ANÁLISIS DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN UTILIZANDO LA METODOLOGÍA MAGERIT EN LA INSTITUCIÓN EDUCATIVA DOMINGO SAVIO EN LA CIUDAD DE FLORENCIA – CAQUETÁ

ADRIANA PAREDES SALINAS

UNIVERSIDAD ABIERTA Y A DISTANCIA "UNAD"

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA "ECBTI"

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

FLORENCIA – CAQUETÁ

2018

ANÁLISIS DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN UTILIZANDO LA METODOLOGÍA MAGERIT EN LA INSTITUCIÓN EDUCATIVA DOMINGO SAVIO EN LA CIUDAD DE FLORENCIA – CAQUETÁ

ADRIANA PAREDES SALINAS

Proyecto de Grado para optar el título de

Especialista en Seguridad Informática

Asesor:

MARIANO ESTEBAN ROMERO

Ingeniero de Sistemas

Especialista en Seguridad Informática

Docente

UNIVERSIDAD ABIERTA Y A DISTANCIA "UNAD"

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA "ECBTI"

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

FLORENCIA – CAQUETÁ

2018

EXCLUSIÓN DE RESPONSABILIDAD

La universidad no se hace responsable por los conceptos emitidos por mí en esta tesis de grado. La responsabilidad de esta Tesis de Grado, me corresponde EXCLUSIVAMENTE.

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Florencia, Agosto 10 de 2018

CONTENIDO

pág.

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCIÓN

Hoy en día las organizaciones sin importar su tamaño o razón social, dependen cada vez más del uso de tecnologías de la información y la comunicación, que son utilizadas como apoyo en la mejora de sus procesos y el logro de los objetivos institucionales.

La información se ha vuelto el activo más importante de toda organización, y la gestión eficiente de ésta se ha convertido en logro determinante para el alcance de los objetivos institucionales; es por ello que se ha percibido la necesidad de obtener servicios informáticos de calidad que administren de forma efectiva y ética los activos de información. Es muy importante destacar que la gestión de la seguridad de la información, promueve a que una organización obtenga ventajas competitivas y brinde servicios de mayor calidad con el objetivo de satisfacer las necesidades y expectativas del cliente.

Este proyecto se basa en un análisis de riesgos relacionados con las tecnologías de la información basado en la metodología Magerit, como herramienta de la seguridad de la información que permite determinar los factores de riesgo a los que potencialmente podría estar expuestos los activos de información de la Institución.

Teniendo en cuenta que la Institución Educativa Domingo Savio, es una organización cuya infraestructura tecnológica está en continuo crecimiento, no cuenta con una eficiente planificación, y que de su uso depende la prestación de servicios sensibles; se hace necesario realizar un análisis de riesgos de la seguridad de la información que permita determinar controles adecuados para alcanzar un nivel de seguridad razonable.

La finalidad de este proyecto consiste en desarrollar un análisis de riesgos de la seguridad de la información que enmarcan el funcionamiento de la Institución Educativa Domingo Savio. Para el logro de este proyecto se va a llevar a cabo la metodología Magerit, que consiste en analizar el impacto que puede sufrir la organización en el momento en que se materialicen violaciones de seguridad a los activos de información, así como identificar las posibles fallas que se puedan presentar a futuro y poder tomar las medidas preventivas y correctivas más adecuadas. Finalmente, se realizará un informe final en donde se determinen mecanismos de control y gestión de la seguridad de la información a la alta gerencia, teniendo en cuenta los resultados obtenidos en la evaluación de riesgos, y que apoyará a la organización hacia la continuidad en la oferta del servicio educativo de calidad.

1. EL PROBLEMA DE INVESTIGACIÓN

1.1. DESCRIPCIÓN

La Institución Educativa Domingo Savio es una organización de carácter privado que ofrece servicios educativos enmarcados en la reglamentación del Ministerio de Educación Nacional, y que actualmente se encuentra certificado en calidad bajo la norma ISO 9001:2008 desde el año 2010, con el apoyo del ente certificador APPLUS Colombia.

Ésta organización cuenta con infraestructura tecnológica que contribuye a la mejora en la prestación de servicios educativos de calidad, y que como parte del desarrollo institucional crecen de manera no planificada, para responder a las necesidades existentes. La Institución no cuenta con un sistema de seguridad de la información que permita la gestión de las vulnerabilidades, amenazas y riesgos, en lo que se podría verse expuesta la información y los activos asociados a ella; y por lo tanto, no cuenta con políticas de seguridad de la información que permita minimizar la probabilidad de ocurrencia de los riesgos latentes que puedan afectar la integridad, confidencialidad y disponibilidad de la información.

Es de vital importancia diagnosticar y analizar lo concerniente con la infraestructura tecnológica de la organización, ya que en sus instalaciones se realizan todos los procesos misionales y se llevan a cabo procedimientos sensibles como el acceso a la plataforma institucional en donde se publican las notas de los estudiantes, todos los procedimientos relacionados con la gestión de talento humano, administrativo y financiero; y la organización no posee acciones encaminadas a la gestión del riesgo en la seguridad de la información.

Teniendo en cuenta lo anteriormente mencionado, la institución necesita integrar Políticas de Seguridad de la Información como resultado de un análisis de riesgos; con el fin de no verse perjudicada por delitos informáticos, como intrusiones de seguridad, modificación y/o robo de información, denegación del servicio, y otros, que podrían afectar el normal funcionamiento de los procesos y la prestación de un servicio educativo de calidad.

1.2. FORMULACIÓN

Por tal razón, se plantea el siguiente interrogante: ¿Cómo identificar riesgos latentes en seguridad de la información utilizando la metodología MAGERIT, que permita establecer Políticas de Seguridad de la Información en la Institución Educativa Domingo Savio en la ciudad de Florencia – Caquetá?

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

• Identificar riesgos latentes en seguridad de la información utilizando la metodología MAGERIT, que permita establecer Políticas de Seguridad de la Información en la Institución Educativa Domingo Savio en la ciudad de Florencia – Caquetá.

1.3.2. OBJETIVOS ESPECÍFICOS

- Identificar y clasificar los activos de información presentes en la Institución Educativa Domingo Savio.

- Realizar el análisis de riesgos en los activos de información más críticos de la Institución Educativa Domingo Savio utilizando la metodología MAGERIT.

- Evaluar los riesgos latentes identificados, que permita proponer Políticas de Seguridad de la Información en la Institución Educativa Domingo Savio.

- Elaborar las Políticas de Seguridad de la Información en donde se determinen las estrategias que contribuyan a la mejora del control de la seguridad de la Información.

1.4. JUSTIFICACIÓN DEL PROBLEMA

La Institución Educativa Domingo Savio es una organización privada, certificada en calidad desde el año 2010, convirtiéndose en la primera institución que certifica la calidad del servicio educativo en el departamento del Caquetá. Es por eso, que con el fin de ofrecer servicios de calidad, y de garantizar la integridad de la información, surge la necesidad de realizar un análisis de riesgos relacionados con los activos de información críticos, que puedan afectar el desarrollo de los procesos misionales de la organización.

Dado que la Institución Educativa Domingo Savio, es una organización cuya infraestructura tecnológica está en continuo crecimiento, que no cuenta con una eficiente planificación, y que de su uso depende la prestación de servicios sensibles; puede verse afectada por riesgos latentes como delitos informáticos que pueden ocasionar pérdidas económicas y vulnerar la integridad, confidencialidad y disponibilidad de la información.

El análisis de riesgos de la organización, permitirá elaborar un documento en donde se definan políticas de seguridad de la información. Cabe destacar la importancia de la custodia de la información, ya que en algunos momentos puede estar clasificada de forma crítica, tanto para la organización, como para las partes interesadas.

