herramientas para la gestión eficaz de acceso a la información, y la implementación de mecanismos y medidas de seguridad tanto físicas como lógicas, orientadas a la prevención y detección de amenazas internas y externas que puedan atentar contra la seguridad de la organización y la continuidad del negocio.

---

[1] La **Asociación Española para el Control de la Calidad (AECC)** (como así se denominaba en sus inicios) fue fundada en el año 1961 por un grupo de profesionales que deseaban mejorar sus conocimientos en las técnicas de Control de Calidad, en el ámbito de una asociación que pudiera acoger tanto a las empresas como a los expertos en la materia.

[2] Tomado de: http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion.

La seguridad de la información en una organización, es un proceso de mejora continua que demanda la participación activa de toda la organización y busca preservar, entre otros, los siguientes principios de la información:

- La confidencialidad, asegurando que solo las personas debidamente autorizadas tengan acceso a la información.

- La disponibilidad, asegurando que la información esté totalmente disponible para las personas debidamente autorizadas cuando ellos la requieran.

- La integridad, asegurando que la información no sea modificada sin la debida autorización.

- La autenticidad, con el propósito de garantizar la identidad de la persona que genera la información. La autenticidad de la información, es la capacidad de asegurar que el emisor de la información es quien dice ser y no un tercero que esté intentando suplantarlo.

- El no repudio, con el propósito de conocer exactamente quienes son los actores que participan en una transacción o una comunicación y no puedan negarlo en ningún momento. El no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje.

- La trazabilidad, con el objetivo de poder monitorear o rastrear cualquier operación que se realiza sobre la información desde su mismo origen.

La seguridad de la información dentro de las organizaciones, depende del nivel de protección y seguridad de sus activos de información, por lo tanto, es fundamental la implementación de medidas y controles de seguridad adecuados, y

el permanente monitoreo, revisión y mejora de los mismos de manera proactiva con el objetivo de garantizar su efectividad.

5.1.2. Gestión de seguridad de la información.

La gestión de la seguridad de la información es un proceso continuo que consiste en garantizar que los riesgos de la seguridad de la información sean identificados, valorados, gestionados y tratados por todos los miembros de la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La gestión de la seguridad de la información requiere la participación activa de toda la organización con relación a la planeación, definición, identificación e implementación de controles y medidas orientadas a salvaguardar la seguridad de la información, así como el debido control de acceso a los recursos y activos de información.

La gestión de la seguridad de la información, implica que las organizaciones clasifican sus activos de información en términos de su valor, requerimientos legales, sensibilidad y criticidad, con el propósito de identificar los riesgos que pueden afectar su seguridad y determinar las medidas de prevención, detección, retardo y reacción que se requieran implementar para controlar el acceder no autorizado a las instalaciones, recursos, sistemas e información de la organización, o cualquier amenaza proveniente del entorno, la naturaleza y las acciones del hombre que pueda llegar a comprometer el normal funcionamiento y operación del negocio[3].

[3] Tomado de: http://www.iso27000.es/sgsi.html

5.1.3. Sistema de gestión de seguridad de la información.

Con el objetivo de garantizar que las organizaciones realizan una correcta gestión de la seguridad de la información, es necesario contar con un proceso sistemático, documento, conocido y adoptado por toda la organización, basado en un enfoque de gestión de riesgos. Este proceso, es el que constituye un Sistema de Gestión de Seguridad de la Información.

De acuerdo a la norma NTC-ISO-IEC 27001:2013[4], un sistema de gestión de seguridad de la información tiene por finalidad preservar la confidencialidad, integridad y disponibilidad de la información, a través de la aplicación de un proceso de gestión del riesgo.

Un Sistema de Gestión de Seguridad de la Información, les permite a las organizaciones gestionar de manera efectiva los riesgos asociados a la seguridad sobre sus activos de información mediante la identificación de las amenazas que puedan llegar con comprometer la seguridad sus activos de información, lo cual, genera confianza en sus partes interesadas debido a que demuestra que los riesgos de la organización son debidamente gestionados.

Un Sistema de Gestión de Seguridad de la Información permite el establecimiento de un gobierno de seguridad, soportado en una estructura organizacional, responsabilidades, políticas, procedimientos, procesos y recursos, para gestionar de manera adecuada la seguridad de la información. Proporciona una herramienta que le ayuda a las organizaciones a establecer políticas, procedimientos, medidas y controles de seguridad alineados a los objetivos de negocio, y provee los elementos adecuados para la debida gestión de los riesgos con propósito de poder mantener el riesgo por debajo del nivel definido por la organización. Un Sistema de Gestión de la Seguridad de la Información les permite

[4] NTC-ISO-IEC 27001:2013, Capitulo Introducción.

a las organizaciones tener una visión general del estado de protección y vulnerabilidad de sus activos de información y de la efectividad de las medidas de seguridad que se implementen, insumos que son fundamentales para apoyar la toma de decisiones por parte de la alta directiva con relaciones a las estrategias a seguir.

La implementación de un Sistema de Gestión de Seguridad de la Información, le provee a las organizaciones un proceso de mejora continua que asegura la debida y continua gestión de los riesgos de seguridad y permite la participación activa de toda la organización con relación a la planeación, definición, identificación e implementación de controles y medidas orientadas a salvaguardar la seguridad de los activos de información de la organización.

5.1.4. Normas ISO/IEC 27000.

La familia de las normas ISO/IEC 27000, son un marco de referencia de seguridad a nivel mundial desarrollado por la International Organization for Standardization - ISO e International Electrotechnical Commission – IEC, que proporcionan un marco, lineamientos y mejores prácticas para la debida gestión de seguridad de la información en cualquier tipo de organización. Estas normas especifican los requerimientos que deben cumplir las organizaciones para establecer, implementar, poner en funcionamiento, controlar y mejorar continuamente un Sistema de Gestión de Seguridad de la Información.

En Colombia, el Instituto Colombiano de Norma Técnicas y Certificaciones, ICONTEC, es el organismo encargado de normalizar este tipo de normas.

Las siguientes son algunas de las normas que componen la familia ISO/IEC 27000, las cuales serán el marco teórico que se tendrá en cuenta para efectos del presente trabajo:

- **ISO/IEC 27000.** Esta norma proporciona una visión general de los sistemas de gestión de seguridad de la información y contiene los términos y definiciones que se utilizan en las diferentes normas de la 27000.

- **ISO/IEC 27001.** La última versión de esta norma fue publicada a finales del 2013, y corresponde a la principal norma de la serie 27000 debido a que contiene los diferentes requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información en las organizaciones independiente de su tipo, tamaño o naturaleza. Esta norma también incluye los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adoptadas a las necesidades de la organización.

La versión 2013 de la norma ISO 27001, alineo su estructura conforme a los lineamientos definidos en el Anexo SL12 de las directivas ISO/IEC, con el objetivo de mantener la compatibilidad entre las normas ISO de sistemas de gestión que se han ajustado a este anexo. Este enfoque de la estructura de la nueva ISO27001: basado en el Anexo SL, les ayuda a las organizaciones que deseen integrar sus diferentes sistemas de gestión, como el de Calidad, Ambiental, Seguridad de la Información, etc., en un único sistema integrado de gestión, debido a que las normas ISO que se han ajustado al Anexo SL, manejan aspectos comunes como, la misma estructura de alto nivel e idénticos títulos de numerales, textos y términos.

Los dominios de la norma ISO/IEC 27001: corresponde a los diferentes capítulos que establecen los requerimientos que las organizaciones deben cumplir para el establecimiento de un Sistema de Gestión de Seguridad de la Información, los cuales se resumen a continuación:

- **ISO/IEC 27002.** Guía de buenas prácticas en seguridad de la información que describe de forma detallada las acciones que se deben tener en cuenta para el establecimiento e implementación de los objetivos de control y controles descritos de una forma general en el Anexo A de la norma ISO 27001.

- **ISO/IEC 27003.** Guía que contiene aspectos necesarios para el diseño e implementación de un Sistema de Gestión de Seguridad de la Información de acuerdo a los requerimientos establecidos en la norma ISO/IEC 27001, donde se describe el proceso desde la planeación hasta la puesta en marcha de planes de implementación.

- **ISO/IEC 27004.** Guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un Sistema de Gestión de Seguridad de la Información y de los objetivos de control y controles implementados de acuerdo al Anexo A de la norma ISO 2700113.

- **ISO/IEC 27005.** Esta norma establece los lineamientos para la gestión de riesgos de seguridad de la información y está diseñada para ayudar a las organizaciones en la implementación de un Sistema de Gestión de Seguridad de la Información basada es un enfoque de gestión de riesgos. Entre otros aspectos, establecer lo requerimiento que se deben tener en cuenta para el proceso de valoración de riesgos, relacionados con la identificación, análisis, evaluación y tratamiento de los riesgos en la seguridad de la información.

- **ISO/IEC 27006**. Establece los requisitos relacionados en la norma ISO 27001 que deben cumplir las organizaciones para la acreditación de entidades de

auditoría y certificación de Sistemas de Gestión de Seguridad de la Información.

- **ISO/IEC 27035.** Proporciona una guía sobre la gestión de incidentes de seguridad en la información.

- **CICLO DE MEJORA CONTINÚA VS NORMA ISO/IEC 27001:2013** El ciclo de mejora continua, también conocido como ciclo PDCA (del inglés plan do-check-act) o PHVA (planificar-hacer-verificar-actuar) o Ciclo de Deming por ser Edwards Deming su creador, es uno de los sistemas más usados para la implementación de un sistema de mejora continua, el cual establece los siguientes cuatro pasos o fases esenciales que de forma sistemática las organizaciones deben llevar a cabo para lograr la mejora continua de sus sistemas de gestión:

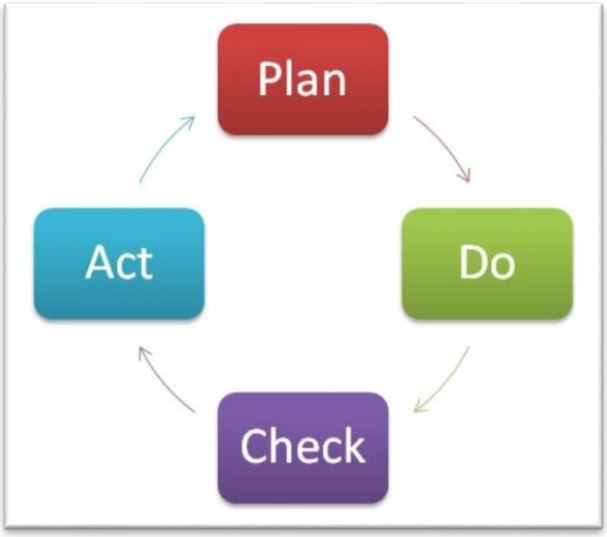

Figura 1: Ciclo de Mejora Continua (Ciclo Deming)
Fuente: http://www.pdcahome.com/5202/ciclo-pdca/

Fase Planificar (Plan):	En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.

Pase Hacer (Do):	En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.
Fase Verificar (Check):	Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.
ase Actuar (Act):	Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

Tabla 1. Fases del Clico de Mejora Continua
Fuente: http://www.pdcahome.com/5202/ciclo-pdca/

En la versión 2013 de la norma ISO/IEC 27001, no aparece la sección de "Enfoque basado en procesos" que existía en la versión 2005, lo cual brinda una mayor flexibilidad en el momento de seleccionar o definir un modelo para la mejora continua del Sistema de Gestión de Seguridad de la Información.

5.1.5. Fase PLANEAR en la norma ISO 27001:2013[5].

Contexto de la organización de la norma ISO 27001:2013, se determina la necesidad de realizar un análisis de las cuestionas externas e internas de la organización y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesas de la organización en el alcance del SGSI.

Liderazgo, se establece las responsabilidades y compromisos de la Alta Dirección respecto al Sistema de Gestión de Seguridad de la Información y entre

[5] NTC-ISO-IEC 27001:2013, Pág. 1-2 s.s.

otros aspectos, la necesidad de que la Alta Dirección establezca una política de seguridad de la información adecuada al propósito de la organización, aseguren la asignación de los recursos para el SGSI y que las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen.

Planeación, se establece los requerimientos para la valoración y tratamiento de riesgos de seguridad y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento.

Soporte, se establece que la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua Sistema de Gestión de Seguridad de la Información.

5.1.6. Fase HACER en la norma ISO 27001:2013.

En el capítulo 8 - Operación de la norma ISO 27001:2013, se indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

5.1.7. Fase VERIFICAR en la norma ISO 27001:2013.

En el capítulo 9 - Evaluación del desempeño, se define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información.

5.1.8. Fase ACTUAR en la norma ISO 27001:2013.

En el capítulo 10 - Mejora20, se establece para el proceso de mejora del Sistema de Gestión de Seguridad de la Información, que a partir de las no-conformidades

que ocurran, las organizaciones deben establecer las acciones más efectivas para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan.

5.2. ANTECEDENTES.

Para lograr los objetivos del presente proyecto a continuación de darán a conocer una serie de antecedentes que servirán de apoyo para tener un amplio concepto y ver resultados y alcances obtenidos en diversos proyectos similares a que se está desarrollando.

5.2.1. Implementación SGSI en la comunidad nuestra señora de gracia.

En este proyecto el autor da a conocer una serie de resultados muy importantes obtenidos luego de la Implementación de sistema de gestión de seguridad de la información (SGSI) en la Comunidad Nuestra Señora de Gracia, como lo es la definición de roles y propuestas de asignación y estructura organizativa, políticas de control, planificación de actividades, responsabilidades, prácticas, procesos y recursos, Propuesta de alineación tecnológica frente a los procesos estratégicos de la organización, Propuesta de un plan de continuidad del negocio permitiendo que la empresa pueda recuperarse después de algún incidente que pudiese presentarse, Capacitación y concientización al Departamento de Sistemas sobre el impacto favorable que tendría el establecimiento de una política en ISO 27001.[6]

[6] Tomado de: http://www.konradlorenz.edu.co/images/stories/articulos/SGSI.pdf

5.2.2. Implementación SGSI aplicada al área recursos humanos DECEVAL S.A.

En este proyecto el autor definen unos alcances para la implementación del sistema de gestión de seguridad de la Información (SGSI), como asegurar que los empleados, contratistas y terceras partes sean conscientes de las amenazas de seguridad, de sus responsabilidades y obligaciones y que estén equipados para cumplir con las políticas de la organización en el desempeños de las labores diarias para reducir el riesgo asociados por los errores humanos.[7]

El presenta proyecto estará alineado con el estándar para la seguridad de información ISO/IEC. 27001. (Information technology - Security techniques - Information security management systems - Requirements). El cual fue aprobado y publicado como estándar internacional en Octubre de 2005 por International Organization for Standardization (ISO) y por la comisión International Electrotechnical Commission (IEC).[8]

[7] Tomado de: https://www.dspace.espol.edu.ec/bitstream/123456789/24204/1/1PROYECTO%20DE%20GRADUACION%20IMPLEMENTACION%20DE%20SGSI%20A%20LA%20EMPRESA.docx.
[8] Tomado de: http://auditoriasistemasucb.pbworks.com/f/NORMA+ISO+27001.doc

5.3. MARCO CONCEPTUAL

5.3.1. Normativa ISO 27001.

Para lograr los objetivos de implementar un SGSI, en la institución se tomará como referencia lo que indica la norma ISO 27001. Esta norma adopta el establecimiento, implementación, operación, seguimiento, revisión, monitoreo y mejora de un sistema de gestión de seguridad de la información (SGSI) en cualquier tipo de empresa u organización sea privada o pública. Actualmente cuenta con una última versión que la 2013.[9]

5.3.2. Seguridad informática.

Cada día las empresas y organizaciones están expuestas a la pérdida de datos e información importante, y estos sucesos pueden ocasionar problemas en el negocio, que puede llevarlo al cierre total de sus actividades, por esta razón es que la seguridad informática hoy día asume un papel muy importante dentro de una organización ya que es la disciplina que se ocupa en diseñar normas, políticas, métodos y técnicas para proveer condiciones seguras y confiables para el procesamiento de datos en un sistemas informático.[10]

5.3.3. Confidencialidad

Propiedad de la seguridad de la información que garantiza que la información personal sea protegida y esta no sea divulgada sin el consentimiento de la persona.

5.3.4. Integridad.

---

[9] Tomado de: http://www.iso27000.es/iso27000.html

[10] Tomado de: http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml

Propiedad de la seguridad de la información que garantiza que la información no ha sido alterada, o modificada por personas no autorizadas.

5.3.5. Disponibilidad.

Propiedad de la seguridad de la información que garantiza que la información esté disponible, y este pueda accederse por las personas, procesos o aplicaciones autorizadas en el momento que esta se requiera.