La seguridad informática nos ofrece herramientas necesarias para la realización de una evaluación, que permita llegar a una serie de políticas de la seguridad de la información que apoyará a la organización en el desarrollo de sus procesos, y en la eficiente gestión de los riesgos latentes.

Con los resultados del análisis de riesgos se hará un documento en donde se determinen políticas de seguridad de la información, que servirá como apoyo para que la organización vea la posibilidad a futuro de implementar un Sistema de Gestión de Seguridad de la Información, paralelo al Sistema de Gestión de Calidad, ya implementado, y de esta manera contribuir a la mejora en la oferta del servicio educativo.

1.5. DELIMITACIÓN

- En este proyecto se va a realizar un análisis de riesgos asociados a los activos de información de la Institución Educativa Domingo Savio, que permita proponer estrategias a la alta gerencia, que contribuyan a la mejora del control y gestión de la información.

- El análisis de riesgos se realizará en la Institución Educativa Domingo Savio en su única sede ubicada en la Calle 25 entre carrera 10 y 11 esquina del Barrio Torasso en la ciudad de Florencia – Caquetá, en donde se encuentran ubicados los activos de información, con el fin de realizar el análisis de riesgos.

- El tiempo requerido para la ejecución del proyecto, así como la disponibilidad del personal de la organización, teniendo en cuenta su calendario de trabajo y las actividades institucionales que se realicen durante la vigencia del proyecto.

- No se garantiza que las recomendaciones que se realicen a la hora de la ejecución del proyecto sean implementadas en la institución, ya que esta decisión será de competencia por parte de la alta gerencia.

- El desarrollo del proyecto dependerá de la filosofía y políticas institucionales, enmarcadas en la propiedad del cliente de algunos activos.

2. MARCO DE REFERENCIA

2.1. ANTECEDENTES

Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor del Cauca[1]. Esta tesis de grado se llevó a cabo en la Institución Universitaria Colegio Mayor del Cauca en la ciudad de Popayán Cauca, que cuenta con una infraestructura tecnológica en crecimiento y el desarrollo del proyecto se plantea realizar un análisis de riesgos con el fin de proponer controles de seguridad de la información. Como resultados obtenidos, se aplicó la metodología MAGERIT logrando desarrollarse todos los objetivos planteados, y se plantearon controles y políticas de seguridad de la información, como base para la implementación de un Sistema de Gestión de Seguridad de la Información.

Análisis y diseño de un Sistema de Gestión de Seguridad Informática en la Empresa Aseguradora Suárez Padilla & Cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización[2]. Esta tesis de grado se desarrolló en la ciudad de Bogotá, en la Empresa Aseguradora Suárez Padilla & Cía. Ltda., en donde se realizó un diagnóstico de los riesgos críticos de la organización con base en la norma ISO 27001:2013. Los resultados obtenidos en el desarrollo del proyecto, fueron un compendio de Políticas asociadas con la seguridad de la información aplicados a la totalidad de los procesos internos y externos de la empresa.

Análisis y gestión de riesgo de la información en los sistemas de información misionales de una entidad del estado, enfocado en un sistema de seguridad de la información[3]. El objetivo de este proyecto de tesis de grado desarrollado en una empresa del estado de la ciudad de Bogotá es gestionar los riesgos asociados a seguridad informática del sistema de información misional de

[1] Caicedo Cuchimba Mildred, Perafán Ruiz John Jairo. Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor del Cauca, 2014.

[2] Suárez Padilla Sandra Yomay. Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez Padilla & Cía. Ltda, que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización, 2015.

[3] Garavito Robles Hina Luz. Análisis y gestión de riesgo de la información en los sistemas de información misionales de una entidad del estado, enfocado en un sistema de seguridad de la información, 2015

la organización, con el fin de determinar controles y medidas que permitan reducir los riesgos hallados durante el análisis. Dentro de los resultados obtenidos en la realización de este proyecto es la evaluación del riesgo de los activos críticos de la entidad, y de ello se realizó una evaluación de salvaguardas, aplicando la metodología MAGERIT.

Análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001 – Sistemas de Gestión de Seguridad de la información dirigido a una empresa de servicios financieros[4]. Este proyecto se desarrolló en la ciudad de Guayaquil y fue aplicado a una entidad financiera. El objetivo de la investigación fue llevar a cabo un análisis de los procesos críticos de la organización relacionados con la seguridad informática y seguridad de la información, cuyo resultado es una serie de recomendaciones con base en la norma ISO/IEC 27001. El resultado obtenido fue un manual de políticas de seguridad de la información ajustados a las necesidades de la empresa.

2.2. MARCO TEÓRICO

2.2.1. Seguridad informática y seguridad de la información

En la actualidad, las organizaciones dependen mucho más del uso de tecnologías de la información, ya sea en menor o en mayor grado, dependiendo de los objetivos institucionales; ya que éstas juegan un papel vital en el tratamiento de la información como el activo corporativo más importante.

La seguridad de la información permite ofrecer servicios informáticos que protegen de forma efectiva la confidencialidad, integridad y disponibilidad de la información[5].

La seguridad informática, como rama de la seguridad de la información, permite establecer métodos y mecanismos de protección y control a la información, con el fin de mantener la confidencialidad, integridad y disponibilidad de la información[6].

Aunque a simple vista, los términos son similares, difieren en aspectos muy relevantes. La seguridad de la información involucra aspectos muchos más

[4] Bailón Sánchez Edber Rafael, Bermúdez Molina Kelly Gabriela. Análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001 – Sistemas de Gestión de Seguridad de la Información dirigido a una empresa de servicios financieros, 2015.

[5] G. R. S. R. M. R. D. J. Escrivá Gascó, Seguridad Informática, Macmillan Iberia, S.A., 2013.

[6] Á. Gómez Vieites, Seguridad en Equipos Informáticos, RA-MA Editorial, 2014.

amplios, que no solo incluyen la parte técnica de la protección de datos, sino también el compromiso y participación de la alta gerencia, así como también la protección de la información sin importar el medio en el que se encuentra almacenada la misma. Mientras que la seguridad informática, se centra en la protección de la infraestructura física, lógica y de comunicación, concentrándose en las vulnerabilidades, básicamente en la parte hardware y software.

2.2.2. Análisis de riesgos informáticos

Antes de definir qué es un análisis de riesgos, se tiene que considerar la definición de riesgo. Según Magerit[7], el riesgo es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

Según Magerit, los activos se podrían ver afectados negativamente si no cuentan con una protección adecuada. Por esta razón, es importante conocer las características de cada activo y así poder determinar el riesgo asociado a cada una de ellas, para estimar en qué medida los activos estos expuestos a ellos.

2.2.3. Herramienta para evaluar la gestión de riesgos ISO 31001

Es una norma internacional que se basa en principios y directrices para la gestión del riesgo. Su flexibilidad le permite ser implementada tanto en pequeñas empresas como en grandes organizaciones del sector público o privado.

La norma posee una arquitectura la gestión del riesgo que se basa en unos principios, el marco de referencia y un proceso que va desde el establecimiento del contexto organizacional hasta el tratamiento del riesgo.