5.3.6. Amenazas.

Esta se refiere a la probabilidad de ocurrencia de un incidente ya sea de origen natural o intencionado; esta representa factores de riesgos que pueden explotar una vulnerabilidad existente.

5.3.7. Riesgos.

Es la magnitud en perdida asumida tras la ocurrencia de la explotación de una amenaza o vulnerabilidad.

5.3.8. Vulnerabilidad.

Es un factor de riesgo el cual representa las debilidades y el grado de exposición de un activo informático, esta permite la explotación de una amenaza.

5.3.9. Activo de información.

Aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida.

5.3.10. Anexo SL.

Nuevo esquema definido por International Organization for Standardization - ISO para todos los Sistemas de Gestión acorde al nuevo formato llamado “Anexo SL”, que proporciona una estructura uniforme como el marco de un sistema de gestión genérico.

5.3.11. Análisis De Riesgos.

Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

- **Causa**: Razón por la cual el riesgo sucede.
- **Ciclo De Deming**: Modelo mejora continua para la implementación de un sistema de mejora continua.
- **Colaborador:** Es toda persona que realiza actividades directa o indirectamente en las instalaciones de la entidad, Trabajadores de Planta, Trabajadores Temporales, Contratistas, Proveedores y Practicantes.
- **Controles**: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.
- **Dueño Del Riesgo Sobre El Activo**: Persona responsable de gestionar el riesgo.
- **Impacto**: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.
- **Incidente De Seguridad De La Información:** Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.
- **Oficial De Seguridad**: Persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información.

- **Probabilidad De Ocurrencia**: Posibilidad de que se presente una situación o evento específico.

5.4. MARCO CONTEXTUAL

5.4.1. La Institución.

Figura 2. Logo de la Institución
Fuente: http://www.uparsistem.edu.co/virtual/index.php

- Empresa: Centro Educativo de Sistemas UPARSISTEM.
- Ciudad: Valledupar – Cesar
- Dirección: Calle 16A No. 12 – 36
- Teléfono: 5743427

5.4.2. Misión.

Formar personas para el trabajo, con valores, espíritu emprendedor, capacidad técnica, y comprometidos con el desarrollo regional con una oferta educativa pertinente, de calidad y articulada con todos los niveles de la educación, a la vanguardia de los avances tecnológicos, en procura del bienestar social y del progreso del país.

5.4.3. Visión.

UPARSISTEM se proyecta como la institución de educación para el trabajo y desarrollo humano líder en el Caribe Colombiano, que contribuye con su oferta educativa a elevar la calidad de vida de los habitantes de la región. Propendemos por el reconocimiento nacional de nuestros programas de formación para el trabajo, por su calidad y pertinencia, cumpliendo con el compromiso de articular la educación con el sector productivo, la comunidad y el desarrollo de la Nación.

5.4.4. Política de Calidad.

UPARSISTEM se compromete a prestar un servicio oportuno, personalizado y confiable para satisfacer las necesidades y expectativas de los clientes a través de la oferta de programas de formación técnico laborales, caracterizado por su pertinencia y calidad, soportados en un talento humano competente, infraestructura adecuada, disponibilidad de recursos y mejoramiento continuo de sus procesos.

5.4.5. Organigrama Institución

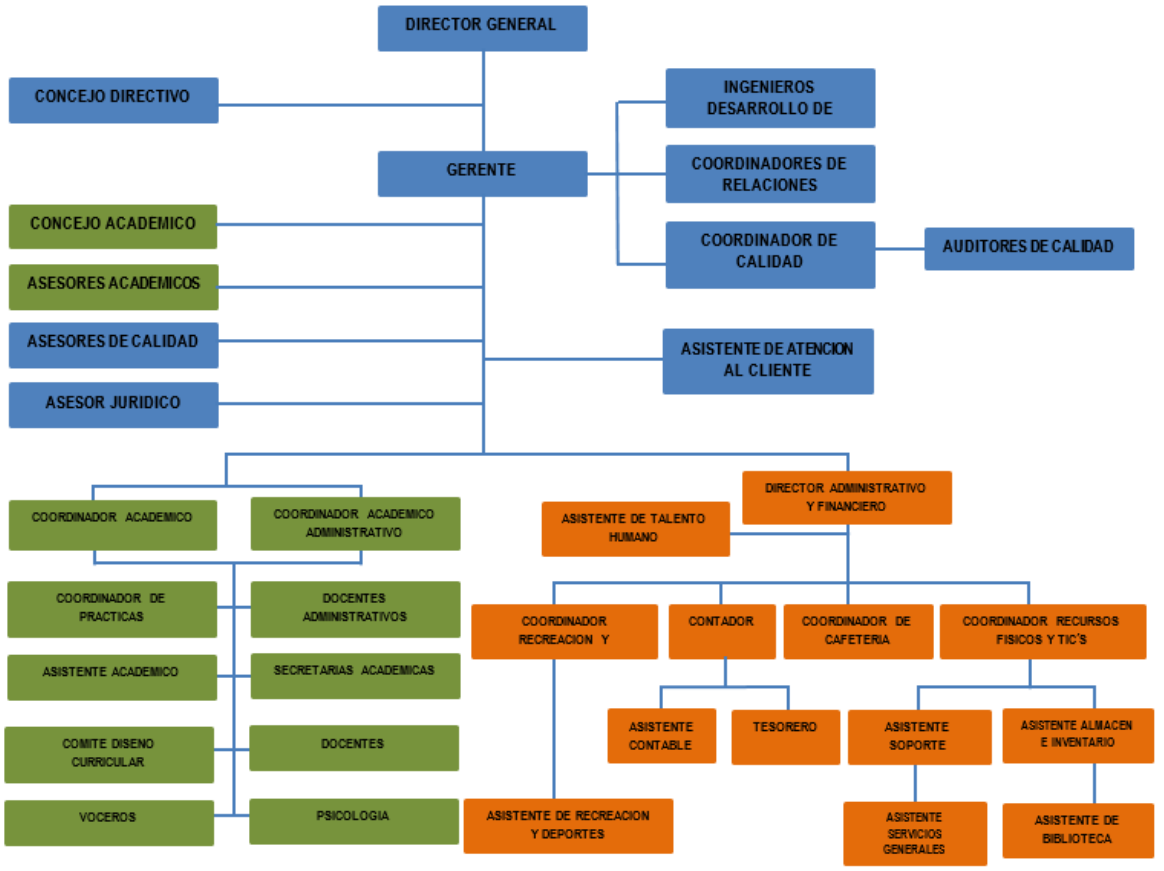

Figura 3. Organigrama Institución
Fuente: Investigación

6. METODOLOGIA.

Para el desarrollo de la propuesta para implementar el sistema de gestión de seguridad informática (SGSI) en el Centro Educativo de Sistemas Uparsistem, este se base en una metodología que tiene un guía paso a paso de procesos a ejecutar de acuerdo a un cronograma de actividades.

6.1. Línea de investigación.

Tomando como referencia la norma ISO/IEC 27001:2013, se puede determinar que la línea de investigación del presente trabajo esta relacionados con los siguientes temas: Tecnología de la información, Seguridad de la Información, Gestión de la Seguridad, Gestión de Riesgos y Sistema de Gestión de Seguridad de la Información.

6.2. Instrumentos De Recolección De Información

Para el desarrollo del presente trabajo de grado, se utilizaron los siguientes mecanismos e instrumentos para la recolección de información:

- ✓ Cuestionario.
- ✓ Observaciones.
- ✓ Entrevistas con funcionarios y sobre todo con el personal de la Dirección de Tecnología de la Entidad.
- ✓ Documentación existente en el sistema de gestión calidad de la entidad.
- ✓ Evaluación con base en la experiencia del autor.

También, se usa de diferentes fuentes de información: primarias, secundarias, tales como tesis, libros, textos, revistas, normas, etc., existentes tanto en medios físicos, electrónicos y publicados en Internet.

6.3. Levantamiento De Información

6.3.1. Diagnóstico General De Seguridad Informática

La siguiente información hace relación al diagnóstico que se elaboró partiendo de las siguientes preguntas.

Figura 4. Encuesta de Control Pregunta 1.
Fuente: el Autor

Figura 5. Encuesta de Control Pregunta 2
Fuente: el Autor

Figura 6. Encuesta de Control Pregunta 3.
Fuente: el Autor

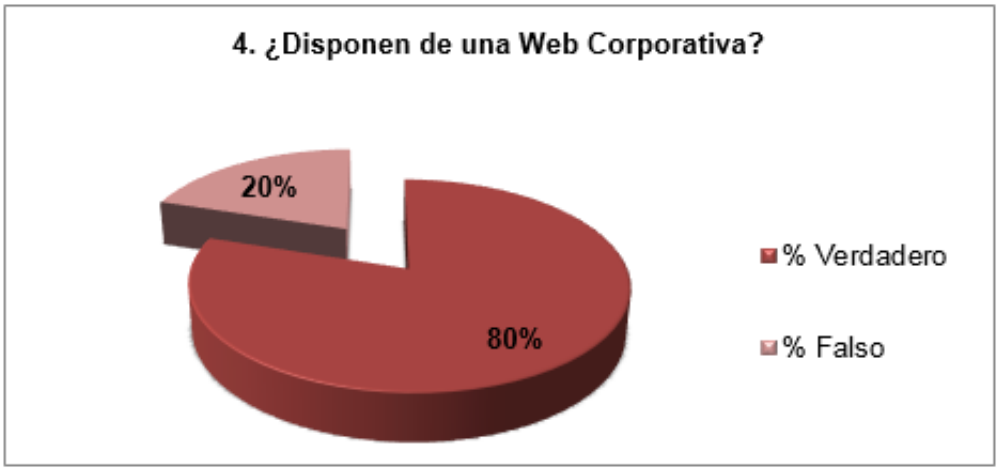

Figura 7. Encuesta Control Pregunta 4.
Fuente: el Autor

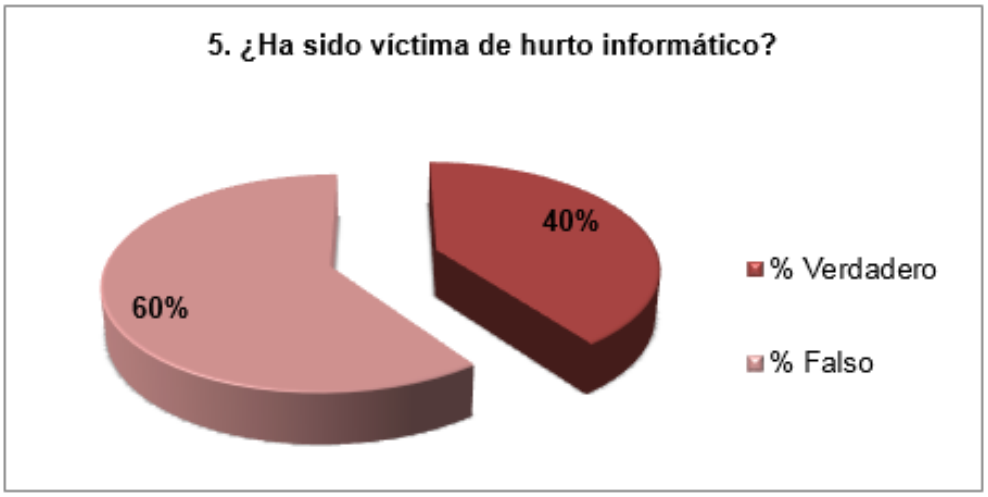

Figura 8. Encuesta Control Pregunta 5.
Fuente: el Autor

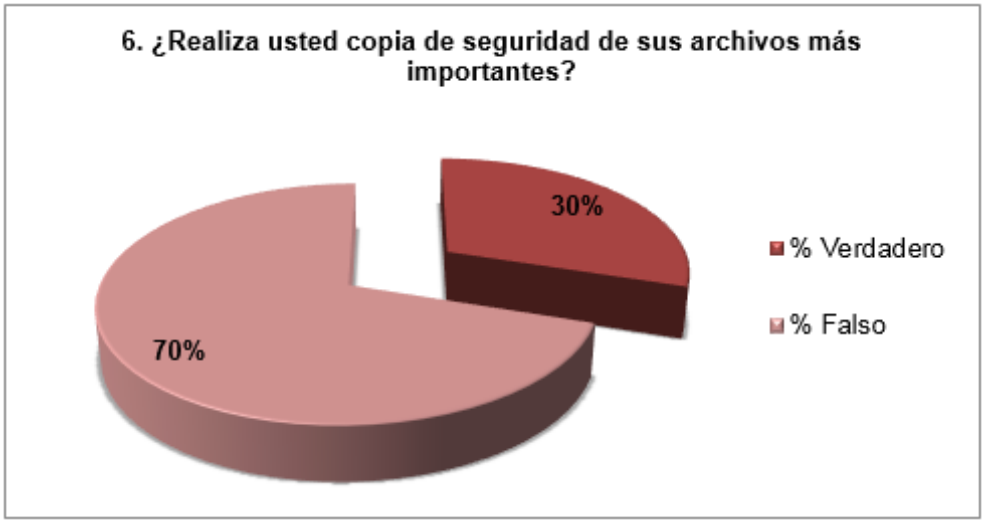

Figura 9. Encuesta Control Pregunta 6.
Fuente: el Autor

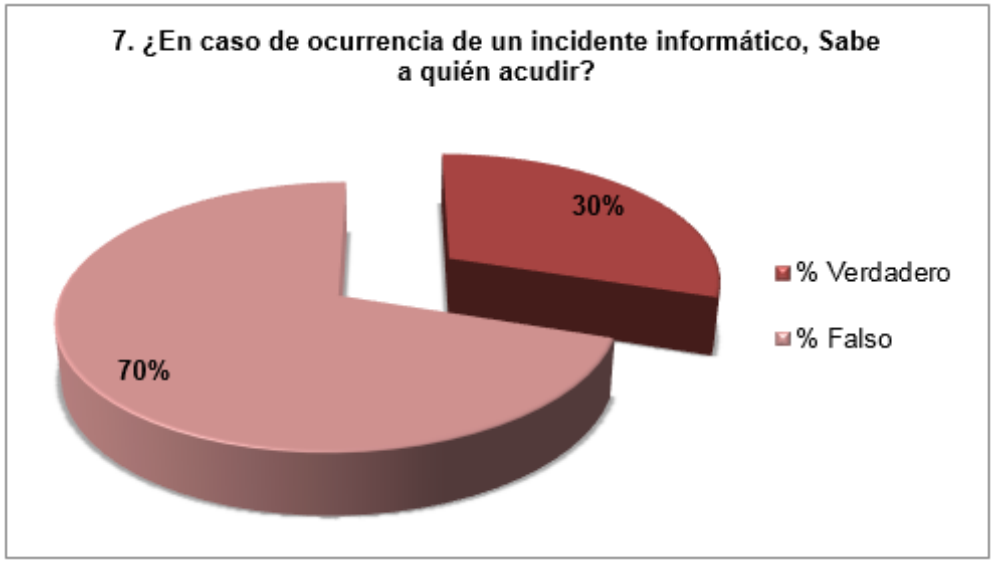

Figura 10. Encuesta Control Pregunta 7.
Fuente: el Autor

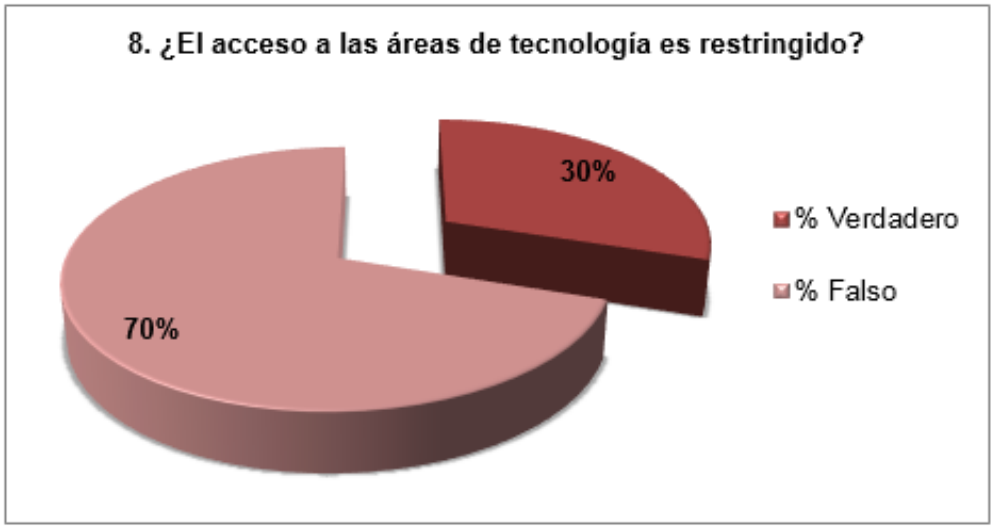

Figura 11. Encuesta Control Pregunta 8.
Fuente. El Autor

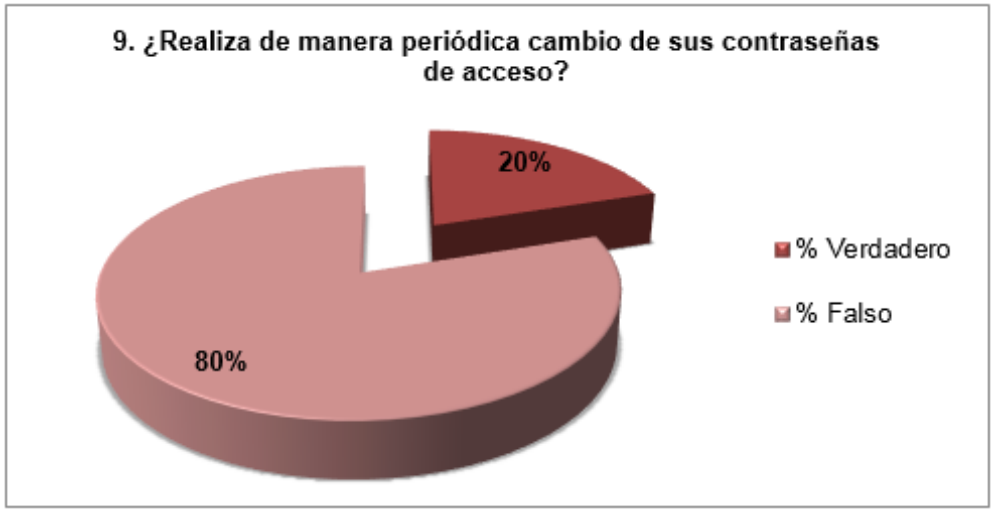

Figura 12. Encuesta Control Pregunta 9.
Fuente: el Autor

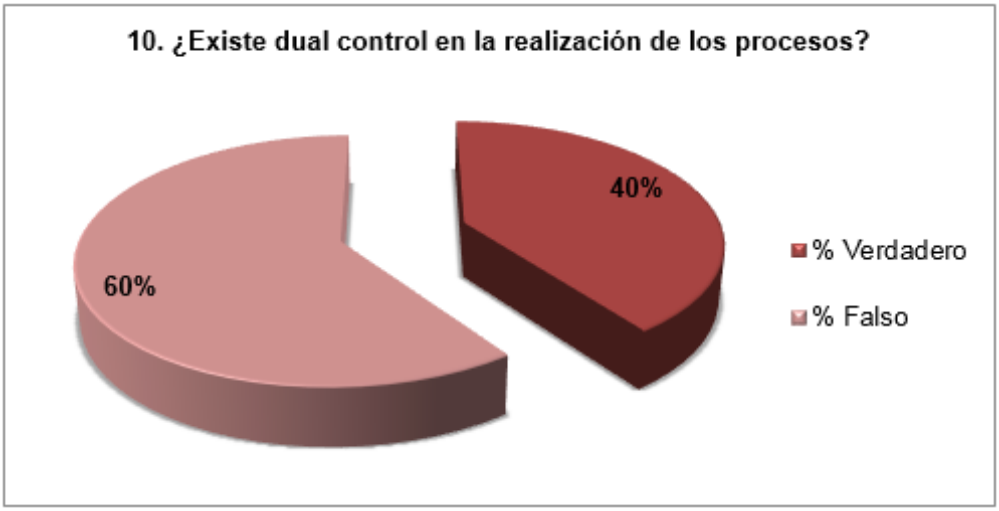

Figura 13. Encuesta Control Pregunta 10.
Fuente: el Autor

6.3.2. Resultados Del Diagnostico Tipo Encuesta

Con la formulación de las anteriores preguntas, se logra establecer el primer indicio de la no aplicabilidad de muchas de las políticas de seguridad informática en las actividades desarrolladas por el establecimiento educativo.

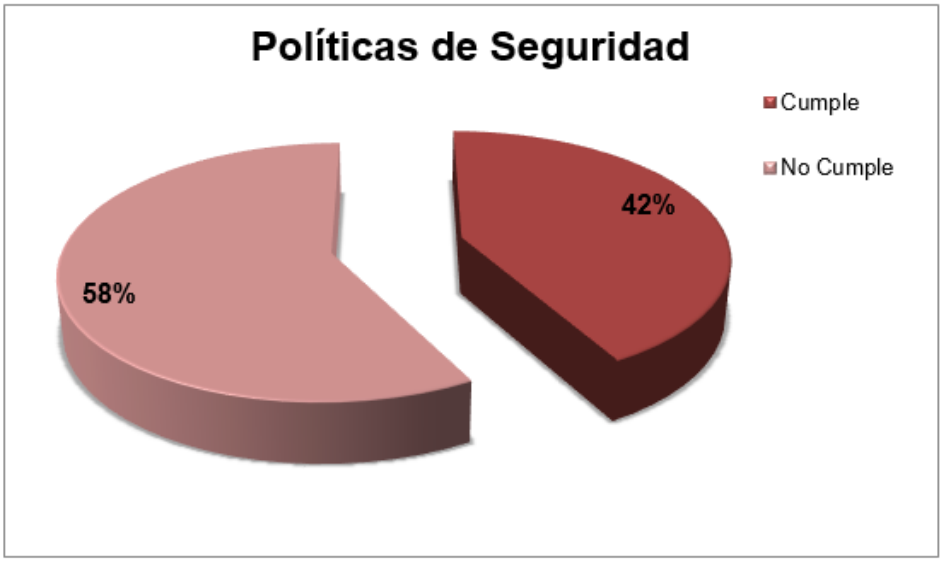

Figura 14. Diagnostico Política de Seguridad.
Fuente: el Autor

6.3.3. Clasificación De Activos Según Magerit

Teniendo en cuenta la clasificación de activos según el modelo normativo MAGERIT se realiza la siguiente tabla, que identifica el tipo de activo que posee la institución y el nombre del mismo.

TIPOS DE ACTIVOS	NOMBRE DE ACTIVO
SERVICIOS INTERNOS [IS]	1. Internet [INTERNET_UPAR] 2. Servidor WEB [SWEB_UPAR] 3. Servidor Telefonía Ip [TI_UPAR] 4. Servidor Base de Datos [SDB_UPAR]
Aplicaciones [SW]	5. Gestión de Matrículas [SIMAT_UPAR] 6. Sistema Gestión Docentes [SIGDOC_UPAR] 7. Sistema Gestión Notas [SGNTA_UPAR] 8. Sistema URPANET [URPANET_UPAR] 9. Portal Web [WEB_UPAR] 10. Herramientas Ofimáticas [OFIMATICAS_UPAR]

	11. Antivirus[ANTV_UPAR] 12. Navegadores WEB [NAV_UPAR] 13. Sistemas Operativos[SO_UPAR]
Equipos [HW]	14. Equipos de Cómputo [PC_UPAR] 15. Tablet [TABLET_UPAR] 16. Cámaras de Seguridad [CAM_UPAR] 17. Enrutadores [ENR_UPAR] 18. Swicth [SWICTH_UPAR] 19. Impresoras [IMP_UPAR] 20. Escáner [ESC_UPAR] 21. UPS [UPS_UPAR] 22. Discos de Estado Solido [SSD_UPAR] 23. VideoBeam [BEAM_UPAR]
Comunicaciones [COM]	24. Central Telefónica [CENTEL_UPAR] 25. Red LAN [LAN_UPAR] 26. Red WIFI [WIFI_UPAR]
Soportes de Información [SOPORINF]	27. Backup SIMAT [BKSIMAT_UPAR] 28. Backup SIGDOC [BKSIGDOC _UPAR] 29. Backup SGNTA [BKSGNTA _UPAR] 30. Backup URPANET [BKURPANET _UPAR]
Equipamiento Auxiliar [AUX]	31. Cableado de RED [CABRED_UPAR] 32. Cableado Electico [CABELE_UPAR 33. Caja de Herramientas [HERR_UPAR] 34. Aires Acondicionados [AACON_UPAR]
Instalaciones [L]	35. Instalaciones de 1 Pisos [INST_UPAR]
Personal [P]	36. Director General [DIRGR_UPAR] 37. Gerente [GER_UPAR] 38. Ingeniero Desarrollo Software [INGD_UPAR] 39. Coordinador de Relaciones [COORD_UPAR]

	40. Coordinador de Calidad [COORDR_UPAR] 41. Auditor de Calidad [AUDC_UPAR] 42. Asesor Jurídico [ASRJ_UPAR] 43. Asesor de Calidad [ASRC_UPAR] 44. Asesor Académico [ASRA_UPAR] 45. Asistente Atención al Cliente [ASIS_UPAR] 46. Coordinador Académico [COORA_UPAR] 47. Docentes [DOC_UPAR] 48. Asistente Académico [ASISAC_UPAR] 49. Secretario Académico [SCRA_UPAR] 50. Director Administrativo y Financiero [DIRAD_UPAR] 51. Asistente Talento Humano[ASIST_UPAR] 52. Contador [CONT_UPAR] 53. Asistente Contable [ASISCON_UPAR] 54. Asistente Soporte [ASISP_UPAR] 55. Asistente Alancen e Inventario [ASISAL_UPAR] 56. Tesorero [TESO_UPAR] 57. Coordinador Recursos Físicos y Tics [COORFIS_UPAR] 58. Asistente Servicios Generales [SERGR_UPAR]

Tabla 2. Inventario Activos.
Fuente: El Autor

6.3.4. Análisis Inicial Control ISO 27001:2013

La norma ISO/IEC 27001:2013 especifica los requerimientos para establecer, implementar, mantener y continuamente mejorar el sistema de gestión de seguridad de la información y agrupa sus requerimientos en 15 cláusulas. La siguiente matriz indica la categorización de cada cláusula de acuerdo a la valoración de procesos inicial:

Descripción del Dominio	Valoración %	Meta
Políticas de Seguridad	0%	100%
Organización de la Seguridad de la Información	14%	100%
Seguridad del Recurso Humano	17%	100%
Gestión de Activos	10%	100%
Control de Acceso	0%	100%
Criptografía	0%	100%
Seguridad Física y del Entorno	20%	100%
Seguridad de las Operaciones	21%	100%
Seguridad de las Comunicaciones	29%	100%
Adquisición, desarrollo y mantenimiento de sistemas	8%	100%
Relación con Proveedores	0%	100%
Gestión de Incidentes de Seguridad de la Información	29%	100%
Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio	25%	100%
Cumplimiento	13%	100%

Tabla 3. Clausulas para análisis de Control ISO 27001
Fuente: el Autor

6.3.5. Estado Inicial Cumplimiento Norma ISO 27001:2013

Figura 15. Estado Inicial Cumplimiento Noma ISO 27001:2103
Fuente: el Autor

En la anterior figura se aprecia un análisis del estado inicial de la institución para el del desarrollo de este proyecto.

7. RESULTADOS.

7.1. Identificación de las amenazas y posibles riegos informáticos a los que se enfrenta el centro educativo de sistemas UPARSISTEM.

En esta fase del proyecto se inicia un análisis de la información obtenida en la fase anterior, incluyendo los activos de la Institución, adicionalmente fueron examinados los procesos de Atención al público. Lo cual permitió hacer un reconocimiento de las laborares realizadas por cada uno de estos departamentos e identificar los aspectos relevantes derivados de su actividad, con el fin de iniciar el diseño del SGSI.

7.1.1. Hallazgos

De esta manera se pudieron determinar los siguientes hallazgos:

- En las visitas realizadas en las instalaciones se observó que existen equipos portátiles sin ningún tipo de seguridad lo que podría suceder que este se extravié y contenga información sensitiva de la institución.
- También se pudo evidenciar que no existe la implementación de bloqueo automático a equipos desatendidos por ausencia del responsable en las estaciones de trabajo.
- Además, se puedo evidenciar que no existe una política de escritorio limpio, y esto permite que personas inescrupulosas con un poco de ingeniería social hacerse a información física que no tiene un buen manejo de custodia.

- No existe un equipo de desarrollo encargado de analizar y verificar aplicaciones, con el fin de ofrecer mejoras en cuanto a los programas o software manejados por la institución educativa.
- Las contraseñas para el manejo del software y página web de la institución, son asignadas de acuerdo a criterios personales de los empleados, sin contar con pautas apropiadas y específicas para determinar las mismas.
- La institución no cuenta con señalizadores que ilustren el paso no autorizado al área de Atención al Público, lo que genera que muchas veces los visitantes llegan de manera muy cercana a la zona donde se encuentran documentos y equipos propios de la actividad económica.
- La copia de seguridad de la información manejada en esta área es realizada de manera esporádica y sin tener en cuenta aspectos mínimos de seguridad de la información.
- No existen términos y condiciones definidos en cuanto al acceso a la página web y sobre los contenidos de la misma, los cuales por naturaleza van dirigidos a la comunidad educativa.

Posterior a la identificación de los hallazgos, se identificaron los procesos relevantes desarrollados en el área de Atención al público, los cuales se resumen de la siguiente manera:

7.1.2. Procesos en Áreas.

- ✓ **Procesos Área Atención a Público.**

PROCESO	DESCRIPCIÓN	FRECUENCIA DIARIA SEMANAL MENSUAL	RESPONSABLE
Atención personalizada a la	Dar respuesta clara, precisa y oportuna a las consultas por los	Diaria	Elicenith García

comunidad estudiantil.	estudiantes, docentes y público en general.		
Recepción de documentación	Recibir y tramitar las solicitudes de PRQS radicas en la institución, con el adecuado ingreso en la plataforma.	Diaria	Elicenith García
Proceso de inscripción	Recibir y tramitar las solicitudes de inscripción y matriculas en los diferentes programas que ofrece la institución, con adecuado ingreso de la información en la plataforma.	Diaria	Yudy Vanessa Cuellar D.
Respaldo de la información	Realizar actualización de los datos de estudiantes y docentes que permita tener una base de datos actualizada.	Diaria	Darwin Rivera
Custodia y clasificación de la documentación	Responder por el manejo de la correspondencia interna y externa, papelería y archivo de institución.	Diaria	Darwin Rivera

Tabla 4. Procesos en Áreas Atención Público.
Fuente: El Autor

Una vez fueron detectados los procesos relevantes derivados de la actividad de atención al público, se relaciona el tipo de sistema que involucra el proceso, los cuales se clasifican según el nivel de criticidad de acuerdo a la siguiente tabla:

- **Rangos de Criticidad:**

El área no puede funcionar sin el sistema.

El área puede funcionar parcialmente sin el sistema.

El área puede funcionar sin el sistema.

- ✓ **Rango de Criticidad Lógicos**

NOMBRE DEL SISTEMA	DESCRIPCIÓN	CRITICIDAD	TIPO DE SISTEMA	NÚMERO DE EQUIPOS CON LA APLICACIÓN

BASE DE DATOS	La aplicación está desarrollada en un motor de base de datos Oracle.	1	Cliente	2
SOFTWARE	Aplicación Urpanet	1	Cliente	2

Tabla 5. Rango de Criticidad Lógicos
Fuente: el Autor

7.1.3. Recursos Asociados al Proceso

- ✓ **Recursos de Hardware asociados al proceso**

TIPO DE HARDWARE	CONFIGURACIÓN	MARCA	CRITICIDAD	UBICACIÓN
Computador portátil	Procesador Intel i3, Memoria RAM 2GB, Windows 8.1pro	HP	1	Atención al cliente
	Procesador Intel i3, Memoria RAM 2GB, Windows 8.1pro	HP	1	

Tabla 6. Recursos asociados a proceso.
Fuente: el Autor

- ✓ **Otros activos ubicados en el área**

DESCRIPCIÓN	TIPO	CRITICIDAD	LOCALIZACIÓN
Aire acondicionado	Split	1	Atención al cliente

Tabla 7. Otros Activos
Fuente: el Autor

De igual manera, la institución realiza la clasificación de sus activos de información, teniendo en cuenta el tipo de activo manejado y la clase del mismo:

- ✓ **Clasificación de Activos**

TIPO DE ACTIVO	DESCRIPCIÓN
[D] Datos / Información	Documentos en medios físicos como: Ficheros, copia de respaldo, datos de configuración, datos de gestión interna, datos de validación de credenciales, código fuente, ejecutables y datos de pruebas.
[S] Servicios Internos	Conectividad a internet, Almacenamiento de ficheros, Intercambios electrónicos de datos, acceso remoto a cuentas locales, servicios de directorios.
[SW] Software / Aplicaciones	Sistemas de información, programas, aplicativos, sistemas de gestión de base de datos, sistemas operativos, aplicaciones de servidores.
[HW] Equipos informáticos(hardware)	equipos de oficinas como: computadores, portátiles, equipamiento de respaldo, soporte de la red, concentradores, conmutadores, firewall, punto de acceso inalámbricos etc.
[COM] Comunicaciones	Dispositivos de conectividad, instalaciones de puntos de red, los servicios de comunicación contratados con terceros, router etc.
[AUX] Equipamiento Auxiliar	Equipos que soportan los sistemas, fuentes de alimentación, cableado, armarios, equipos de climatización etc.
[L] Instalaciones	Lugar donde se tiene los sistemas de información y comunicación, cuartos, edificios, instalaciones de respaldo etc.
[P] Personal	Es el recurso humano que tiene relación con los sistemas de información, como personal interno y externo, operadores, administrador de sistema, desarrolladores, contratistas etc.