[7] GOBIERNO DE ESPAÑA (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Recuperado de: http://administracionelectronica.gob.es/

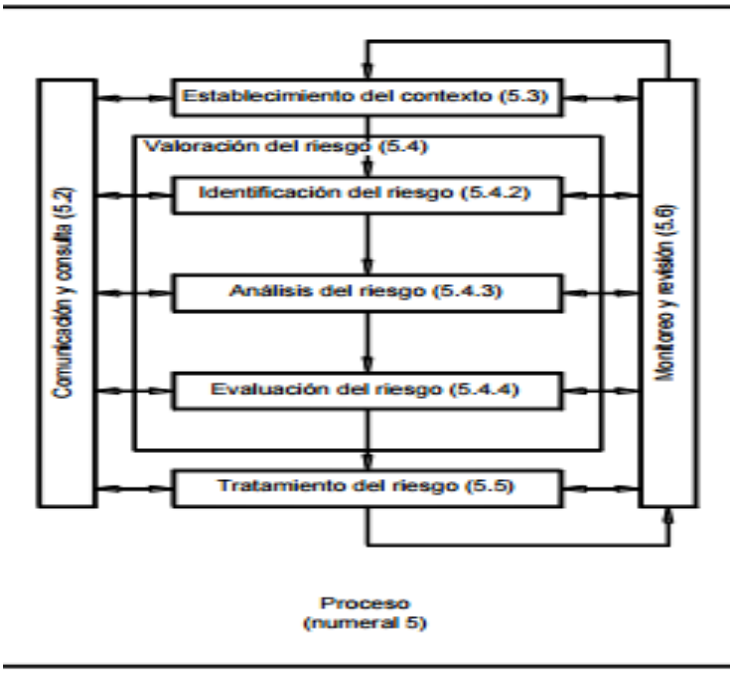


Figura 1. Arquitectura ISO 31001

Fuente: Norma ISO 31000

2.2.4. OCTAVE

Es una metodología de análisis de riesgos cuyo acrónimo significa “Operationally Critical Theart Asset and Vulnerability Evaluation”, que se basa en tres etapas para llevarse a cabo.

Este método fue desarrollado principalmente para ser implementado en grandes organizaciones y se basa principalmente en la identificación de elementos críticos y amenazas a los activos, la identificación de vulnerabilidades tanto de la organización como tecnológicas, y el desarrollo de una estrategia fundamentada en planes para mitigación de riesgos.

2.2.5. Metodología de análisis de riesgos Magerit

Para la realización de este proyecto se escogió ésta metodología, ya que cuenta con guías estructuradas en tres libros: “El método”, un “Catálogo de Elementos” y una “Guía de Técnicas”, que aportan elementos esenciales a las actividades y objetivos para el desarrollo del análisis de riesgos.

MAGERIT[8] implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Magerit persigue los siguientes objetivos:

Directos:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
2. Ofrecer un método para analizar los riesgos derivados del uso de tecnologías de la información y comunicación (TIC).
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

4. Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

[8] GOBIERNO DE ESPAÑA (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Recuperado de: http://administracionelectronica.gob.es/

2.3. MARCO CONCEPTUAL

Información: El objetivo a proteger en toda organización, es la información, considerada como el activo más importante. Por lo tanto, la seguridad de la información está enmarcada en la preservación de las siguientes propiedades[9]: confidencialidad, disponibilidad e integridad.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos o procesos no autorizados.

Disponibilidad: consiste en que la información pueda ser accedida por los usuarios autorizados.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.

Activos: Son todos aquellos elementos que una organización posee y le genera valor: la información, software, hardware, recursos humanos, servicios, etc.

Vulnerabilidad: Son aquellos puntos débiles que tiene una organización, y que en caso de que se materialice le puede ocasionar pérdidas, en la mayoría de las ocasiones, económicas a la organización.

Amenazas: Es una situación que se puede presentar y puede causarle daño a un activo de la organización.

Riesgo: Indica lo que le podría llegar a pasar a un activo, en el caso de que una amenaza se materialice, causándole daños y pérdidas a la organización.

[9] NTC-ISO-IEC 27001

2.4. MARCO CONTEXTUAL

2.4.1. Identificación

Razón Social: INSITUCIÓN EDUCATIVA DOMINGO SAVIO.

NIT: 860.075.756-1.

Dirección: Calle 25 entre carrera 10 y 11 esquina Florencia – Caquetá.

Teléfono: 8-4376968.

Celular: 321 5232316.

Sitio Web: www.colegiodomingosavio.edu.co

E-Mail: rectoria@colegiodomingosavio.edu.co

Propietario: INSTITUTO HIJAS DE LOS SAGRADOS CORAZONES PROVINCIA CORAZÓN DE JESÚS.

Calendario: A – Mixto.

Jornada: Única.

Niveles Académicos: Educación Preescolar, Básica y Media Académica.

Intensificación: Inglés.

Inscripción ante el MEN: 31800100227

Inscripción DANE: 001-18-00227

Código ICFES: 113720

Aprobación: Resolución N° 787 del 17 de diciembre de 2007 de la Secretaría de Educación Municipal de Florencia – Caquetá.

Certificada: N° ECCO-0025/10 por APPLUS Ltda. Desde el 26 de noviembre de 2010, renovada hasta el 12 de noviembre de 2016.

La información anteriormente suministrada, se encuentra expuesta en el PEI de la I.E Domingo Savio de Florencia Caquetá[10].

[10] INSTITUCIÓN EDUCATIVA DOMINGO SAVIO (2016) Plan Educativo Institucional PEI. Recuperado de: www.colegiodomingosavio.edu.co

2.4.2. Descripción del entorno

La presente información está dada en el Plan Educativo Institucional PEI de la Institución Educativa Domingo Savio[6], y ha sido utilizada únicamente para fines informativos.

La Institución Educativa Domingo Savio, se encuentra ubicada en el municipio de Florencia, Capital del departamento del Caquetá. La ciudad está ubicada en el pie de monte de la cordillera oriental, localizada a los 1°37'30´´ de latitud norte y 75°37'03" de longitud oeste; tiene una altura promedio de 242 msnm una precipitación media anual de 3800 mm y se encuentra a una distancia por vía terrestre de 563 Km. De la Capital de la República.

Su ubicación dentro del municipio de Florencia es sobre la parte Nororiental en el Barrio Torasso alto en la calle 25, entre carreras 10 y 11. La Institución Educativa Domingo Savio, es un centro Católico que promueve la formación integral para niños(as) y jóvenes fundamentados en la espiritualidad salesiana, una escuela de calidad con un espacio físico digno y agradable, respetado y amigable, que funciona al máximo de tiempo para cada alumno, ofreciéndole experiencias significativas, con maestros que tienen una visión común y un sentido de misión, donde se fortalece los valores humanísticos, tecnológicos y culturales para la formación de "Buenos Cristianos y Honestos Ciudadanos".

Los procesos de formación que se desarrollan al interior de la institución están encaminados a una educación de calidad, con el fin de formar ciudadanos solidarios, activos, creativos, responsables, generadores de bien común y de convivencia pacífica y democracia. La opción por una Comunidad Educativa abierta a la participación, a las iniciativas de los educadores, Padres de familia, educandos y comunidad en general.

2.4.3. Reseña histórica

La siguiente reseña histórica está dada en el Plan Educativo Institucional PEI de la Institución Educativa Domingo Savio[6], y ha sido utilizada únicamente para fines informativos[6].

El Instituto Hijas de los Sagrados Corazones de Jesús y de María es una Comunidad Religiosa, Educadora, fundada por el sacerdote Salesiano, Luís Mauricio Variara Bussa, el 07 de Mayo de 1905 en agua de Dios Colombia, con la misión de atender a los enfermos de Hansen, a los niños y a los jóvenes[6].

En Enero de 1950 llega a Florencia la Comunidad Hijas de los Sagrados Corazones, con el fin de recibir la Institución Educativa que se identifica como Institución Educativa Sagrados Corazones, siendo su primera directora la Hermana Evangelina Hernández. El Colegio Domingo Savio aparece en la historia a partir de 1953, cuando se organiza el nivel Preescolar de carácter privado, y funcionó hasta 1992 en las instalaciones de la Institución Educativa Sagrados Corazones[6].