Tabla 8. Clasificación de Activos
Fuente: el Autor

7.2. Análisis de las amenazas y vulnerabilidades y establecer controles para del centro educativo de sistemas UPARSISTEM.

A partir de la anterior información, se realiza la valoración de los activos de la institución en atención a la norma ISO 27001:2013, según la cual los activos de información deben ser estimados teniendo en cuenta la disponibilidad, confidencialidad e integridad, obedeciendo al impacto generado por el mismo, de acuerdo con la siguiente tabla:

- ✓ **Clasificación estimada**

CALIFICACIÓN: INTEGRIDAD, CONFIDENCIALIDAD, DISPONIBILIDAD	CLASIFICACIÓN
1	Muy bajo
2	Bajo
3	Medio
4	Alto
5	Muy alto

Tabla 9. Clasificación Estimada.
Fuente: el Autor

Una vez identificada los hallazgos en la institución y evaluados los diferentes activos, se procede a clasificar los mismos según la triada del CÍA:

- ❖ **Escala Cuantitativa y Cualitativa Confidencialidad:**

ESCALA CUANTITATIVA	ESCALA CUALITATIVA	DESCRIPCIÓN
1	Muy bajo	Cualquier usuario del común puede acceder.
2	Bajo	Sólo pueden acceder los empleados de la institución.
3	Medio	Sólo pueden acceder ciertos roles del aplicativo.
4	Alto	Sólo pueden acceder empleados autorizados y con controles de acceso.

5	Muy alto	Sólo pueden acceder funcionarios de alto mando en la institución.

Tabla 10. Escala Cuantitativa y Cualitativa Confidencialidad.
Fuente: el Autor

- **Escala Cuantitativa y Cualitativa de la Integridad:**

ESCALA CUANTITATIVA	ESCALA CUALITATIVA	DESCRIPCIÓN
1	Muy bajo	Cualquier usuario del común puede modificar la información.
2	Bajo	Sólo pueden modificar la información los empleados de la institución
3	Medio	Sólo pueden los usuarios con ciertos roles del aplicativo pueden modificar la información.
4	Alto	Sólo pueden modificar la información empleados autorizados y con controles de acceso
5	Muy alto	Sólo pueden realizar modificaciones funcionarios de alto mando en la institución.

Tabla 11. Escala Cuantitativa y Cualitativa Integridad.
Fuente: el Autor

- **Escala Cuantitativa y Cualitativa Disponibilidad:**

ESCALA CUANTITATIVA	ESCALA CUALITATIVA	DESCRIPCIÓN
1	Muy bajo	El activo está fuera de servicio por una semana y no afecta las actividades de la institución.
2	Bajo	El activo está fuera de servicio por tres días y no afecta las actividades de la institución.
3	Medio	El activo está fuera de servicio por un día y no afecta las actividades de la institución.
4	Alto	El activo está fuera de servicio hasta por 6 horas consecutivas.
5	Muy alto	El activo está disponible siempre.

Tabla 12. Escala Cuantitativa y Cualitativa Disponibilidad.
Fuente: el Autor

De esta manera se realizará la valoración de cada activo, de acuerdo a los términos de Confidencialidad, Integridad y Disponibilidad, el valor del activo de información está dado por:

[D] Disponibilidad.

[I] Integridad de los Datos.

[C] Confidencialidad de la Información.

[A] Autenticidad

[T] Trazabilidad.

- ✓ **Valoración Según Rango y Criterio**

CLASIFICACIÓN DEL VALOR DEL ACTIVO CLASIFICACIÓN VALOR DEL ACTIVO	RANGO SEGÚN VALOR DEL ACTIVO Criterio		
Muy Alto	MA	10	Daño Muy grave
Alto	A	8-9	Daño grave
Medio	M	5-7	Daño Importante
Bajo	B	2-4	Daño Menor
Muy Bajo	MB	0-1	Irrelevante a efecto práctico.

Tabla 13. Valoración Según Rango y Criterio.
Fuente: Magerit v3 Libro 2 - Catalogo de elementos

7.2.1. Valoración de los Activos

Con la metodología Magerit, permite realizar una valoración de cada uno de los activos de acuerdo a la tabla No. 2 Inventarios de activos. Esto con el fin de valorar la consecuencia de la materialización de una amenaza, de aquí la valoración que recibe un activo en una cierta dimensión esta se contempla como la medida del perjuicio para la institución si este va a dañar en cierta dimensión.

- ✓ **Valoración de Activos Tipo: Aplicaciones[SW]**

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]

Gestión de Matrículas [SIMAT_UPAR]	[MA]	[MA]	[M]	[A]	[A]
Sistema Gestión Docentes [SIGDOC_UPAR]	[MA]	[MA]	[M]	[A]	[A]
Sistema Gestión Notas [SGNTA_UPAR]	[MA]	[MA]	[M]	[A]	[A]
Sistema URPANET [URPANET_UPAR]	[MA]	[MA]	[M]	[A]	[A]
Portal Web [WEB_UPAR]	[M]	[A]			
Herramientas Ofimáticas [OFIMATICAS_UPAR]	[MA]	[A]			
Antivirus [ANTV_UPAR]	[A]				
Navegadores WEB [NAV_UPAR]	[A]	[A]			
Sistemas Operativos [SO_UPAR]	[MA]	[A]			

Tabla 14. Valoración de Activo Tipo Aplicaciones
Fuente: el Autor

- ✓ **Valoración de Activos Tipo: Servicios Internos[IS]**

Activo	**Dimensiones de Seguridad**				
	[D]	**[I]**	**[D]**	**[A]**	**[D]**
Internet [INTERNET_UPAR]	[A]	[A]			
Servidor WEB [SWEB_UPAR]		[MA]	[A]		
Servidor Telefonía IP [TI_UPAR]	[B]	[B]			
Servidor Base de Datos [SDB_UPAR]	[MA]	[MA]		[MA]	[A]

Tabla 15. Valoración de Activos Tipo Servicios Internos
Fuente: el Autor

- ✓ **Valoración de Activos Tipo: Equipos[HW]**

Activo	**Dimensiones de Seguridad**				
	[D]	**[I]**	**[C]**	**[A]**	**[T]**
Equipos de Cómputo [PC_UPAR]	[M]	[M]	[MA]	[M]	
Tablet [TABLET_UPAR]	[M]	[M]	[M]	[M]	
Cámaras de Seguridad [CAM_UPAR]	[B]				
Enrutadores [ENR_UPAR]	[MA]	[A]			

Swicth [SWICTH_UPAR]	[M]	[M]	[MA]	[M]	
Impresoras [IMP_UPAR]	[B]	[B]			
Escáner [ESC_UPAR]	[B]	[B]			
UPS [UPS_UPAR]	[M]				
Discos de Estado Solido [SSD_UPAR]	[MA]	[M]	[MA]	[M]	
VideoBeam [BEAM_UPAR]	[B]	[B]			

Tabla 16. Valoración de Activos Tipo: Equipos
Fuente: el Autor

- ✓ **Valoración de Activos Tipo: Comunicaciones[COM]**

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
Central Telefónica [CENTEL_UPAR]	[B]	[D]			
Red LAN [LAN_UPAR]	[A]	[M]			[M]
Red WIFI [WIFI_UPAR]	[A]	[M]			[M]

Tabla 17. Valoración de Activos Tipo: Comunicaciones
Fuente: el Autor

- ✓ **Valoración de Activos Tipo: Soportes de Información[SOPORINF]**

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
Backup SIMAT [BKSIMAT_UPAR]	[MA]	[A]	[MA]	[MA]	[A]
Backup SIGDOC [BKSIGDOC _UPAR]	[MA]	[A]	[MA]	[MA]	[A]
Backup SGNTA [BKSGNTA _UPAR]	[MA]	[A]	[MA]	[MA]	[A]
Backup URPANET [BKURPANET _UPAR]	[MA]	[A]	[MA]	[MA]	[A]

Tabla 18. Valoración de Activos Tipo: Soportes de Información
Fuente: el Autor

- ✓ **Valoración de Activos Tipo: Equipos Auxiliares [AUX]**

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
Cableado de RED [CABRED_UPAR]	[M]	[A]	[A]		
Cableado Electico [CABELE_UPAR]	[B]		[B]		

Caja de Herramientas [HERR_UPAR]	[B]	[B]			
Aires Acondicionados [AACON_UPAR]	[B]	[B]			

Tabla 19. Valoración de Activos Tipo. Equipos Auxiliares
Fuente: el Autor

- ✓ **Valoración de Activos Tipo: Instalaciones [L]**

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
Gabinete de Red [GAB]	[B]	[B]			

Tabla 20. Valoración de Activos Tipo: Instalaciones
Fuente: el Autor

- ✓ **Valoración de Activos Tipo: Personal [P]**

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
Director General [DIRGR_UPAR]	[A]		[MA]		[A]
Gerente [GER_UPAR]	[MA]	[A]	[A]	[MA]	[A]
Ingeniero Desarrollo Software [INGD_UPAR]	[MA]	[A]	[A]	[A]	[A]
Coordinador de Relaciones [COORD_UPAR]	[A]		[MA]		[A]
Coordinador de Calidad [COORDR_UPAR]	[A]		[MA]		[A]
Auditor de Calidad [AUDC_UPAR]	[MA]	[MA]	[MA]	[A]	[A]
Asesor Jurídico [ASRJ_UPAR]	[A]		[A]		[A]
Asesor de Calidad [ASRC_UPAR]	[A]	[A]	[A]	[A]	
Asesor Académico [ASRA_UPAR]	[A]	[A]	[A]		
Asistente Atención al Cliente [ASIS_UPAR]	[A]	[A]	[A]		[A]
Coordinador Académico [COORA_UPAR]	[A]		[MA]		[A]
Docentes [DOC_UPAR]	[A]	[A]	[A]		[A]
Asistente Académico [ASISAC_UPAR]	[A]	[A]	[A]		[A]
Secretario Académico [SCRA_UPAR]	[A]	[A]	[A]		[A]

Director Administrativo y Financiero [DIRAD_UPAR]	[A]		[MA]		[A]
Asistente Talento Humano [ASIST_UPAR]	[A]	[A]	[A]		[A]
Contador [CONT_UPAR]	[A]		[MA]		[A]
Asistente Contable [ASISCON_UPAR]	[A]	[A]	[A]		[A]
Asistente Soporte [ASISP_UPAR]	[A]	[A]	[A]		[A]
Asistente Alancen e Inventario [ASISAL_UPAR]	[A]		[MA]		[A]
Tesorero [TESO_UPAR]	[A]	[A]	[A]		[A]
Coordinador Recursos Físicos y Tics [COORFIS_UPAR]	[A]	[MA]	[MA]		[A]
Asistente Servicios Generales [SERGR_UPAR]	[A]	[A]	[A]		[A]

Tabla 21. Valoración de Activos Tipo: Personal
Fuente: el Autor

7.2.2. *Caracterización de las Amenazas*

Para la caracterización de las amenazas su objetivo es determinar la degradación de cada activo; esto consiste en evaluar el valor que pierde el activo, en el caso que se materialice una amenaza. Estas amenazas se han tomado de la metodología MAGERIT 3.0

[N] Desastres Naturales

[I] De origen Industrial

[E] Errores o fallos no intencionados

[A] Ataques intencionados.

La metodología MAGERIT sugiere que se realicen dos tareas muy importantes que son:

a) Identificar las Amenazas
b) Valorar las Amenazas

- ✓ **Frecuencia de Amenazas**

Valor			Criterio
4	Muy Frecuente	MF	A diario
3	Frecuente	F	Mensualmente
2	Frecuencia Normal	FN	Una vez a año
1	Poco Frecuente	PF	Cada Varios años

Tabla 22. Valor frecuencia de amenazas.
Fuente: Magerit v3 Libro 2 - Catalogo de elementos

- ✓ **Degradación de la Amenazas**

Valor	Criterio	
100%	MA	Degradación muy Alta del Activo
80%	A	Degradación Alta considerable del Activo
50%	M	Degradación Media del Activo
10%	B	Degradación Baja del Activo
1%	MB	Degradación muy Baja del Activo

Tabla 23. Valor degradación de amenazas
Fuente: Magerit v3 Libro 2 - Catalogo de elementos

- ✓ **Identificación y Valoración Amenazas Tipo: Aplicaciones**

Activos / Amenazas	Frecuencia	Dimensiones de Seguridad				
		D	I	C	A	T
[E.1] Errores de los usuarios	F	MA	A			
[E.2] Errores del Administrador	FN	A				
[E.4] Errores de Configuración	FN	A				
[E.14] Escapes de Información	PF			A		
[A.11] Acceso no Autorizado	FN	MA				
[A.15] Modificación deliberada de la Información	PF		MA			

Tabla 24. Valoración de Amenazas tipo: Aplicaciones
Fuente: el Autor

- ✓ **Identificación y Valoración Amenazas Tipo: Servicios Internos**

Activos / Amenazas	Frecuencia	Dimensiones de Seguridad				
		D	I	C	A	T
[E.20] Vulnerabilidades de los programas	PF	MA				

[A.5] Suplantación de la Identidad del Usuario	FN			A	A	
[A.8] Difusión de software dañino	FN	A				
[A.24] Denegación de Servicios	PF	MA				

Tabla 25. Valoración de Amenazas tipo: Servicios Internos
Fuente: el Autor

✓ Identificación y Valoración Amenazas Tipo: Equipos

Activos / Amenazas	Frecuencia	Dimensiones de Seguridad				
		D	I	C	A	T
[N.1] Fuego	PF	MA	MA	MA	MA	MA
[I.2] Daño por Agua	PF	MA	MA	MA	MA	MA
[I.5] Avería de origen físico o lógico	PF	A				
[E.23] Errores de mantenimiento/ actualización equipo (hardware)	FN	A				
[A.11] Acceso no autorizado	FN			A		
[A.23] Manipulación de los Equipos	FN			A		

Tabla 26. Valoración de Amenazas tipo: Equipos
Fuente: el autor

✓ Identificación y Valoración Amenazas Tipo: Comunicaciones

Activos / Amenazas	Frecuencia	Dimensiones de Seguridad				
		D	I	C	A	T
[N.*] Desastre Natural	PF	MA				MA
[I.5] Avería de origen físico o lógico	FN	MA				
[I.8] Fallos de servicios de Comunicaciones	PF	A				
[E.2] Errores de Administrador	PF	A		A		
[A.4] Manipulación de configuración	PF			A	A	

Tabla 27. Valoración de Amenazas tipo: Comunicaciones
Fuente: el autor

✓ Identificación y Valoración Amenazas Tipo: Soportes de Información

Activos / Amenazas	Frecuencia	Dimensiones de Seguridad				
		D	I	C	A	T
[E.1] Errores de los usuarios	F	MA	A	A		
[E.2] Errores del Administrador	FN	A		A		
[E.4] Errores de Configuración	FN	A		A		
[E.14] Escapes de Información	PF			A		
[A.15] Modificación deliberada de la información	PF		MA			

Tabla 28. Valoración de Amenazas tipo: Soportes de Información
Fuente: el autor

✓ Identificación y Valoración Amenazas Tipo: Equipos Auxiliares

Activos / Amenazas	Frecuencia	Dimensiones de Seguridad				
		D	I	C	A	T

[I.5] Avería de origen físico o lógico	PF	A				

Tabla 29. Valoración de Amenazas tipo: Equipos Auxiliares
Fuente: el autor

✓ **Identificación y Valoración Amenazas Tipo: Instalaciones**

Activos / Amenazas	Frecuencia	Dimensiones de Seguridad				
		D	I	C	A	T
[A.26] Ataque destructivo	PF	MA				

Tabla 30. Valoración de Amenazas tipo: Instalaciones
Fuente: el autor

✓ **Identificación y Valoración Amenazas Tipo: Personal**

Activos / Amenazas	Frecuencia	Dimensiones de Seguridad				
		D	I	C	A	T
[E.7] Deficiencia en la organización	FN	A				
[E.15] Alteración accidental de la información	FN	A	A			
[A.30] Ingeniería social.	PF		A			

Tabla 31. Valoración de Amenazas tipo: Personal
Fuente: el autor

7.2.3. Estado del Riesgo

Se realiza con el fin de analizar los datos recopilados en la caracterización de las amenazas y así evaluar el estado del riesgo, donde se incluye el estimado de impacto y el riesgo. Para ello se toma la siguiente escala para calificar el valor de los activos de acuerdo a su magnitud.

MA: Muy alto.
A: Alto.
M: Medio.
B: Bajo.
MB: Muy Bajo

- **Estimación del Impacto**

El objetivo de este proceso es determinar el alcance del daño que se produce sobre los activos de información en el caso de que se materialice una amenaza. Para ello se evalúa el grado de percusión que pueda presentar cada uno de los activos dentro

de las dimensiones de valoración analizadas como son: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad.

- ✓ **Valores estimado de Impacto**

IMPACTO		DEGRADACIÓN				
		1%	10%	50%	80%	100%
VALOR	MA	M	A	A	MA	MA
	A	B	M	M	A	A
	M	MB	B	B	M	M
	B	MB	MB	MB	B	B
	MB	MB	MB	MB	MB	MB

Tabla 32. Valores Estimados de Impacto
Fuente: Magerit V.3 Libro II

- ✓ **Valoración Impacto en los Activos de Información**

ACTIVOS	AMENAZAS	IMPACTO ACUMULADO					IMPACTO RESIDUAL				
		D	I	C	A	T	D	I	C	A	T
Aplicaciones	[E.1] Errores de los usuarios										
	[E.2] Errores del Administrador										
	[E.4] Errores de Configuración										
	[E.14] Escapes de Información										
	[A.11] Acceso no Autorizado										
	[A.15] Modificación deliberada de la Información										
Servicios Internos	[E.20] Vulnerabilidades de los programas										
	[A.5] Suplantación de la Identidad del Usuario										
	[A.8] Difusión de software dañino										
	[A.24] Denegación de Servicios										
Equipos	[N.1] Fuego										
	[I.2] Daño por Agua										
	[I.5] Avería de origen físico o lógico										
	[E.23] Errores de mantenimiento/										

	actualización equipo (hardware)												
	[A.11] Acceso no autorizado												
	[A.23] Manipulación de los Equipos												
Comunicaciones	[N.*] Desastre Natural												
	[I.5] Avería de origen físico o lógico												
	[I.8] Fallos de servicios de Comunicaciones												
	[E.2] Errores de Administrador												
	[A.4] Manipulación de configuración												
Soportes de Información	[E.1] Errores de los usuarios												
	[E.2] Errores del Administrador												
	[E.4] Errores de Configuración												
	[E.14] Escapes de Información												
	[A.15] Modificación deliberada de la información												
Equipos Auxiliares	[I.5] Avería de origen físico o lógico												
Instalaciones	[A.26] Ataque destructivo												
Personal	[E.7] Deficiencia en la organización												
	[E.15] Alteración accidental de la información												
	[A.30] Ingeniería social.												

Tabla 33. Valoración Impacto en los Activos
Fuente: el Autor

- **Estimación de los Riesgos**

Para realizar la estimación de los riesgos de hace unos de la siguiente escala cualitativa tomando como entradas impacto acumulado y frecuencia.

✓ **Valor de Frecuencia**

VALOR			CRITERIO
100	Muy Frecuente	MF	A Diario

10	Frecuente	F	Mensualmente
1	Normal	FN	Una vez al Año
1/10	Poco Frecuente	PF	Cada Varios Años

Tabla *34.* Valor de Frecuencia
Fuente: el autor

- ✓ **Criterios de Valoración para estimado de Riesgos**

RIESGO		FRECUENCIA			
		PF	FN	F	MF
Impacto	MA	M	A	MA	MA
	A	B	A	MA	MA
	M	B	M	A	A
	B	MB	B	M	A
	MB	MB	MB	B	B

Tabla 35. Criterios Valoración para estimado de Riesgos
Fuente: el autor

La estimación del riesgo es tomado de los valores de la frecuencia de ocurrencia de cada una de las amenazas, frente a los activos e impactos acumulados ya que estos deben de tener una acción de forma urgente.

- ✓ **Valoración de Riesgos en activos**

ACTIVOS	AMENAZAS	IMPACTO					FRECUENCIA	RIESGO
		D	I	C	A	T		
Aplicaciones	[E.1] Errores de los usuarios						F	
	[E.2] Errores del Administrador						FN	
	[E.4] Errores de Configuración						FN	
	[E.14] Escapes de Información						PF	
	[A.11] Acceso no Autorizado						FN	
	[A.15] Modificación deliberada de la Información						PF	
Servicios Internos	[E.20] Vulnerabilidades de los programas						PF	
	[A.5] Suplantación de la Identidad del Usuario						FN	
	[A.8] Difusión de software dañino						FN	

	[A.24] Denegación de Servicios						**PF**	
Equipos	[N.1] Fuego						**PF**	
	[I.2] Daño por Agua						**PF**	
	[I.5] Avería de origen físico o lógico						**PF**	
	[E.23] Errores de mantenimiento/ actualización equipo (hardware)						**FN**	
	[A.11] Acceso no autorizado						**FN**	
	[A.23] Manipulación de los Equipos						**PF**	
Comunicaciones	[N.*] Desastre Natural						**PF**	
	[I.5] Avería de origen físico o lógico						**PF**	
	[I.8] Fallos de servicios de Comunicaciones						**PF**	
	[E.2] Errores de Administrador						**PF**	
	[A.4] Manipulación de configuración						**PF**	
Soportes de Información	[E.1] Errores de los usuarios						**F**	
	[E.2] Errores del Administrador						**FN**	
	[E.4] Errores de Configuración						**FN**	
	[E.14] Escapes de Información						**PF**	
	[A.15] Modificación deliberada de la información						**FN**	
Equipos Auxiliares	[I.5] Avería de origen físico o lógico						**PF**	
Instalaciones	[A.26] Ataque destructivo						**PF**	
Personal	[E.7] Deficiencia en la organización						**FN**	
	[E.15] Alteración accidental de la información						**FN**	
	[A.30] Ingeniería social.						**PF**	

Tabla 36. Valoración de Riesgos en los activos
Fuente: el autor

8. CONTROLES

Los controles son aplicados de acuerdo a los resultados obtenidos en la tabla sobre la estimación de riesgos teniendo en cuenta las necesidades y características de cada activo.

8.1. Medidas de seguridad para preservar los activos informáticos del centro educativo de sistemas UPARSISTEM, con base a la confidencialidad, integridad y disponibilidad.

A continuación se describe la revisión del cumplimiento de los controles en el anexo A de la norma ISO 27001:2013.

- ✓ **Cumplimiento Controles Norma ISO 27001:2013 Anexo A.**

CENTRO EDUCATIVO DE SISTEMAS UPARSISTEM NORMA ISO 27001 ANEXO A
DOMINIOS Y CONTROLES
DOMINIO 5. POLÍTICA DE SEGURIDAD INFORMÁTICA
De acuerdo a la verificación de los Documentos internos de la Institución No se evidencia La Política de Seguridad de la Información en la Institución.
DOMINIO 6. ORGANIZACIÓN DE LA INFORMACIÓN.
6.1 Organización Interna
En la Institución se evidencia que cada funcionario conoce y tiene asignado una serie de funciones objeto de la descripción de sus cargos, pero revisando el Manuel de procesos estos no están Documentados.
6.2 Dispositivos Móviles y Teletrabajo
En las visitas y entrevistas realizadas en la institución se evidencia que los funcionarios y terceros no cuentan con una política de seguridad de la Información.
DOMINIO 7. SEGURIDAD DEL RECURSO HUMANO
7.1 Antes de Asumir el Empleo
En La Institución tiene implementado y documentado el procedimiento de Gestión del Personal el cual cumple con todos los requisitos legales vigentes.
7.2 Durante el empleo
En la duración del tiempo laborado no se evidencia que exista una capacitación sobre seguridad de la información.
7.3 Terminación y cambio de Empleo
En La Institución tiene implementado y documentado el procedimiento de Gestión del Personal el cual cumple con todos los requisitos legales vigentes.
DOMINIO 8. GESTIÓN DE ACTIVOS
8.1 Responsabilidad por los Activos
En La Institución tiene implementado formato para la gestión de inventarios de los activos, pero este a la fecha no está documentado
8.2 Clasificación de la Información
En La Institución enumera la información y la clasifica en Restringida, Confidencial, Pública y Interna.
8.3 Manejo de Medios
En la verificación de los Documentos la Institución no cuenta con un procedimiento de manejos de medios, y la trasferencia de medios físicos no se encuentra controlados.
DOMINIO 9. CONTROL DE ACCESO

9.1 Requisitos del Negocio para el control de acceso
De acuerdo a la verificación de los Documentos internos de la Institución No se evidencia La Política de Seguridad de la Información en la Institución.
9.2 Gestión de acceso de Usuarios
La institución actualmente cuenta con la creación de usuarios, con directorio activo para la gestión de los privilegios en la red de datos y el proxy de navegación. Hay algunos puntos muy importantes para trabajar, como lo es la verificación de derechos de acceso, equipos desentendidos, y diseñar el procedimiento de escritorio limpio.
9.3 Responsabilidades de los usuarios
En la Institución cada usuario conoce sus responsabilidades las cuales hacen parte de la descripción del perfil de su cargo, pero este No está documentado, en el procedimiento de gestión del personal, para así definir las responsabilidades y controles en materia de seguridad de la información.
9.4 Control de acceso a sistemas y aplicaciones
La Institución cuenta con la creación de acceso a los sistemas de información y aplicaciones, así como la asignación de los privilegios.
DOMINIO 10. CRIPTOGRAFÍA
10.1 Controles Criptográficos
La Institución No cuenta con un sistema de Cifrado / Encryption para la conservación de los datos en su formato mediante sistema autenticación de Cifrado seguro.
DOMINIO 11. SEGURIDAD FÍSICA Y DEL ENTORNO
11.1 Áreas Seguras
La institución actualmente cuenta con controles de acceso físicos.
11.2 Equipos
La institución cuenta con controles para la realización de mantenimiento de equipos de cómputo, cuenta con cableado estructurado, y controles de ingreso y salida de equipos.
DOMINIO 12. SEGURIDAD DE LAS OPERACIONES
12.1 Procedimientos operacionales y responsabilidades
La institución cuenta con procedimientos operacionales, estos se encuentran documentados con la asignación de responsables.
12.2 Protección contra códigos maliciosos
Uparsistem cuenta con instalación de antivirus en todos los equipos de cómputo, y control de acceso lógicos mediante firewall.
12.3 Copias de Respaldo
La institución realiza copia de respaldo de todas las bases de datos. Estudiantes, clientes, nomina, contables, periódicamente (Mensual)
12.4 Registro y monitoreo
La institución en la actualidad no realiza monitorio de las bases de datos.
12.5 Control de Software Operacional
La institución cuanta con el bloqueo de instalación de software.
12.6 Gestión de la Vulnerabilidad Técnica
La Institución no cuenta con manuales para la gestión de incidentes de seguridad, no tiene implementado el monitoreo, atención y seguimiento a los mismo.
12.7 Consideraciones sobre auditorias de sistemas de Información
La institución no cuenta con la gestión de auditoria de los sistemas de información.
DOMINIO 13. SEGURIDAD DE LAS COMUNICACIONES
13.1 Gestión de la seguridad de las redes
La institución actualmente cuenta con controles en la gestión de la seguridad de las redes, firewall.
13.2 Transferencia de Información
La Institución No cuenta con la implementación del manual de transferencia de información.
DOMINIO 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
14.1 Requisitos de Seguridad de los Sistemas de Información
La institución en la adquisición de desarrollo de software cuenta con controles de seguridad.

14.2 Seguridad de los procesos de desarrollo y soporte
14.3 Datos de Prueba
Las pruebas se realizan con datos de producción para la validación de sistemas de información.
DOMINIO 15. RELACIÓN CON LOS PROVEEDORES
15.1 Seguridad de la Información en la relación con los proveedores
La Institución No cuenta con acuerdos de confidencialidad de la información.
15.2 Gestión de la prestación de servicios de proveedores
La Institución No cuenta con acuerdos de confidencialidad de la información.
DOMINIO 16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
16.1 Gestión de incidentes y mejoras en la seguridad de la Información
La Institución no cuenta con manuales para la gestión de incidentes de seguridad, no tiene implementado el monitoreo, atención y seguimiento a los mismo.
DOMINIO 17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
17.1 Continuidad de Seguridad de la Información
La Institución No cuenta con una política de continuidad del negocio, con el fin de mantener en operación los procesos más críticos.
17.2 Redundancias
La Institución no cuenta redundancia en el firewall, proxy, UPS, canales.
DOMINIO 18. CUMPLIMIENTO
18.1 Cumplimiento de requisitos legales y contractuales
18.2 Revisiones de Seguridad de la Información

Tabla 37: Cumplimiento Controles Norma ISO 27001:2013 Anexo A.
Fuente: el Autor

8.2. Plan de Tratamiento de Riesgos.

Con base a las visitas realizadas en la institución, y entrevistas con los diferentes funcionarios que conocen los procesos así como el análisis de la información en sus áreas de trabajo, se han identificado oportunidades para la mejora de acuerdo al análisis de riesgos, que conducen a proponer el siguiente plan de tratamiento de riesgos, con el fin de enriquecer el Sistema de Gestión de Seguridad de la Información SGSI:

- ✓ **Plan Tratamiento Riesgo**

N	Plan de Tratamiento	Afecta			Control	Descripción Plan de Acción	Responsable	Fecha
		D	I	C				
1	Medidas preventivas para reducir riegos	X	X	X	Gestión de Incidentes de	Definir, documentar e implementar una política de gestión de incidentes de	Dirección de las Tics	05 de Junio 2017

					Seguridad de la Información	seguridad al interior de la institución.		
2	Reducir el Riesgo		X		Criptografía	Implementar mecanismos que garanticen el cifrado de la información que es intercambiada con terceros a través de correos electrónicos	Dirección de la Tics	30 de Mayo 2017
3.	Medidas preventivas para reducir riegos			X	Control de Acceso	Revisar periódicamente en estado de los usuarios, roles y permisos en los sistemas de información.	Dirección de la Tics	30 de Mayo 2017
4	Medidas preventivas para reducir riegos			X	Control de Acceso	Implementar el bloqueo de los dispositivos externos en los equipos de cómputo en la institución	Dirección de la Tics	30 de Mayo 2017
5	Disminuir el Riesgo		X	X	Control de Acceso	Garantizar que la policita de contraseña segura y bloqueo automática este implementada	Dirección de la Tics	30 de Mayo 2017
6	Disminuir el Riesgo		X		Seguridad Física y del Entorno	Reforzar los controles para la salida de equipos de cómputo de la institución	Dirección de la Tics	30 de Mayo 2017
7	Medidas preventivas para reducir riegos			X	Seguridad de Recursos Humanos	Implementar acuerdos de confidencialidad de la información en los contratos de trabajo de los empleados de la institución.	Dirección Talento Humano	30 de Mayo 2017
8	Medidas preventivas para reducir riegos			X	Seguridad de las Operaciones	Implementar y definir política de protección y privacidad de la información personal.	Dirección de la Tics	05 de Junio 2017
9	Medidas preventivas para reducir riegos	X	X		Gestión de la Continuidad del Negocio	Fijar e implementar política de continuidad del negocio en la institución.	Dirección General	19 de Junio 2017
10	Disminuir el Riesgo		X		Seguridad de Recursos Humanos	Mejorar el procedimiento de gestión del personal en la institución.	Dirección Talento Humano	30 de Mayo 2017
11	Medidas preventivas	X	X		Organización de la Seguridad	Implementar y definir manuales para los dispositivos móviles.	Dirección de la Tics	30 de Mayo 2017

	para reducir riegos				de la Información			

Tabla 38: Plan de Tratamiento de los Riesgos
Fuente: el Autor

9. PROPUESTA POLÍTICA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN SGSI PARA LA INSTITUCIÓN.

En esta fase del proyecto se da inicio para realizar la propuesta para implementar el Sistema de Gestión de Seguridad Informática para la institución acorde a sus necesidades, con la creación de una policita de seguridad de la información.

9.1. Políticas de seguridad informática recomendad para la institución.

Se elaboró la política de seguridad de la información el cual corresponde al documento que contiene las normas y lineamientos que rigen la seguridad de la información en la institución, responsabilidades y obligaciones de todos los empleados y contratistas que tengan acceso a la información de la institución **(Ver Anexo 4)**.