En 1992, siendo Superiora Provincial la Hna. María del Pilar Galeano y Directora de la Comunidad de Florencia la Hermana María Lucia Quiroga, se toma la decisión y se realiza la construcción de la sede propia para el Colegio Domingo Savio. En 1993 se inicia la labor educativa en la sede que actualmente tiene, ubicada en la Calle 25 entre Carreras 10 y 11 Esquina, Barrio Torasso, y la Hna. Rosadelia Velandia direcciona estos pasos en compañía de la Hna. María del Carmen Díaz como Coordinadora, y como docentes las Hnas. Beatriz Toro y Jakeline Bello. Debido a la acogida que tiene el colegio en su proceso de formación a nivel preescolar y ahora con más espacio en su nueva sede, en 1994 se inician labores en Educación Básica Primaria, con dos grupos en grado Primero. Esto constituye el arranque de un nuevo proceso de formación en valores, que día a día se viene consolidando, dando respuesta a una necesidad sentida en la región, y siendo reconocidos por el agregado que se da a la sociedad. Para la Institución Educativa Domingo Savio, educar es motivar y acompañar el crecimiento total de la persona y su compromiso en la creación de una sociedad basada en el amor, la justicia y la paz (CFR. Consta. HHSSCC art. 25)[6].

Para 1995, la Hna. Miryam Fabiola García Pérez llega a direccionar la Institución en compañía de la Hna. Rosa Adela Velandia, Coordinadora Académica y Luz Amparo Santos como Administradora, y en 1996 y 1997 la Institución estuvo bajo la responsabilidad de la Hna. Stella María Ramírez Cobos como Directora, Ana Belén Gamba, Coordinadora Académica y Luz Amparo Santos Administradora[6].

Durante los años 1999 y 2000 la Hna. Elena Alfonso Arias actuó como rectora, la Hna. Jakeline Bello como Coordinadora General y Hna. Blanca Lilia Marulanda C. secretaria, ordenamiento realizado por la Superiora Provincial Hna. María del Pilar Galeano. En los años 2001 y 2002, la Dirección del Colegio está a cargo de la Hna. Elena Alfonso Arias, acompañada de la Hna. Celia García como Coordinadora de disciplina, la Hna. Bernarda Forero como auxiliar contable la Docente Claudia Murcia Cedeño como Coordinadora académica, laborando como secretaria Adriana Dussan Núñez durante el primer año; Para su segundo año, la Coordinación académica y de disciplinaria la desempeño la Docente María Eugenia Sánchez y como secretaria Adriana Dussan Núñez[6].

Durante los años 2003 y 2004, regresa a la dirección del Colegio la Hna. Stella María Ramírez Cobos, con la colaboración de la Hna. Maricela Chaparro en la Coordinación Académica y de disciplina. Se ha de resaltar que para el año 2004, la institución Educativa Domingo Savio ha completado los tres niveles de educación a impartir y como resultado de este proceso se exalta la primera promoción de bachilleres con énfasis en inglés, con un total de nueve egresados[6].

Para el año 2005, se plantea la posibilidad de desarrollar el proceso para la Certificación de Calidad, a través de la fundación Lideres Siglo XXI, MEALS DE COLOMBIA, gestión que se realiza bajo la dirección de la Hna. Stella María Ramírez Cobos y como Coordinadora Académica y Disciplinaria la Hna. Dora Aliria Pastor. Se da la segunda promoción de Bachilleres con énfasis en inglés, con un total de 11 estudiantes[6].

En los siguientes años y hasta su fallecimiento en septiembre de 2011, la dirección de la institución estuvo a cargo de la Hna. Stella María Ramírez Cobos. En sus ideales se encontraba el hecho de ver a la Institución Domingo Savio, Certificada de Calidad, y es por ello que a sus superioras les solicito quedarse en la institución hasta obtener dicho logro y ver que lo planeado se continuara; había comentado que terminado el 2011 se iría para donde la comunidad la requiriera. En dicho periodo se inicia el trabajo de la certificación de calidad, logro que de obtiene en noviembre de 2010 con la resolución ECCOL-0025/2010 expedida por la empresa certificadora Applus-Colombia[6].

Este proceso se llevó a cabo con la colaboración de Hna. Dora Aliria Pastor (Coordinadora en el 2006); Hna. Camila Botero (Coordinadora, 2007), la Hna. Teresa Martínez (Proyecto Pastoral, 2007 y coordinadora disciplina 2008) y la Hna. Delia Toctaguano (docente 2007-2009, coordinadora disciplina 2010); El docente M.Sc. José Antonio Marín Peña (Coordinador Académico 2008-2013), Hna. Hna. Luz Nelly Paipilla Cipagauta (coordinadora de disciplina 2011-2012)[6].

Durante todo el proceso de consolidación y sostenimiento del Sistema de Gestión de Calidad, se dio una participación importante de los docentes que laboran, quienes direccionaban cada una de las gestiones de las cuales se compone el sistema, acciones que se llevaron a cabo con la asesoría en su etapa inicial por la empresa Grupo Gc consultores Ltda. De la ciudad de Bogotá, con el Dr. Carlos Rafael González Contreras en la dirección del mismo, y el acompañamiento del Mg. Juan Alexander Triviño Quiceno, en la coordinación del proyecto de Gestión de Calidad. El Sistema de Gestión de Calidad continúa con su proceso de certificación, al punto que al interior de la institución Educativa, es un pilar del direccionamiento para la planeación, desarrollo, evaluación y se mejora de todas las acciones que se llevan a cabo[6].

Para continuar con el proceso y la sinergia generada por la Hna. Stella María Ramírez Cobos en la Institución, en el 2011, llega la Hna. Martha Inés Silva Quintana, quien proyecto toda su energía de juventud para sacar adelante los proyectos previstos, tal como el de la intensificación en ingles con proyección hacia la consolidación de una institución bilingüe. A de tenerse en cuenta que La comunidad educativa a nivel de padres de familia sigue participando activamente con lo cual la Institución se fortalece y se posiciona como una de las mejores en el Departamento. Su acompañamiento se da hasta Julio de 2013, momento en el cual da paso para que desde Agosto del mismo año, las directrices del accionar académico, pastoral y social en la institución estén en cabeza de la Hna. Yolanda Castellanos Alvarado, quien se pone al frente del proceso de recertificación del Sistema de Gestión de Calidad, proceso en el que su auditoria externa se prevé para octubre de 2013[6].

Ha de reconocerse que desde el año 2004 a la fecha (con excepción del 2005), los resultados de las Pruebas para el Ingreso a la Educación Superior (Prueba Saber 11) realizadas por los estudiantes de la institución ante el ICFES, han obtenido puntajes que ubican a la Institución Educativa Domingo Savio, en el nivel Superior. Es de resaltar que por su desempeño en la prueba, varios estudiantes han obtenido becas por parte de reconocidas universidades tales como la Universidad del Rosario, Universidad Externado de Colombia y Universidad Nacional de Colombia Sede Manizales[6].

Tanto la Misión como la Visión, estás dadas en el Plan Educativo Institucional PEI de la Institución Educativa Domingo Savio6, y ha sido utilizada únicamente para fines informativos[6].

2.4.4. Misión

La Institución Educativa Domingo Savio es un centro Católico que promueve la evangelización de los niños(as), jóvenes y enfermos. Fundamentamos nuestra filosofía en los principios del Carisma Salesiano Victimal. Acompañamos a nuestros destinatarios en su formación integral fortaleciendo la instauración y experiencia de valores humanísticos, trascendentes, tecnológicos y culturales para generar líderes comprometidos y solidarios, capaces de una sana convivencia en diálogo fraterno y en paz con la naturaleza[6].

2.4.5. Visión

Nos proyectamos como una Institución Educativa que continúa certificada de calidad y reconocida por su excelente servicio, comprometida con el desarrollo social y cultural de la región a través de la fundamentación en valores, el desarrollo de las diferentes áreas del conocimiento, y el dominio de una segunda lengua, para formar jóvenes capaces de responder a las exigencias de la globalización y contribuir a la construcción de una sociedad justa, solidaria y fundamentada en los principios filosóficos salesianos de ser: " Buenos Cristianos y Honestos ciudadanos"[6].

2.4.6. Política de calidad

La siguiente política de calidad está dada en el Plan Educativo Institucional PEI de la Institución Educativa Domingo Savio[6], y ha sido utilizada únicamente para fines informativos.

Ofrecer una propuesta educativa evangelizadora, con intensificación en inglés para promover el desarrollo integral de capacidades en los estudiantes hacia el éxito académico y de convivencia. Desarrollar un sistema de gestión de calidad con mejoramiento continuo y eficaz en cada uno de los procesos donde la comunidad intervenga en la formación de personas íntegras, competitivas, capaces de desenvolverse dentro de una sociedad que cada vez se hace más exigente[6].

2.4.7. Objetivos de calidad

Los siguientes objetivos de calidad se encuentran descritos en el Plan Educativo Institucional PEI de la Institución Educativa Domingo Savio[6], y ha sido utilizada únicamente para fines informativos.

- Crear espacios de convivencias fraterna, dinamismo de comunicación y participación para asumir los procesos formativos.

- Realizar acciones que favorezcan el desarrollo integral y armónico de la comunidad educativa para hacer posible la experiencia e instauración de valores humanísticos, trascendentes, tecnológicos y culturales.

- Desarrollar el proyecto de segunda lengua en primera etapa de intensificación para llegar a la meta de institución bilingüe.

- Desarrollar y mantener el proceso de gestión de calidad certificado, actualizando de manera permanentemente, y que se vea reflejado en el mejoramiento continuo de la propuesta pedagógica

2.4.8. Mapa de procesos

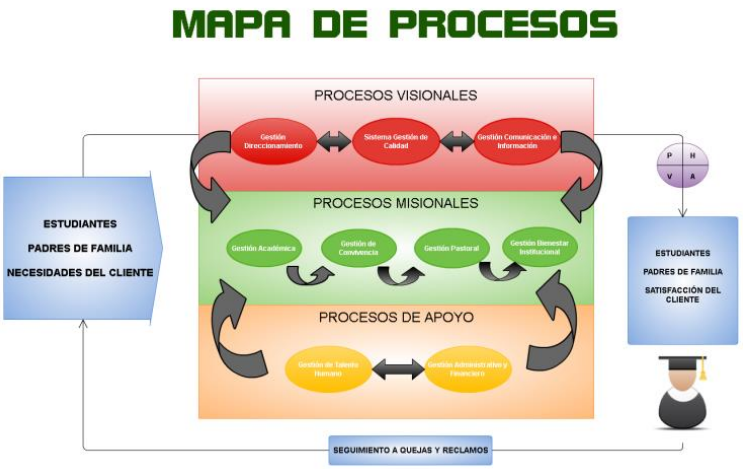


Figura 2. Mapa de procesos Institución Educativa Domingo Savio

Fuente: PEI[6]

2.5. MARCO LEGAL

Existen algunos estándares que brindan herramientas esenciales para el análisis y la gestión de riesgos aplicables para empresas tanto del sector público como del privado, y que brindan ventajas al momento de identificar amenazas y vulnerabilidades en la gestión de activos de información.

ISO 31000: Es una norma internacional que se basa en principios y directrices para la gestión del riesgo. Su flexibilidad le permite ser implementada tanto en pequeñas empresas como en grandes organizaciones del sector público o privado. Es tan versátil que brinda diversas posibilidades de manera sistemática para una oportuna gestión del riesgo, que le permita a la organización cumplir con los objetivos institucionales, por medio del desarrollo, implantación y mejoramiento continuo cuyo objetivo sea integrar el proceso de gestión de riesgo en los procesos de gobierno, de estrategia de planificación, de gestión y de elaboración de informe, así como en las políticas, los valores y en la cultura de toda la organización[11].

OCTAVE: Operationally Critical Theat, Asset and Vulnerability Evaluation (Octave, por sus siglas en inglés), desarrollada por Computer Emergency Response Team (CERT), facilita el análisis de riesgos de una empresa, por medio de tres etapas:

- Construcción de perfiles de amenazas basadas en activos.
- Identificación de vulnerabilidades en la infraestructura.
- Desarrollo de estrategias y planes de seguridad.

Es una metodología enfocada en la gestión de la evaluación del riesgo con el fin de tomar decisiones basadas en los riesgos sobre los activos más críticos de una organización, y con eso asegurar la continuidad del negocio[12].

MAGERIT: Es una metodología para la gestión de riesgos que se enfocaba en las empresas públicas de España, pero que puede implementarse en todo tipo de organizaciones gracias a su versatilidad y que cuenta con guías estructuradas en tres libros: “El método”, un “Catálogo de Elementos” y una “Guía de Técnicas”, que

[11] ISO (2016) ISO 31000 – Gestión de Riesgos: Recuperado de: http://www.iso.org/iso/home/standards/iso31000.htm

[12] ISACA (2010). Metodologías y Normas para el análisis de riesgos: ¿Cuál debo aplicar? Recuperado de: http://www.isaca.org/chapters7/Monterrey/Events/Documents/20100302%20Metodolog%C3%ADas%20de%20Riesgos%20TI.pdf

aportan elementos esenciales a las actividades y objetivos para el desarrollo del análisis de riesgos. También cuenta con una herramienta software denominada PILAR. MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información[13].

ISO 27000: Son una serie de buenas prácticas para la implementación de un Sistema de Gestión de Seguridad de la Información en organizaciones públicas, privadas, grandes o pequeñas. Se basan en una serie de objetivos de control y controles para que las organizaciones determinen su implementación.

LEY 1273 de 2009: Es la ley denominada "De la protección de la Información y de los datos", la cual crea un nuevo bien jurídico para la protección de los sistemas que utilicen tecnologías de la información y la comunicación.

[13] GOBIERNO DE ESPAÑA (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Recuperado de: http://administracionelectronica.gob.es/

3. DISEÑO METODOLÓGICO

MAGERIT (Metodología de Análisis y Gestión del Riesgo de los Sistemas de Información), es una metodología elaborada por el Consejo Superior de Administración Electrónica de España[3]. Esta metodología es una herramienta para el análisis de riesgos en el tratamiento de datos y sistemas informáticos.

Con la metodología MAGERIT se busca analizar el impacto que pueda causar una vulnerabilidad en una organización, así como también, identificar las posibles fallas que se puedan presentar a futuro y poder tomar las medidas preventivas y correctivas más adecuadas.

3.1. TIPO DE INVESTIGACIÓN

En la Escuela de Ciencias Básicas, Tecnología e Ingeniería (ECBTI) de la Universidad Nacional Abierta y a Distancia (UNAD), se encuentran definidas unas líneas de investigación, orientadas para el desarrollo del proyecto de grado de los candidatos a Especialistas en Seguridad Informática. Para este proyecto, se aplicará una metodología de análisis de riesgos, la cual permitirá detectar vulnerabilidad que puedan estar afectando la organización, y a partir de esto, definir una serie de controles que le permitan mitigar el impacto de los riesgos asociados a los activos de información.

A partir del levantamiento de la información de la organización que permita identificar y clasificar activos de información, se diseñará un análisis de riesgos utilizando la metodología Magerit. Seguidamente se propondrá una serie de controles y recomendaciones que le permitan a la organización gestionar la seguridad de la información.