9.1.1. Observaciones Acordes Estándar ISO 27002.

LR. Requerimiento Legal, **CO.** Obligación Contractual, **BR/BP.** Requerimiento de Negocio/Mejores prácticas, **RRA:** resultado de evaluación de riesgo. **(Ver Tabla 39. Observaciones Acorde Estándar ISO 27002.)**

9.2. Estado Final Cumplimiento Norma ISO 27001:2013.

Estado de madurez final (General y por dominio) de los controles de seguridad de la información en la institución según ISO/IEC 27001:2013 previa implementación del SGSI.

Figura 16: Estado Final Cumplimiento Norma ISO 27001:2013
Fuente: el Autor

9.3. Capacitación sobre el sistema de gestión de seguridad de la información (SGSI), a toda la institución, de Uparsistem.

Se realizó una visita en las instalaciones de la institución con la alta gerencia para coordinar los permisos necesarios, y así presentar la policita de gestión de seguridad de la Información leerla a todos los empleados de la misma., logrando así una alta asistencia de los funcionarios. **(Ver Anexo 3. Listado de Asistencia Capacitación**). Adjunto unas imágenes del personal en el auditorio.

Observaciones Acorde al Estándar ISO 27002.

ISO/IEC 27001:2013 Anexo A. Controles			Razones para la selección del Control				
Clausula	**Sec**	**Objetivo de Control**	**LR**	**CO**	**BR/ BP**	**RRA**	**Observaciones**
5 Políticas de Seguridad	**5.1**	**Dirección de gestión para la seguridad de la información**					
	5.1.1	Políticas para la seguridad de la información			**X**	**X**	La Gerencia debe aprobar el documento de la política, una vez realizado esta se debe publicar y comunicar a todos los empleados de la institución.
	5.1.2	Revisión de las políticas para la seguridad de la información				**X**	La política de seguridad de la información debe ser revisada regularmente, y a su vez documentada para asegurar su continuidad.
Clausula	**Sec**	**Objetivo de Control**	**LR**	**CO**	**BR/ BP**	**RRA**	**Observaciones**
6 Organización de la Seguridad de la Información	**6.1**	**Organización Interna**					
	6.1.1	Roles y responsabilidades para la seguridad de la Información			**X**		Se deben definir los roles y responsabilidades de la seguridad de la información dentro de la institución.
	6.1.2	Separación de Deberes			**X**		Definir los deberes de la seguridad de la información de los funcionarios en la institución.
	6.1.3	Contacto con las Autoridades				**X**	Incluir el contacto con las autoridades para el procedimiento de gestión de incidentes.
	6.1.4	Contacto con grupos de interés especial			**X**		Contar con el contacto de grupos especiales como, Grupos investigación.
	6.1.5	Seguridad de la Información en la gestión de proyectos			**X**	**X**	Fijar políticas, procedimiento, manuales en los proyectos que se implementen en la institución en seguridad de la información.
	6.2	**Dispositivos Móviles y Teletrabajo**					
	6.2.1	Política para Dispositivos Móviles			**X**		Implementar políticas de acceso seguro a dispositivos móviles.
	6.2.2	Teletrabajo			**X**		Si es viable contemplar el teletrabajo, es de vital importancia establecer políticas de

							acceso remoto a los servidores de la institución y/o aplicaciones, por intermedio de canales seguros como. Ejemplo (VNP).
Clausula	**Sec**	**Objetivo de Control**	**LR**	**CO**	**BR/ BP**	**RRA**	**Observaciones**
7 Seguridad del Recurso Humano	**7.1**	**Antes de Asumir el Empleo**					
	7.1.1	Selección		**X**	**X**		Control implementado, con oportunidad de mejoras.
	7.1.2	Términos y condiciones del empleo	**X**	**X**			Control implementado, con oportunidad de mejoras.
	7.2	**Durante el empleo**					
	7.2.1	Responsabilidades de la Dirección			**X**	**X**	Introducir como otro si al contrato de trabajo, la aceptación de los empleados y/o contratistas en cumplimiento de la política de seguridad de la información.
	7.2.2	Toma de conciencia, educación y formación en Seguridad			**X**	**X**	Fijar un proyecto de capacitación a los empleados y/o contratistas en la toma de decisiones en seguridad de la información, y sensibilizar al interior de la organización sobre el SGSI.
	7.2.3	Proceso Disciplinario			**X**	**X**	Incluir en un documento Procedimiento Procesos Disciplinarios al incumplimiento de normas, manuales, procedimiento y política de seguridad de la información en la institución.
	7.3	**Terminación y cambio de Empleo**					
	7.3.1	Terminación o cambio de responsabilidades de Empleo			**X**	**X**	Definir un Procedimiento en la Gestión del Personal, en el cual se indique que actividades realizar al momento de la terminación laboral o cambio del contrato de trabajo al interior de la institución.
Clausula	**Sec**	**Objetivo de Control**	**LR**	**CO**	**BR/ BP**	**RRA**	**Observaciones**
8 Gestión de Activos	**8.1**	**Responsabilidad por los Activos**					
	8.1.1	Inventario de Activos			**X**	**X**	Se debe de elaborar un procedimiento para la conservación y actualización del inventario de activos de la institución.
	8.1.2	Propiedad de los Activos		**X**			Control implementado, con oportunidad de mejoras.

	8.1.3	Uso aceptable de los activos				X	Aplicar una policita de uso aceptable de los activos, aprobarla y divulgarla entre los empleados y contratistas de la institución.
	8.1.4	Devolución de Activos				X	Validar que el control este aplicado en la institución, por medio de los procesos comprometidos.
	8.2	**Clasificación de la Información**					
	8.2.1	Clasificación de la Información			X		No hay un instructivo formal donde se defina la clasificación de la información en la institución.
	8.2.2	Etiquetado de la Información			X	X	Toda la documentación de la institución debe de contar con etiquetado de la información de acuerdo a sus niveles de clasificación aplicados en la institución.
	8.2.3	Manejo de Activos			X	X	Este control debe estar contenido en el procedimiento de clasificación de la información, y depende de su nivel y clasificación.
	8.3	**Manejo de Medios**					
	8.3.1	Gestión de medios removibles				X	Fijar procedimiento para compra y manejo de medios removibles en la institución.
	8.3.2	Disposición de Medios				X	Aplicar medidas en la institución para la disposición de medios.
	8.3.3	Transferencia de medios físicos					Fijar procedimiento para la trasferencia de información en medios físicos en la institución.
Clausula	**Sec**	**Objetivo de Control**	**LR**	**CO**	**BR/ BP**	**RRA**	**Observaciones**
9 Control de Acceso	**9.1**	**Requisitos del Negocio para el control de acceso**					
	9.1.1	Política del Control de Acceso			X		Realizar aprobación de la policita de seguridad de la información al interior de la institución.
	9.1.2	Acceso a redes y servicios de red			X		
	9.2	**Gestión de acceso de Usuarios**					
	9.2.1	Registro y cancelación de acceso de usuarios				X	Aplicar Procedimientos de crear y anular usuarios, para tener el control de los mismos en el acceso a las aplicaciones de la institución.
	9.2.2	Suministro de acceso de usuarios				X	Con la aplicación del procedimiento de crear y anular usuarios es de vital

							importancia definir los diferentes niveles de acceso y privilegios asignados a los usuarios en los sistemas de información
	9.2.3	Gestión de Derechos de acceso privilegiado				**X**	Definir los diferentes niveles de acceso y privilegios asignados a los usuarios en los sistemas de información.
	9.2.4	Gestión de la Información secreta de autenticación de los usuarios				**X**	Dentro del mismo procedimiento de crear y anular usuarios, definir los lineamientos para la asignación de nombres de usuarios y establecer estructuras para contraseñas seguras a los usuarios para el acceso a los sistemas de información de la institución.
	9.2.5	Revisión de los derechos de acceso de los usuarios				**X**	La anulación de los derechos de accesos se deben realizar de acuerdo al procedimiento de gestión del personal, así es de suma importancia mencionar en el documento la frecuencia de revisión de privilegios de los sistemas de información.
	9.2.6	Retiro o ajuste de los derechos de los usuarios				**X**	
	9.3	**Responsabilidades de los usuarios**					
	9.3.1	Uso de información de autenticación secreta				**X**	Control implementado, con oportunidad de mejoras.
	9.4	**Control de acceso a sistemas y aplicaciones**					
	9.4.1	Restricción de acceso a la información			**X**	**X**	Con base a la asignación de los privilegios en los sistemas de información, así mismo se debe restringir el acceso a información de acuerdo al nivel de clasificación que se tenga.
	9.4.2	Procesamiento de Ingreso Seguro			**X**	**X**	Fijar un procedimiento de ingreso seguro a los equipos de cómputo de la institución.
	9.4.3	Sistema de Gestión de contraseñas			**X**	**X**	Asignar contraseñas genéricas, para que el usuario una vez se autentique realice el cambio de esta.
	9.4.4	Uso de programas utilitarios privilegiados			**X**	**X**	No es posible vigilar de forma centralizada que programa pueda o ejecutar el usuario.
	9.4.5	Control de acceso a códigos fuente de programas				**X**	Definir procedimiento para el acceso a códigos fuentes de programas en donde solo el personal autorizado, pueda acceder a ellos previa solicitud y consulta.

Clausula	Sec	Objetivo de Control/Control	LR	CO	BR/ BP	RRA	Observaciones
10 Criptografía	**10.1**	**Controles Criptográficos**					
	10.1.1	Política sobre el uso de controles criptográficos			**X**		Diseñar, documentar e implementar policitas de control criptográficos para la institución.
	10.1.2	Gestión de llaves			**X**		Definir un procedimiento para la gestión de llaves y certificados digitales de forma centralizada.
Clausula	**Sec**	**Objetivo de Control/Control**	**LR**	**CO**	**BR/ BP**	**RRA**	**Observaciones**
11 Seguridad Física y del Entorno	**11.1**	**Áreas Seguras**					
	11.1.1	Perímetro de Seguridad Física			**X**		Control implementado, con oportunidad de mejoras.
	11.1.2	Controles de acceso Físicos			**X**		Control implementado, con oportunidad de mejoras.
	11.1.3	Seguridad de oficinas, recintos e instalaciones			**X**		Control implementado, con oportunidad de mejoras.
	11.1.4	Protección contra amenazas externas y ambientales			**X**		Control implementado, con oportunidad de mejoras.
	11.1.5	Trabajo en áreas seguras			**X**		Definir áreas de trabajo seguras dentro de la institución con el control de acceso y lo mismo a equipos electrónicos sea restringido.
	11.1.6	Áreas de despacho y carga			**X**		
	11.2	**Equipos**					
	11.2.1	Ubicación y protección de los equipos			**X**		Es importante fortalecer este control con la salida de equipos y concientizar a los usuarios en la protección física del mismo. Es debido a las visitas realizadas se pudo evidenciar muchos equipos portátiles sin protección.
	11.2.2	Servicios de suministro			**X**		Control implementado, con oportunidad de mejoras.
	11.2.3	Seguridad del cableado			**X**		Control implementado, con oportunidad de mejoras.
	11.2.4	Mantenimiento de equipos			**X**		Control implementado, con oportunidad de mejoras.
	11.2.5	Retiro de activos				**X**	Fijar un procedimiento que indique el método para el retiro de activos.

	11.2.6	Seguridad de equipos y activos fuera de las instalaciones			**X**		Definir un procedimiento el cual indique los métodos de seguridad de los equipos y activos fuera de la institución.
	11.2.7	Disposición segura o reutilización de equipos			**X**		Implementar un guía en la institución para una segura reutilización de los equipos, o eliminación del mismo.
	11.2.8	Equipo de usuario desatendido			**X**		Control implementado, con oportunidad de mejoras.
	11.2.9	Pantalla de escritorio limpio y pantalla limpia				**X**	Definir una policita de escritorio limpio y pantalla limpia, en la que la información física confidencial este custodiada bajo llave.
Clausula	**Sec**	**Objetivo de Control**	**LR**	**CO**	**BR/ BP**	**RRA**	**Observaciones**
12 Seguridad de las Operaciones	**12.1**	**Procedimientos operacionales y responsabilidades**					
	12.1.1	Procedimientos de operación documentados			**X**		Control implementado, con oportunidad de mejoras.
	12.1.2	Gestión de cambios			**X**		Fijar un procedimiento de gestión de cambios.
	12.1.3	Gestión de capacidad			**X**		Ejecutar seguimiento, analizar los resultados de las mediciones realizadas. Sustentar con actas cada actividad.
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación			**X**		Fijar los ambientes de desarrollo, pruebas y operación del negocio.
	12.2	**Protección contra códigos maliciosos**					
	12.2.1	Controles contra códigos maliciosos			**X**		Ejecutar seguimiento de control contra los códigos maliciosos, manteniendo un buen antivirus. Así mismo incidentes o eventos que se presenten en el firewall.
	12.3	**Copias de Respaldo**					
	12.3.1	Respaldo de la Información			**X**		Ejecutar planes para realizar copias de respaldo de la información de forma periódica, en discos compartidos para su revisión de manera confiable.
	12.4	**Registro y monitoreo**					
	12.4.1	Registro de eventos			**X**		Definir los conductos para los reportes de eventos de seguridad que se presenten en la institución.

	12.4.2	Protección de la Información de Registro			X		Asegurar un almacenamiento seguro de la información, así como los eventos de seguridad que se presenten en la institución.
	12.4.3	Registros del administrador y del operador			X		Revisar los registros y actividades en los sistemas de información y proteger su almacenamiento.
	12.4.4	Sincronización de relojes			X		Control implementado, con oportunidad de mejoras.
	12.5	**Control de Software Operacional**					
	12.5.1	Instalación de software en sistemas operativos			X		Definir los parámetros de seguridad para la instalación de software en los sistemas operativos, garantizando una adecuada ejecución del proceso.
	12.6	**Gestión de la Vulnerabilidad Técnica**					
	12.6.1	Gestión de las Vulnerabilidades técnicas				X	Fijar un procedimiento de las gestiones de vulnerabilidades técnicas en el cual se incorpore los reportes y los tiramientos que se den de forma segura.
	12.6.2	Restricciones sobre la instalación de software					Control implementado, con oportunidad de mejoras.
	12.7	**Consideraciones sobre auditorias de sistemas de Información**					
	12.7.1	Controles de auditorías de sistemas de Información			X		Definir mecanismos de monitoreo y control de auditorías en los sistemas de información.
Clausula	**Sec**	**Objetivo de Control**	**LR**	**CO**	**BR/ BP**	**RRA**	**Observaciones**
13 Seguridad de las Comunicaciones	**13.1**	**Gestión de la seguridad de las redes**					
	13.1.1	Controles de Redes			X		Se aconseja que se implemente solución de control de acceso a la red. Con el fin de que los equipos de los funcionarios se conecten a la red de la institución.
	13.1.2	Seguridad de los servicios de Red			X		Se debe registrar todos servicios de red, aplicando los controles de seguridad se acoja a cada caso.
	13.1.3	Separación de las Redes			X		Definir una adecuada segmentación de la red, de acurdo al personal de la institución.
	13.2	**Transferencia de Información**					

	13.2.1	Políticas y procedimientos de transferencia de Información			**X**		Fijar procedimiento e Implementar métodos de transferencia de información en la institución.
	13.2.2	Acuerdos sobre transferencia de información			**X**		Fijar procedimiento e Implementar métodos de transferencia de información en la institución.
	13.2.3	Mensajería Electrónica			**X**	**X**	Validar que exista cifrado de correo electrónico en la institución para el envió de los mismo, y que este activo.
	13.2.4	Acuerdos de Confidencialidad o no divulgación			**X**	**X**	Diseñar acuerdo de confidencialidad de la información con los empleados en sus contratos de trabajos.
Clausula	**Sec**	**Objetivo de Control**	**LR**	**CO**	**BR/ BP**	**RRA**	**Observaciones**
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	**14.1**	**Requisitos de Seguridad de los Sistemas de Información**					
	14.1.1	Análisis y especificación de requisitos de seguridad de la Información			**X**		Fijar que todos los proyectos que se realicen en la institución, consideren tener los requerimientos de seguridad informática.
	14.1.2	Seguridad de servicios de aplicaciones en redes Publicas			**X**	**X**	Asegurar el protocolo de transferencia de archivo, que no esté expuesto, como acceso anónimo.
	14.1.3	Protección de los servicios de las aplicaciones transaccionales			**X**	**X**	Asegurar el protocolo de transferencia de archivo, que no esté expuesto, como acceso anónimo.
	14.2	**Seguridad de los procesos de desarrollo y soporte**					
	14.2.1	Política de desarrollo seguro			**X**		Fijar, publicar política de desarrollo seguro en los sistemas de información de la institución.
	14.2.2	Procedimientos de control de cambios en sistemas			**X**		Fijar, publicar procedimiento de control de cambios en los sistemas de la institución y la infraestructura tecnológica.
	14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación			**X**		Fijar, publicar guía, procedimiento, formatos y listas de chequeo cuando hay cambios en la plataforma tecnológica.
	14.2.4	Restricción en los cambios a los paquetes de software			**X**		Fijar, publicar procedimiento para la restricción en los cambios de paquetes de software.
	14.2.5	Principios de construcción de sistemas seguros			**X**		Fijar principios y estándares de seguridad en desarrollo de software.