3.2. DISEÑO DE INVESTIGACIÓN

Para desarrollar este trabajo se va a utilizar la Metodología MAGERIT, la cual contempla las siguientes etapas:

ETAPA 1. **Caracterización de Activos**

TAREA 1.1 Identificación de Activos

TAREA 1.2 Dependencia entre activos

TAREA 1.3 Valoración de activos

ETAPA 2. **Caracterización de las amenazas**

TAREA 2.1 Identificación de las amenazas

TAREA 2.2 Valoración de las amenazas

ETAPA 3. **Caracterización de las salvaguardas**

TAREA 3.1 Identificación de las salvaguardas pertinentes

TAREA 3.2 Valoración de las salvaguardas

ETAPA 4. **Estimación del estado del riesgo**

TAREA 4.1 Estimación del Impacto

TAREA 4.2 Estimación del riesgo

3.3. POBLACIÓN

La investigación se realizó en el interior de las instalaciones de la Institución Educativa Domingo Savio, en su única sede ubicada en el Barrio El Torasso de la ciudad de Florencia Caquetá. El análisis de la información se enfocará a las áreas de trabajo de la Institución, principalmente en donde se encuentran los activos de información críticos, en este caso, la Sala de Sistemas, el área de contabilidad, oficina de coordinación académica y de convivencia, oficina de secretaría, sala de profesores y el área de WiFi público que ofrece la institución. En estas oficinas laboran aproximadamente 33 personas, y el WiFi cuanta con aproximadamente 400 usuarios diarios.

3.4. MUESTRA

El análisis de riesgos se realizó en las áreas administrativas de la institución, como oficinas de secretaría, sala de docentes, coordinaciones, rectoría, contabilidad y sala de sistemas.

3.5. FUENTES DE INFORMACIÓN

La información será suministrada por el personal vinculado con la Institución Educativa Domingo Savio, y se describen a continuación:

Nombre: Hna. Eva María Zarta Santos

Cargo: Rectora Institución Educativa Domingo Savio

Funciones: Es la persona encargada de realizar control sobre el cumplimiento de las funciones correspondiente al personal de la Institución.

Nombre: Laura Ligia Céspedes Buitrago

Cargo: Contadora Pública Institución Educativa Domingo Savio

Funciones: Es la persona responsable de las actividades de los procesos relacionados con la Gestión Administrativa y Financiera de la institución.

Nombre: Xiomara Naranjo Pastrana

Cargo: Auxiliar Contable

Funciones: Brindar apoyo a la Gestión Administrativa y Financiera de la Institución.

Nombre: Rocío del Pilar Martínez

Cargo: Secretaria

Funciones: Es la persona encargada de las actividades de los procesos relacionados con la Gestión de Talento Humano, además es coadministrador de la Plataforma de Notas Institucional.

Nombre: Oscar Eduardo Espinosa

Cargo: Ingeniero de Sistemas.

Funciones: Administrador de la Plataforma de Notas Institucional.

3.6. TÉCNICA E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Para el desarrollo de este trabajo de grado se llevaron a cabo diferentes instrumentos que permitieron recolectar la información necesaria para cumplir con los objetivos propuestos. Las técnicas e instrumentos utilizados fueron:

- Cuestionarios.
- Entrevistas.
- Levantamiento de inventarios.
- Inspección visual.
- Registro fotográfico

4. RESULTADOS

4.1. IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

4.1.1. Identificación de los activos críticos de la organización

Mediante la ejecución de esta etapa, se podrá identificar y clasificar los activos relevantes de la organización.

Los activos de información más relevantes para la Institución Educativa Domingo Savio son los siguientes (Anexo D):

GRUPO MAGERIT	NOMBRE DEL ACTIVO	CÓDIGO
SERVICIOS INTERNOS [SERVICE]	Internet	[INTERNET]
	Acceso a gestión de notas	[EXT]
DATOS O INFORMACIÓN [D]	Contraseñas de acceso al sistema	[PASSWORD]
	Copias de Seguridad	[BACKUP]
SOFTWARE [SW]	Antivirus	[AV]
	Office	[OFFICE]
	Sistema operativo	[SO]
HARDWARE [HW]	Equipos de Escritorio	[PC]
	Equipos Portátiles	[MOBILE]
	Impresoras	[PRINT]
	Routers	[ROUTER]
	Switch	[SWITCH]
SOPORTES DE INFORMACIÓN [MEDIA]	Memorias USB	[BACKUP]
	Material Impreso	[VR]

EQUIPAMIENTO AUXILIAR [AUX]	UPS	[UPS]
	Aires Acondicionados	[AC]
	Rack	[RACK]
	Cableado	[CABLING]
REDES DE COMUNICACIONES [COM]	Red Inalámbrica	[WIFI]
	Red Local	[LAN]
INSTALACIONES [L]	Edificio	[BUILDING]
PERSONAL [P]	Usuarios Internos	[UI]
	Administrador de Sistemas	[ADM]
	Operadores	[OP]

Tabla 1. Activos de Información I.E Domingo Savio

Fuente: Autor

4.1.2. Dependencia entre los activos

El objetivo de esta tarea es determinar la dependencia entre los activos más importantes de la organización. Cuando se habla de dependencia, quiere decir que en el momento en que una amenaza sea materializada en un activo inferior, pueda afectar a un activo de orden superior.

Esta dependencia de activos se determinó por medio de una encuesta realizada a los operadores de la institución, por medio del cual se pudo categorizar los activos de información más importantes.

Para la institución es de vital importancia, el sistema de gestión de notas, puesto que en él se registra información que hace parte de los objetivos misionales de la organización.

Los documentos impresos que corresponden en mayor parte al Sistema de Gestión de Calidad, constituyen un nivel superior, puesto que son de vital importancia para la organización.

Los activos inferiores son, los equipos de comunicaciones, que a pesar de representar un apoyo a las operaciones de la organización, no constituyen el cese de los procesos cuando uno de ellos falle.

Finalmente, cabe resaltar que todos los activos de información relevantes de la organización se encuentran resguardados en la misma edificación.

A continuación se muestra el gráfico en donde se representa la dependencia entre los activos de información más relevantes de la organización.

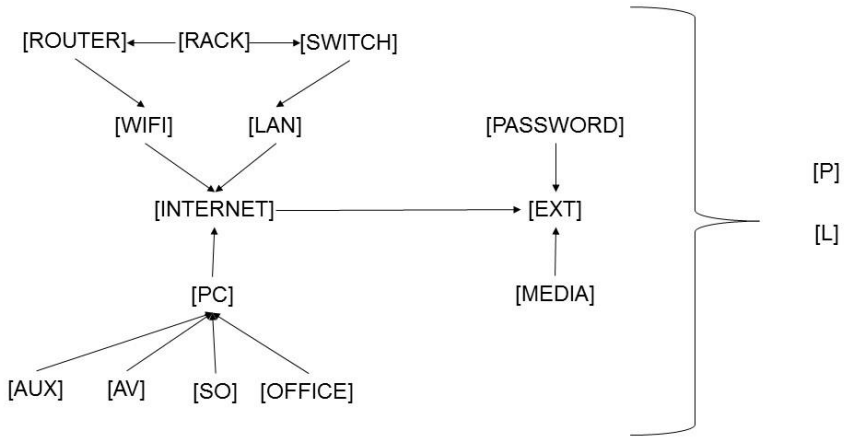


Figura 3. Dependencia entre los activos

Fuente: Autor

4.1.3. Valoración de los activos

El objetivo de esta tarea es determinar la valoración de cada activo de información importante de la organización, con respecto a las dimensiones disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad. Es decir, que se evalúa cada activo sobre las características mencionada anteriormente.

Los criterios de valoración a tener en cuenta, son los establecidos en Magerit Versión 3 – Catalogo de Elementos:

VALOR		CRITERIO
10	Extremo	Daño extremadamente grave
9	Muy Alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a factores prácticos

Tabla 2. Criterios de Valoración

Fuente: Magerit V3 Catálogo de Elementos

Dimensiones de Valoración:

- Disponibilidad [D]
- Integridad [I]
- Confidencialidad [C]
- Autenticidad [A]
- Trazabilidad [T]

GRUPO DE ACTIVO	ACTIVO	DIMENSIONES				
		[I]	[C]	[D]	[T]	[A]
SERVICIOS INTERNOS [SERVICE]	Internet [INTERNET]			[3]	[3]	[3]
	Acceso a gestión de notas [EXT]	[8]	[8]	[9]	[7]	[6]
DATOS O INFORMACIÓN [D]	Contraseñas de acceso al sistema [PASSWORD]	[7]	[9]			[4]
	Copias de Seguridad [BACKUP]	[7]	[7]	[1]		
SOFTWARE [SW]	Antivirus [AV]			[3]		
	Office [OFFICE]			[3]		
	Sistema Operativo [SO]			[3]		
HARDWARE [HW]	Equipos de Cómputo [PC]	[5]		[5]		
	Equipos Portátiles [MOBILE]	[1]		[1]		
	Impresoras [PRINT]			[1]		
	Routers [ROUTER]			[1]	[7]	
	Switch [SWITCH]			[5]	[3]	
SOPORTES DE INFORMACIÓN [MEDIA]	Material Impreso [VR]	[3]	[6]	[3]		
	Memoria USB [BACKUP]		[4]	[3]		

EQUIPAMIENTO AUXILIAR [AUX]	UPS [UPS]			[3]		
	Aires Acondicionados [AC]			[1]		
	Rack [RACK]	[7]				
	Cableado [CABLING]			[3]		
REDES DE COMUNICACIONES [COM]	Red Inalámbrica [WIFI]			[1]	[7]	
	Red Local [LAN]			[5]	[7]	
INSTALACIONES [I]	Edificio [BUILDING]			[9]		
PERSONAL [P]	Usuarios Internos [UI]		[6]	[3]		
	Administrador de Sistemas [ADM]		[6]	[3]		
	Operadores [OP]		[6]	[3]		

Tabla 3. Valoración de los activos de información más relevantes de la institución

Fuente: Autor

Con la anterior información y el análisis y valoración de cada uno de los activos, se tiene como resultado el modelo de valor el cual se encuentra en la sección de anexos.

4.2. ANÁLISIS DE RIESGOS EN LOS ACTIVOS MÁS CRÍTICOS DE LA ORGANIZACIÓN

Para la recolección de la información inicial se realizaron dos encuestas dirigidas al personal de la Institución (Anexo B), los cuales se encuentran encargados de la gestión de la información misional de la institución, los resultados obtenidos y de mayor relevancia fueron los siguientes:

- El 50% de los empleados manifiestan que no reciben mantenimiento periódico a los equipos de cómputo en los cuales se llevan a cabo procesos misionales que incluyen gestión de información.
- El 50% de los empleados manifestaron que solamente reciben mantenimiento anual de los equipos de cómputo.
- El 100% de los empleados respondieron que no existe un tiempo determinado para realizar actualización de los equipos de cómputo de la institución.
- El 50% de los empleados manifiestan que su equipo de cómputo no cuenta con una protección de contraseña.

- El 50% de los empleados respondieron que nunca cambian la contraseña de ingreso de su equipo de cómputo.
- El 100% de los empleados cuentan con conexión a internet, y además que no cuentan con ninguna restricción para su navegación.
- Según la encuesta la institución se ha visto afectada por amenazas naturales tales como, tormentas y sobrecargas eléctricas.
- Los empleados manifiestan que las copias de seguridad de la información de la institución las realizan en la nube y en dispositivos de almacenamientos propios de la institución.
- La encuesta dio como resultados que los empleados de la institución almacenan información reservada y confidencial en los equipos de cómputo.
- El 90% de los empleados saben qué es un hacker.
- El 45,5% de los empleados manifiestan conocer información acerca de mecanismos de protección de información, de los cuales usan: copias de seguridad, antivirus actualizado, firewall, actualizaciones automáticas y navegación segura.

Además se realizó una verificación fotográfica (Anexo c) en la cual se evidenciaron algunos inconvenientes:

- La ubicación no segura de los routers inalámbricos.
- Averías físicas de algunos equipos de cómputo.
- El fácil acceso a equipos auxiliares como routers y switch.
- Fácil acceso al cableado estructurado.

Se tomó un pantallazo (Anexo D) de uno de los equipos de la institución, el cual muestra que el sistema operativo se encuentra activado, pero la organización no cuenta con las debidas licencias. Y también se cuenta con una imagen que evidencia cómo el software de ofimática solicita su activación, y debido a que la institución no cuenta con su licencia lo que podría dejar de funcionar en algún momento.

Teniendo en cuenta la anterior información, se procede a identificar las amenazas sobre los activos críticos identificados en la anterior etapa.

4.2.1. Identificación de amenazas significativas

Para esta actividad se tiene como objetivo la caracterización de las amenazas, identificación y valoración de las mismas.

Para ello se tendrá en cuenta el catálogo de amenazas establecidas en Magerit Versión 3, Catálogo de Elementos.

4.2.1.1. Caracterización de Amenazas

Según Magerit Versión 3, las amenazas se clasifican en cuatro categorías:

- Desastres naturales [N]
- De origen Industrial [I]
- Errores y fallos no intencionados [E]
- Ataques Intencionados [A]

4.2.1.2. Identificación de Amenazas

El objetivo de esta tarea es identificar las amenazas más relevantes que pueden afectar a los activos más representativos de la organización (Anexo C).

GRUPO DE ACTIVO	ACTIVO	AMENAZAS
SERVICIOS INTERNOS [SERVICE]	Internet [INTERNET]	A.7 Uso no previsto A.24 Denegación del servicio
	Acceso a gestión de notas [EXT]	E.1 Errores de los usuarios. A.15 Modificación deliberada de la información.
DATOS O INFORMACIÓN [D]	Contraseñas de acceso al sistema [PASSWORD]	A.5 Suplantación de identidad del usuario.
	Copias de Seguridad [BACKUP]	E.19 Fugas de Información. A.7 Uso no previsto
SOFTWARE	Antivirus [AV]	E.8 Difusión de software dañino.

[SW]		E.20 Vulnerabilidades de los programas (software).
	Office [OFFICE]	I.5 Avería de origen físico o lógico. E.20 Vulnerabilidades de los programas (software). E.21 Errores de mantenimiento / actualización de programas (software).
	Sistema Operativo [SO]	I.5 Avería de origen físico o lógico. E.20 Vulnerabilidades de los programas (software). E.21 Errores de mantenimiento / actualización de programas (software).
HARDWARE [HW]	Equipos de Cómputo [PC]	N.2 Daños por agua I.5 Avería de origen físico o lógico. I.6 Corte del suministro eléctrico. E.23 Errores de mantenimiento / actualización de equipos (hardware).
	Equipos Portátiles [MOBILE]	I.5 Avería de origen físico o lógico.
	Impresoras [PRINT]	I.5 Avería de origen físico o lógico. I.6 Corte del suministro eléctrico.
	Routers [ROUTER]	I.5 Avería de origen físico o lógico. I.6 Corte del suministro eléctrico. A.11 Acceso no autorizado.
	Switch [SWITCH]	I.5 Avería de origen físico o lógico. I.6 Corte del suministro eléctrico. A.11 Acceso no autorizado.
SOPORTES DE INFORMACIÓN [MEDIA]	Material Impreso [VR]	N.* Desastres naturales. E.1 Errores de los usuarios.
	Memoria USB [BACKUP]	I.5 Avería de origen físico o lógico. E.19 Fugas de información. E.25 Pérdida de equipos.
EQUIPAMIENTO AUXILIAR [AUX]	UPS [UPS]	I.* Desastres industriales.
	Aires Acondicionados [AC]	I.* Desastres industriales. I.6 Corte del suministro eléctrico. E.23 Errores de mantenimiento / actualización de equipos (hardware).
	Rack [RACK]	A.11 Acceso no autorizado.
	Cableado [CABLING]	I.* Desastres industriales.
REDES DE	Red Inalámbrica	I.8 Fallo de servicios de

COMUNICACIONES [COM]	[WIFI]	comunicaciones. A.11 Acceso no autorizado. A.24 Denegación del servicio
	Red Local [LAN]	I.8 Fallo de servicios de comunicaciones.
INTALACIONES [I]	Edificio [BUILDING]	N.* Desastres naturales.
PERSONAL [P]	Usuarios Internos [UI]	E.28 Indisponibilidad del personal. A.30 Ingeniería Social.
	Administrador de Sistemas [ADM]	E.28 Indisponibilidad del personal.
	Operadores [OP]	E.28 Indisponibilidad del personal. A.30 Ingeniería Social.