	14.2.6	Ambiente de desarrollo seguro			X		Fijar controles de seguridad para desarrollo en ambiente seguro.
	14.2.7	Desarrollo contratado externamente			X		Control implementado, con oportunidad de mejoras.
	14.2.8	Pruebas de seguridad en sistemas			X		Definir un programa de pruebas de seguridad de los sistemas de información.
	14.2.9	Pruebas de aceptación de sistemas			X		Definir policita de aceptación de los sistemas de información en la institución.
	14.3	**Datos de Prueba**					
	14.3.1	Protección de los datos de prueba			X		Fijar un procedimiento para la protección de los datos usados para prueba, que contenga el uso y manejo adecuado.
Clausula	**Sec**	**Objetivo de Control**	**LR**	**CO**	**BR/ BP**	**RRA**	**Observaciones**
15 Relación con los proveedores	**15.1**	**Seguridad de la Información en la relación con los proveedores**					
	15.1.1	Política de seguridad de la información para las relaciones con los proveedores			X		Fijar en la política de seguridad de la información, esta debe contener la seguridad de las mismas frente a los proveedores.
	15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores			X		Control implementado, con oportunidad de mejoras.
	15.1.3	Cadena de Suministro de tecnología de información y comunicaciones			X		Control implementado, con oportunidad de mejoras.
	15.2	**Gestión de la prestación de servicios de proveedores**					
	15.2.1	Seguimiento y revisión de los servicios de los proveedores			X		Aplicar programas de auditoria a las empresas que le prestan servicios a la institución.
	15.2.2	Gestión de cambios en los servicios de los proveedores			X		Validar el proceso de gestión de cambios en los servicios de los proveedores.
Clausula	**Sec**	**Objetivo de Control/Control**	**LR**	**CO**	**BR/ BP**	**RRA**	**Observaciones**
16 Gestión de Incidentes de Seguridad de la Información	**16.1**	**Gestión de incidentes y mejoras en la seguridad de la Información**					
	16.1.1	Responsabilidades y procedimientos			X	X	Definir y publicar procedimientos de gestión de incidentes de seguridad al interior de la institución.

	16.1.2	Reporte de eventos de seguridad de la información			X	X	Definir y publicar procedimientos de gestión de incidentes de seguridad al interior de la institución.
	16.1.3	Reportes de debilidades de seguridad de la información			X	X	Definir y publicar procedimientos de gestión de incidentes de seguridad al interior de la institución.
	16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos			X	X	Definir y publicar procedimientos de gestión de incidentes de seguridad al interior de la institución.
	16.1.5	Respuesta a incidentes de seguridad de la Información			X	X	Definir y publicar procedimientos de gestión de incidentes de seguridad al interior de la institución.
	16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la Información			X	X	Definir y publicar procedimientos de gestión de incidentes de seguridad al interior de la institución.
	16.1.7	Recolección de Evidencia			X	X	Definir y publicar procedimientos de gestión de incidentes de seguridad al interior de la institución.
Clausula	**Sec**	**Objetivo de Control**	**LR**	**CO**	**BR/ BP**	**RRA**	**Observaciones**
17 Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio	**17.1**	**Continuidad de Seguridad de la Información**					
	17.1.1	Planificación de la continuidad de la seguridad de la Información			X	X	Definir, publicar e implementar una política de continuidad del negocio para la institución.
	17.1.2	Implementación de la continuidad de la Seguridad de la Información			X	X	Definir, publicar e implementar una política de continuidad del negocio para la institución.
	17.1.3	Verificación, revisión y evaluación de la continuidad de seguridad de la Información			X	X	Definir, publicar e implementar una política de continuidad del negocio para la institución.
	17.2	**Redundancias**					
	17.2.1	Disponibilidad de instalaciones de procesamiento de información			X	X	Control implementado, con oportunidad de mejoras.
Clausula	**Sec**	**Objetivo de Control**	**LR**	**CO**	**BR/ BP**	**RRA**	**Observaciones**
18 Cumplimiento	**18.1**	**Cumplimiento de requisitos legales y contractuales**					
	18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales			X		Control implementado, con oportunidad de mejoras.

	18.1.2	Derechos de propiedad Intelectual			**X**		Control implementado, con oportunidad de mejoras.
	18.1.3	Protección de Registros			**X**		Fortalecer los controles de acceso a la información en la institución.
	18.1.4	Privacidad y protección de información de datos personales			**X**		Definir policita y pautas para la protección de la privacidad de la información personal.
	18.1.5	Reglamentación de Controles Criptográficos			**X**		Definir procedimiento de reglamentación de controles criptográficos.
	18.2	**Revisiones de Seguridad de la Información**					
	18.2.1	Revisión Independiente de la Seguridad de la Información			**X**		Aprobar y dar a conocer la política de seguridad de la información en la institución.
	18.2.2	Cumplimiento con las políticas y normas de seguridad			**X**	**X**	Definir los mecanismos que permitan el cumplimiento de la policita de seguridad de la información.
	18.2.3	Revisión del cumplimiento técnico			**X**	**X**	Definir los mecanismos que permitan el cumplimiento de la policita de seguridad de la información.

Tabla 39: Observaciones Acorde Estándar ISO 27002.
Fuente: el autor

10. CRONOGRAMA

ACTIVIDAD	FEBRERO				MARZO				ABRIL				MAYO				JUNIO			
	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
Fase1. Levantamiento de Informacion																				
Fase2. Proceso de Analisis																				
Fase 4. Verificacion de los Riesgos																				
Fase 3. Inicio Propuesta para el SGSI																				
Fase 4. Capacitacion SGSI																				
Fase 5. Entrega Informe Final																				

Figura 17: Cronograma de actividades
Fuente: el Autor

11. CONCLUSIÓN

En el planteamiento de un sistema de gestión de Seguridad de la Información, basados a normas y lineamientos de seguridad como lo es la Norma ISO/IEC 27001:2013, la cual se basa en un modelo de mejores prácticas es la herramienta de gran apoyo que permite identificar diferentes aspectos que deben tener en cuenta una institución u organización, que decide establecer un modelo de seguridad de la información, para ello si la empresa decide lograr cumplir al pie lo sugerido en la norma ISO/IEC 27001:2103, conseguir materializar en los tiempos adecuados y sostenible un Sistema de Gestión de Seguridad de la Información (SGSI) , dependiendo de la naturaleza de la entidad, y cultura frente al tema de seguridad de la información.

Como se evidencio a lo largo de este trabajo es claro que la información y datos son el activo más preciado y vital con que una institución cuenta. Por lo que partiendo de esta premisa una institución como lo es el Centro educativo de Sistemas UPARSISTEM, es muy importante tener un Sistema de Gestión de Seguridad de la Información, en cual este dirigido a sus necesidades y negocios.

Con base a los resultados logrados al tratar de aplicar los requisitos de la norma ISO 27001:2013, se obtuvieron una colección de valores que permitieron fijar el estado de madurez de la institución frente a la gestión de seguridad de la información.

- ✓ Es de vital importancia y necesario fijar una política de Seguridad de la Información, aprobada por la alta gerencia para así lograr garantizar su implementación, actualización y cumplimiento.

- ✓ Es necesario implementar controles adecuados, y reforzar los que están para asegurar que la seguridad de la información entre en el ciclo de vida del desarrollo de la institución.

- ✓ Es necesario implementar un procedimiento de gestión de incidentes de seguridad de la información, para así proporcionar a la institución de mecanismos para los reportes de seguridad y respuesta a los eventos e incidentes de seguridad de la información.

12. BIBLIOGRAFIA

- ✓ CABALLERO QUESADA Alonso Eduardo (2013). Manual de pruebas y Hacking con Kali Linux. {12 de octubre de 2016}. {En línea}. Disponible en: (http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf).

- ✓ DOCUMENTACIÓN OFICIAL DEL SOFTWARE KALI LINUX, {12 de octubre de 2016}. {En línea}. Disponible en: (http://www.kali.org/official-documentation).

- ✓ GUERRÓN JORGE. (2013). Elaboración de un plan para la implementación del sistema de gestión de seguridad de la información. Lonja. {12 de octubre de 2016}. {En línea}. Disponible en: (http://openaccess.uoc.edu/webapps/o2/bitstream/10609/19067/24/jguerronTFM0113memoria.pdf).

- ✓ HERRAMIENTAS, web destinada a gestión de programas en seguridad de la información. {13 de octubre de 2016}. {En línea}. Disponible en: (http://www.iso27000.es/herramientas.html).

- ✓ ARQUEZ DE MELO, José “Comunicación e integración latinoamericana: El papel de ALAIC”. {En línea}. {13 de octubre de 2016} disponible en: (www.mty.itsem.mx/externos/alaic/texto1html).

- ✓ METODOLOGÍA MAGERIT Y ANEXOS, herramienta PILAR. {13 de octubre de 2016}. {En línea}. {13 de octubre de 2016} disponible en: (https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/).

- ✓ MINTIC GOBIERNO DE COLOMBIA. “Ley 1273 de 2009 delitos informáticos”. {En línea}. {15 de octubre de 2016} disponible en: (http://www.mintic.gov.co/portal/604/w3-article-3705.html).

- ✓ MONJE C. (2011). Metodología de la investigación cuantitativa y cualitativa. Guía didáctica. {En línea}. {17 de octubre de 2016}. disponible en: (http://carmonje.wikispaces.com/file/view/Monje+Carlos+Arturo++Gu%C3%ADa+did%C3%A1ctica+Metodolog%C3%ADa+de+la+investigaci%C3%B3n.pdf).

- ✓ PALLAS MEGA GUSTAVO. (2009), Metodología de implantación de un SGSI en un grupo empresarial jerárquico, Universidad de la República, Montevideo Uruguay. {En línea}. {15 de octubre de 2016} disponible en: (http://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf).

Anexos 1. Carta Aceptación Desarrollo Proyecto

Valledupar 20 de Octubre de 2015.

Doctora
DORIANA BUELVAS RODRIGUEZ
Gerente
Centro Educativo de Sistemas UPARSISTEM
Valledupar – Cesar

Referencia: Solicitud de aprobación para desarrollar proyecto de grado en área de Seguridad informática en las Instalaciones de UPARSISTEM

Reciba un Cordial Salud,

Muy respetuosamente me dirijo a usted para solicitarle me sea autorizado el desarrollo de mi proyecto de grado en las instalaciones del Centro Educativo de Sistemas UPARSISTEM, en área de seguridad informática, como requisito de graduación para la Especialización en seguridad informática en la Universidad Nacional Abierta y a Distancia (UNAD).

Agradezco su atención y colaboración brindada

Cordialmente,

RUBEN DARIO ACUÑA MONTES
C.C. 77090411 de Valledupar
Ingeniero de Sistemas

Visto Bueno Aceptación
DORIANA BUELVAS RODRIGUEZ
Gerente

UPARSISTEM
AUTORIZACIÓN
Nº2
Fecha Propuesta:

Anexos 2. Formato encuesta aplicada.

ENCUESTA DE ESTADO GENERAL SEGURIDAD INFORMÁTICA

Valledupar – Cesar 2016

1. DATOS GENERALES	
1.1. Ubicación (Departamento - Cargo):	
1.2. Nombre de la persona encuestada:	
1.3. Relación laboral:	
1.4. Teléfono contacto:	**1.5. Correo electrónico:**
PREGUNTAS **Marque con una x una de las siguientes opciones:**	
1. ¿HA ESCUCHADO O TIENE CONOCIMIENTO SOBRE SEGURIDAD INFORMÁTICA?	
1. Si ☐ 2. No ☐	
2. ¿PIENSA USTED QUE ES IMPORTANTE LA SEGURIDAD INFORMÁTICA?	
1. Si ☐ 2. No ☐	
3. ¿TIENE CONOCIMIENTO SOBRE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA?	
1. Si ☐ 2. No ☐	
4. ¿DISPONEN DE UNA WEB CORPORATIVA?	
1. Si ☐ 2. No ☐	

5. ¿HA SIDO VÍCTIMA DE HURTO INFORMÁTICO?

1. Si ☐
2. No ☐

6. ¿REALIZA USTED COPIA DE SEGURIDAD DE SUS ARCHIVOS MÁS IMPORTANTES?

1. Si ☐
2. No ☐

7. ¿EN CASO DE OCURRENCIA DE UN INCIDENTE INFORMÁTICO, SABE A QUIÉN ACUDIR?

1. Si ☐
2. No ☐

8. ¿EL ACCESO A LAS ÁREAS DE TECNOLOGÍA ES RESTRINGIDA?

1. Si ☐
2. No ☐

9. ¿REALIZA DE MANERA PERIÓDICA CAMBIO DE SUS CONTRASEÑAS DE ACCESO?

1. Si ☐
2. No ☐

10. ¿EXISTE DUAL CONTROL EN LA REALIZACIÓN DE LOS PROCESOS?

1. Si ☐
2. No ☐

Anexos 3: Listado de Asistencia Capacitación SGSI

CONTROL DE ASISTENCIA A CAPACITACIONES, REUNIONES Y EVENTOS

UPAR-002.08 | Fecha: 01/04/2017

TIPO: Capacitación [X] Reunión [ ] Evento [ ]

Tema: Sistema de Gestión de Seguridad de la Información (SGSI)

Facilitador: Rubén Darío Acuña Montes

No.	NOMBRE	CARGO	FIRMA
1	Jeisa Fariño fernandez	Docente	[illegible]
2	Hermes Quiroz	Coordinador	[illegible]
3	Carlos A Aris Gonzalez.	Docente	[illegible]
4	Elicenith Garcia	Atención Cliente	Elcenith G.
5	Estefanny Plata	Asistente Academica	Estefany Plata
6	Darwin Rivera C	Coordinación Cel.	[illegible]
7	Yarcel Navarro Vergel	Assistencia al cliente	[illegible]
8	Yolieth Quintero Prado	Asistencia al cliente	Q. Yolieth Q.
9	Yudy Vanessa Cuellar Dominguez	Asistencia al cliente	Yudy Cuellar.
10	Luis Alfredo Rangel	Asistente Academico	Luis Rangel.
11	Arturo Jose Vanegas	Asist en soporte	[illegible]
12	Alberto Alvarez Hurtado	Docente	[illegible]
13	Marta Zuleima Gomez Leal	Asistente al cliente	M. Gomez Leal.
14	Lucia Garcia Gonzalez	Asistente al cliente	Lucia Gonzalez
15	Hisnaldo Ortiz	Asist. contabilidad	[illegible]

CODIGO: UPAR-002.08 | VERSIÓN: 3 FECHA: 01/06/12 | PAGINA 1 DE 2

CONTROL DE ASISTENCIA A CAPACITACIONES, REUNIONES Y EVENTOS

UPAR-002.08	Fecha: 01/04/2017

16	ANGIE LORENA FUENTES CALDERÓN.	ASISTENTE AT. CLIENTE.	ANGIE FUENTES.
17	Rubiela Bolaño Ramos	Docente	
18	Frank Murcia	Docente	
19	Jorge Santiago	Docente	
20	Carlos Augusto Arias	Docente	
21	Lorena Hernandez	Asistente Almacen	Lorena H.
22	Jaider Lopez.	Docente	
23	OSMER E MEJIA TORRES	DOCENTE	
24	Sol Margarita Vidal Piscitelli	Atención al cliente	Sol M. Vidal P.
25	Brenda Palomino Romero	Atencion al cliente	
26	Leoildo Carrillo Mojico	Coordinador Academico	
27	Carlos Cárdoba C.	Docente	
28	Pedro Fernandez Quiroz	Docente	
29	Jhon Fontes	Docente	
30	Jeiner Hurtado Montes	DOCENTE.	

Anexos 4: Política de Seguridad de la Información Código GSI-UPAR-POL-001

	POLÍTICA	**CÓDIGO: GSI-UPAR-POL-001**
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	**VERSIÓN: 1**
		FECHA: 01/ABRIL/2017

TABLA DE CONTENIDO.

1. GLOSARIO DE TÉRMINOS

Confidencialidad: La confidencialidad consiste en asegurarse de que solamente aquellos que tienen autorización puedan acceder a la información. [ISO/IEC 27002:2005(E)]. Es la propiedad de que la información no esté disponible ni sea divulgada a personas, entidades o procesos sin autorización.

Continuidad: La continuidad es el proceso de establecer, por adelantado, las capacidades necesarias para evitar o reducir el impacto de un acontecimiento que provoca la interrupción de las operaciones en una o más unidades de negocios. (Política de Gestión de Continuidad del Negocio de Uparsistem).

Disponibilidad: La disponibilidad consiste en asegurarse de que los usuarios autorizados tengan acceso a la información y a los sistemas de apoyo, cuando se requiera. [ISO/IEC 27002:2005(E)]. Se trata de la propiedad de que una entidad autorizada, bajo solicitud, pueda tener acceso y utilizar la información.

Incidente de seguridad: Es un acontecimiento o una serie de acontecimientos que pone en riesgo la confidencialidad, la integridad o la disponibilidad de la información, datos o servicio informático, servicio que se proporciona por medios informáticos o medios automáticos que son propiedad de cualquier cliente, empleado o entidad corporativa.

Información: La información hace referencia a la representación de hechos, que son recopilados para efectuar operaciones comerciales. Utilizada de manera intercambiable con datos, el término incluye, archivos de datos estructurados y no estructurados, archivos de audio o vídeo, mensajes electrónicos o de correo de voz, fax u otro tipo de mensajes, impresos, copias de respaldo o archivadas del original por cualquier medio, etc.

Infraestructura tecnológica: La infraestructura tecnológica es un término que cubre varios componentes de tecnología de la información compartida, documentación vinculada, contratos y factores que facilitan los sistemas de aplicaciones de apoyo y los procesos comerciales. La infraestructura de tecnología de la información, entre otras cosas, comprende lo siguiente:

- Arquitectura y normas para mejorar la interoperabilidad, implementación, actualización y operación.
- Los componentes tecnológicos como el hardware de las computadoras, software del sistema operativo, sistemas de administración de bases de datos, programas intermedios o middleware, etc.
- Infraestructura de comunicaciones como red de datos o de voz (incluyendo el acceso remoto), utilidades, protocolos y tecnologías relacionados.

- Aplicaciones compartidas y estándar como correo electrónico, correo de voz, provistas como servicio operativo.
- Procesos y servicios operativos, como integración, prestación de servicios, administración de aplicaciones y datos, etc.
- Recursos intangibles como el capital intelectual que diferencia los servicios de Uparsistem y constituye una fuente de ventaja competitiva.

Integridad: La integridad hace referencia a garantizar la precisión y totalidad de los métodos de información y de procesamiento. [ISO/IEC 27002:2005(E)].

Propietario de la información/sistema: El propietario de la información/sistema es la persona que se designa para custodiar la información. El "propietario de la información/sistema" ejerce los derechos de propiedad y/o responsabilidades de custodia de Uparsistem a fin de salvaguardar y administrar la información. En el caso de aplicaciones compartidas que se ofrecen como "servicios", el propietario del servicio que es responsable de la prestación del mismo será el "propietario de la información/sistema" designado.

Recursos del sistema de información: El término incluye información, sistemas de aplicaciones, personas e infraestructura tecnológica para apoyar los objetivos comerciales de Uparsistem. El término incluye todos los aparatos y equipo adquiridos (comprados, arrendados o en préstamo), creados y/o contratados.

Riesgos de Tecnología de la Información: El riesgo en la pérdida de datos y/o la pérdida a nivel financiero debido a alteraciones en el sistema o fallas en los controles que sean consecuencia de factores internos o externos.

Sistema de aplicaciones: El sistema de aplicaciones hace referencia a los sistemas automatizados de usuario y procedimientos que procesan información. El término incluye software, documentación, sistema de controles internos, instrucciones de ejecución y parámetros.

Usuario operativo: La gerencia asigna al usuario operativo como responsable de la utilización del sistema de aplicaciones que actualiza la información para ofrecer el servicio a los clientes y/o la administración interna de la información.

2. INTRODUCCIÓN.

La Política de Seguridad de la Información (en lo sucesivo, la “Política”) define el compromiso del Centro Educativo de Sistemas Uparsistem para administrar efectiva y eficazmente los riesgos, de manera coordinada y conforme a los reglamentos aplicables en todo lugar donde la institución mantiene operaciones.

Uparsistem se basan en la confianza y dependen estrechamente de la información. Ya sea la información que emana directamente de la institución o la que nos confían los estudiantes, Clientes, proveedores u otras partes con las cuales Uparsistem realiza negocios, es un activo valioso y, por lo tanto, debe protegerse en forma adecuada. La seguridad de la información conlleva la protección de la misma, lo cual incluye el apoyo a los recursos de los sistemas de información, para protegerlos de una amplia variedad de amenazas, cuya naturaleza está cambiando continuamente. Dichas amenazas comprenden errores y omisiones, fraudes, accidentes y daños deliberados. La tecnología se encuentra en constante evolución; por lo tanto, Uparsistem está obligado a evaluar los riesgos de forma continua con el fin de proteger nuestros activos.

La seguridad de la información es fundamental para Uparsistem y tiene el objeto de asegurar el éxito de sus actividades y de mantener su reputación. Las políticas, normas, procedimientos, controles de sistemas y capacitación relacionados con la seguridad de la información conforman una parte esencial del marco general de la gestión de riesgos y los controles internos de Uparsistem, con el fin de asegurar que la información, bajo su custodia, no sea explotada, mal utilizada, cambiada y/o divulgada sin descubrir tales acciones. Los niveles apropiados de seguridad de la información protegen la reputación de Uparsistem y

sustentan la política de Uparsistem con respecto a hacer las cosas apropiadas, hacerlas bien y tratar con las personas idóneas.

Uparsistem es propietario o tiene el derecho de utilización de toda la información que se procesa o se conserva en sus sistemas y que es creada, adquirida y operada durante sus operaciones. Conforme a su obligación de supervisar y administrar las actividades de Uparsistem, la Alta Dirección tiene el derecho de acceder o autorizar el acceso, examinar, controlar y/o investigar todo tipo de información, sistemas de aplicaciones de apoyo e infraestructura tecnológica.

2.1. Ámbito

Esta Política, sujeta a cualquier requisito legal o reglamentario local o jurisdiccional, se aplica a:

- Todas las subsidiarias de propiedad absoluta o controlada por el Centro Educativo de Sistemas Uparsistem, donde haya sido adoptada formalmente.
- Terceros, mediante compromisos contractuales.

Esta Política define los requisitos de protección manuales y electrónicos de la información registrada, procesada, recopilada, compartida, transmitida o archivada en un formato electrónico, así como los sistemas de aplicaciones de apoyo y la infraestructura tecnológica. En este contexto, la información incluye los archivos de datos estructurados o no estructurados, archivos de audio o vídeo, correo electrónico, correo de voz, fax u otros tipos de mensajes, impresos, copias de respaldo o copias archivadas de los originales por cualquier medio óptico, magnético o cualquier otro medio.

La información debe protegerse durante todo su ciclo de procesamiento, lo que comprende su producción, recopilación, conservación, archivo, transmisión, utilización y destrucción final. La información recopilada inicialmente con el estudiante debe protegerse desde su punto de adquisición por Uparsistem hasta el punto de entrega de la misma al estudiante.

Si una unidad de negocios autoriza un acuerdo que estipula que una tercera parte pueda generar, recopilar, archivar o utilizar, transmitir o disponer de la información en su representación, entonces dicha unidad es responsable de estar al tanto de los procedimientos y prácticas de seguridad de la tercera parte y de asegurarse de que cumpla con los requisitos de esta Política1, así como de cualquier reglamentación aplicable.

La Política de Seguridad de la Información enfrenta los riesgos actuales en la medida que estos evolucionan y contribuye a mantener los riesgos de seguridad de la información a un nivel aceptable. Los riesgos de seguridad de la información implican un riesgo en la pérdida de datos y/o la pérdida a nivel financiero debido a interrupciones en los sistemas o fallas en los controles, como resultado de factores internos o externos. Es parte del inventario de riesgos.

Esta Política debe leerse a todos los empleados, terceros y contratistas del centro educativo de sistemas Uparsistem.

La gestión de los riesgos de la seguridad de la información exige la coordinación entre los diferentes equipos. Todos los grupos juegan un papel integral en los esfuerzos de la evaluación de los riesgos y en la implementación de la seguridad de la información.

2.2. Cumplimiento

El cumplimiento de esta Política es obligatorio para todas las personas o procesos que tienen acceso a los recursos de los sistemas de información del Centro educativo de sistemas Uparsistem. Basados en las declaraciones de certificación o recertificación anual efectuadas conforme a las Pautas para la Conducta en los Negocios de Uparsistem, todos los empleados a todos los niveles tienen la responsabilidad de mantener la precisión, confidencialidad y seguridad de las comunicaciones, de las operaciones y de la información.

Las tentativas deliberadas o constantes de infringir o las infracciones a esta Política implican la aplicación de medidas disciplinarias conforme a las Pautas para la Conducta en los Negocios de Uparsistem y las políticas de Talento Humano.

2.3. Actualización de la política

El custodio de esta Política del centro educativo de sistemas Uparsistem es la Dirección de las Tics. Este último es responsable de garantizar que dichos documentos se mantengan actualizados y sean apropiados.

Esta Política se revisa, actualiza y aprueba como mínimo cada dos años por medio del proceso siguiente:

- La Dirección de las Tics revisa y recomiendo los cambios a esta Política, según sea necesario, y de acuerdo a los cambios que se presentan en el panorama de riesgo.
- El Comité de Dirección de las Tics revisa y otorga su visto bueno a la Política.
- La Alta gerencia y el Comité del a Dirección de las Tics revisa y aprueba la Política para presentarla y publicarla.

Es de vital importancia que se documenten y aprueben las siguiente policita en el centro educativo de sistemas Uparsistem, para su referencia.

- El Manual de Seguridad de la Información de Uparsistem, hace parte integral de la Política de Seguridad de la Información, pues debe contener los requisitos legales y reglamentarios locales que son de obligatorio cumplimiento.
- Políticas para la Protección de la Privacidad de la Información Personal.
- Política de Cumplimiento de Uparsistem.
- Política de Continuidad del Negocio de Uparsistem.
- Acuerdo del Usuario Móvil de Uparsistem.

3. OBJETIVOS

La política de seguridad de la información del Centro Educativo de Sistemas “UPARSISTEM” constituye una buena práctica de negocio que ayudará a las áreas a proteger sus activos de información. Esta Política contiene los requisitos mínimos de seguridad de la información que deben cumplirse. Cada área debe considerar en sus procesos los estándares de seguridad de esta Política de seguridad.

Como Institución responsable protegemos la información que nuestros clientes nos brindan, además de garantizar la confidencialidad, la integridad y la disponibilidad de nuestra propia información. La falta de protección de los activos de información podría provocar pérdidas financieras, dañar la reputación o tener un impacto negativo en la confianza de los clientes.

4. ALCANCE

La Política de seguridad de la información aplica a todos los activos de información, los procesos, empleados directos e indirectos y terceros que acceden a los activos de información de la Institución.

5. AUDIENCIA

La Política de Seguridad de la Información aplica a todos los funcionarios del Centro Educativo de Sistemas “UPARSISTEM” y terceros que procesen, almacenen o transmitan información de “UPARSISTEM”.

6. DECLARACIONES Y PRINCIPIOS DE LA POLÍTICA

6.1. Declaraciones de la política

Uparsistem empleará los medios razonables para asegurar la confidencialidad de la información bajo su custodia, garantizar su integridad y asegurar la disponibilidad y continuidad de los sistemas de aplicaciones de apoyo y la infraestructura tecnológica.

Estos objetivos deben alcanzarse a un costo acorde con los riesgos de los negocios, y en forma congruente tanto con la necesidad de información fiable como con la necesidad de proporcionar un nivel de servicio apropiado a través de diversos canales de servicio que continuamente cumplan o sobrepasen las expectativas comerciales y de los clientes, y deben estar conforme a los requisitos legales, reglamentarios o contractuales.

6.2. Principios de seguridad de la información

Se deberán aplicar y respetar los principios de seguridad de la información que se describen a continuación para proteger la información.

6.2.1. Responsabilidad Individual

Todos los empleados, oficiales y directores tienen la responsabilidad de proteger la información, ya sea que se trate de información de propiedad exclusiva o de información confiada a Uparsistem por sus estudiantes, proveedores u otras partes con quienes Uparsistem realiza negocios, por medio del cumplimiento de esta Política y cualquier política, norma o procedimiento pertinente con sus funciones.

Las personas deben tener el cuidado, la diligencia y la habilidad que se esperaría de una persona razonablemente prudente al tratar información sensible e informar al superior jerárquico correspondiente sobre cualquier inquietud relacionada con acontecimientos sospechosos relativos a la seguridad por medio de la cadena de mando.

6.2.2. Responsabilidad del negocio

La unidad de negocios y áreas de apoyo a tecnología de la información de Uparsistem tienen la responsabilidad de administrar los riesgos en materia de seguridad de la información vinculados con sus procesos comerciales, sistemas de aplicaciones e infraestructura tecnológica a través de la aplicación de los principios siguientes:

- **Responsabilidad:** Toda información y todo sistema de aplicaciones de apoyo, incluso aquellos operados por terceras partes, debe tener un “propietario de la información/sistema” designado, quien se considera el custodio designado de la información durante la totalidad de su ciclo de procesamiento, desde el momento en que se origina o recopila la información hasta su disposición final apropiada.
- **Proporcionalidad**: La información debe protegerse contra un riesgo acorde con lo delicado de la misma, la complejidad y ámbito del negocio, necesidades en relación con el servicio al cliente e intereses de Uparsistem.
- **Derecho de accesibilidad:** Se debe acceder, cambiar y utilizar la información, los sistemas de aplicaciones de apoyo y la infraestructura tecnológica solamente para fines legítimos. El acceso, incluso el acceso iniciado por el estudiante, se debe autentificar y basarse en el principio del derecho mínimo de accesibilidad, o “necesidad de conocer”.
- **Acuerdos de contratación externa:** Se debe solicitar a los proveedores externos, incluso a empresas contratadas para fines de incremento de personal, por medio de un contrato, implementar y hacer respetar continuamente los procedimientos y prácticas sobre seguridad que cumplan con los requisitos de esta Política. En caso necesario, se debe controlar periódicamente a los proveedores de servicios a fin de confirmar que satisfacen sus obligaciones estipuladas en el contrato.
- **Cumplimiento legal:** Se debe cumplir con todos los requisitos legales y reglamentarios aplicables en materia de seguridad de la información en países donde se opera. Como mínimo, en cada jurisdicción, las unidades de negocio deben poder demostrar el cumplimiento de las leyes y reglamentos aplicables mediante la adopción de las normas de seguridad y los códigos de conducta pertinentes.
- **Uso de la tecnología:** En Uparsistem, solo se permite el uso de programas y equipos informáticos autorizados y registrados.
- **Protección de datos:** La protección de datos y la confidencialidad de la información personal debe corresponder en forma apropiada a lo delicado de la información y debe estar conforme a las leyes y reglamentos pertinentes.

- **Sensibilización:** Se debe comunicar continua y regularmente la necesidad de mantener la seguridad de la información a todos los empleados, oficiales, socios, consultores y docentes, proveedores de servicio.
- **Control:** La Dirección de las Tics y la Alta Gerencia deben controlar y revisar regularmente los procedimientos y mecanismos de control de seguridad de la información para confirmar que siempre operan en forma fiable; que se cumple continuamente con las políticas, normas y pautas sobre seguridad; y que los procedimientos y mecanismos son adecuados para identificar y responder a las actividades inusuales o inaceptables, incluso con respecto a las operaciones iniciadas por el cliente.
- **Evaluación y mejoramiento:** Se debe evaluar y mejorar regularmente la idoneidad de los procedimientos y mecanismos de control sobre la seguridad de la información, según sea necesario, a fin de que los mismos correspondan a las cambiantes amenazas, los riesgos y las opciones de control, de manera que satisfagan continuamente las obligaciones comerciales, las expectativas razonables de servicio al cliente y los requisitos reglamentarios.
- **Informes sobre incidentes:** Los incidentes relacionados con la seguridad son importantes y la respuesta a los mismos debe ser fiable. Se deberá enviar, de forma inmediata o en cuanto las circunstancias lo permitan, un informe sobre los incidentes relacionados con la seguridad a la Dirección de las Tics. Los incidentes que involucren información personal detallada de un cliente deberán informarse también a la Alta Gerencia.

7. OTROS DOCUMENTOS

Manuel De Seguridad De Información

8. CONTROL DE CAMBIOS

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	01/Abril/2017	Creación

ELABORÓ		REVISÓ	APROBÓ
Nombre:	Rubén Darío Acuña Montes	**Nombre:**	**Nombre:**
Cargo:	Especialista en Seguridad Informática en Formación	**Cargo:**	**Cargo:**
Fecha:	01/Abril/2017	**Fecha:**	**Fecha:**