Tabla 4. Identificación de amenazas por cada uno de los activos de información.

Fuente: Autor

4.2.1.3. Valoración de las amenazas

El objetivo fundamental de esta tarea, es determinar la probabilidad de ocurrencia de una amenaza con respecto a cada activo, y especificar la degradación que podría causar la amenaza en cada una de las dimensiones del activo, si ésta se llegara a materializar.

Para evaluar la probabilidad de ocurrencia de cada amenaza, se tendrá en cuenta los siguientes criterios:

VALOR CUALITATIVO	FRECUENCIA	DESCRIPCIÓN
CS	A Diario	Casi Seguro
MA	Cada Semana	Muy Alto
P	Cada Mes	Posible
PP	Cada Año	Poco Probable
MB	Cada Varios Años	Muy Baja
MR	Cada Siglo	Muy Rara

Tabla 5. Probabilidad de Ocurrencia

Fuente: Autor

VALOR CUALITATIVO	DEGRADACIÓN	DESCRIPCIÓN
MA	Desastroso	Muy Alta
A	Mayor	Alta
M	Moderado	Media
B	Menor	Baja
MB	Insignificante	Muy Baja

Tabla 6. Degradación del activo de información

Fuente: Autor

ACTIVOS	AMENAZAS	P	DIMENSIONES				
			[I]	[C]	[D]	[T]	[A]
SERVICIOS INTERNOS [SERVICE]							
Internet [INTERNET]	A.7 Uso no previsto	CS	-	-	B	-	-
	A.24 Denegación del servicio	PP	-	-	A		
Acceso a gestión de notas [EXT]	E.1 Errores de los usuarios.	PP	A	A	-	-	-
	A.15 Modificación deliberada de la información.	MB	A	-	-	-	-
DATOS O INFORMACIÓN [D]							
Contraseñas de acceso al sistema [PASSWORD]	A.5 Suplantación de identidad del usuario.	PP	A	A	-	-	A
Copias de Seguridad [BACKUP]	E.19 Fugas de Información.	MB	-	M	-	-	-
	A.7 Uso no previsto	PP	-	B	-	-	-
SOFTWARE [SW]							
Antivirus [AV]	E.8 Difusión de software dañino.	PP	-	-	B	-	-
	E.20 Vulnerabilidades de los programas (software).	PP	-	-	B	-	-
Office [OFFICE]	I.5 Avería de origen físico o lógico.	PP	-	-	A	-	-
	E.20 Vulnerabilidades de los programas (software).	PP	-	-	A	-	-
	E.21 Errores de mantenimiento / actualización de programas	P	-	-	A	-	-

	(software).						
Sistema Operativo [SO]	I.5 Avería de origen físico o lógico.	PP	-	-	A	-	-
	E.20 Vulnerabilidades de los programas (software).	PP	-	-	A	-	-
	E.21 Errores de mantenimiento / actualización de programas (software).	P	-	-	A	-	-
HARDWARE [HW]							
Equipos de Cómputo [PC]	N.2 Daños por agua	PP	-	-	M	-	-
	I.5 Avería de origen físico o lógico.	P	-	-	M	-	-
	I.6 Corte del suministro eléctrico.	P	-	-	B	-	-
	E.23 Errores de mantenimiento / actualización de equipos (hardware).	PP	-	-	MB	-	-
Equipos Portátiles [MOBILE]	I.5 Avería de origen físico o lógico.	PP	-	-	MB	-	-
Impresoras [PRINT]	I.5 Avería de origen físico o lógico.	MB	-	-	MB	-	-
	I.6 Corte del suministro eléctrico.	P	-	-	MB	-	-
Routers [ROUTER]	I.5 Avería de origen físico o lógico.	PP	-	-	A	-	-
	I.6 Corte del suministro eléctrico.	P	-	-	MB	-	-
	A.11 Acceso no autorizado.	PP	-	-	A	-	-
Switch [SWITCH]	I.5 Avería de origen físico o lógico.	MB	-	-	A	-	-
	I.6 Corte del suministro eléctrico.	P	-	-	MB	-	-
	A.11 Acceso no autorizado.	PP	-	-	A	-	-
SOPORTES DE INFORMACIÓN [MEDIA]							
Material Impreso [VR]	N.* Desastres naturales.	MB	M	-	A	-	-
	E.1 Errores de los usuarios.	MA	A	-	M	-	-
Memoria USB [BACKUP]	I.5 Avería de origen físico o lógico.	MB	-	-	M	-	-
	E.19 Fugas de información.	MB	-	MB	-	-	-

	E.25 Pérdida de equipos.	PP	-	-	MB	-	-
EQUIPAMIENTO AUXILIAR [AUX]							
UPS [UPS]	I.* Desastres industriales.	PP	-	-	M	-	-
Aires Acondicionados [AC]	I.* Desastres industriales.	PP	-	-	M	-	-
	I.6 Corte del suministro eléctrico.	P	-	-	M	-	-
	E.23 Errores de mantenimiento / actualización de equipos (hardware).	PP	-	-	M	-	-
Rack [RACK]	A.11 Acceso no autorizado.	P	-	-	A	M	-
Cableado [CABLING]	I.* Desastres industriales.	MB	-	-	MB	-	-
REDES DE COMUNICACIONES [COM]							
Red Inalámbrica [WIFI]	I.8 Fallo de servicios de comunicaciones.	P	-	-	M	-	-
	A.11 Acceso no autorizado.	MA	-	-	-	A	-
	A.24 Denegación del servicio	MA	-	-	A	-	-
Red Local [LAN]	I.8 Fallo de servicios de comunicaciones.	PP	-	-	M	-	-
INSTALACIONES [L]							
Edificio [BUILDING]	N.* Desastres naturales.	MR	-	-	M	-	-
PERSONAL [P]							
Usuarios Internos [UI]	E.28 Indisponibilidad del personal.	P	-	-	M	-	-
	A.30 Ingeniería Social.	P	-	A	-	-	-
Administrador de Sistemas [ADM]	E.28 Indisponibilidad del personal.	PP	-	-	B	-	-
Operadores [OP]	E.28 Indisponibilidad del personal.	P	-	-	B	-	-
	A.30 Ingeniería Social.	P	-	M	-	-	-

Tabla 7. Valoración de amenazas por activos de información

Fuente: Autor

4.2.2. Se identifican las salvaguardas existentes y se valora la eficacia de su implantación

El objetivo de esta actividad es identificar las salvaguardas oportunas que le permitan a la organización mitigar el riesgo que pueda afectar los activos de información relevantes de la institución. Es decir, que las salvaguardas son mecanismos que permiten que el riesgo sea disminuido, hasta tal punto en que se convierta en insignificante ante un activo de información.

Esta actividad constituye de dos tareas, la identificación de salvaguardas eficaces para la organización y la valoración de estas salvaguardas.

La identificación de salvaguardas se hace con base en la investigación e identificación anterior de los riesgos potenciales y se tiene en cuenta el libro Magerit Versión 3. Catálogo de Elementos.

4.2.2.1. Identificación de Salvaguardas eficaces para la organización

El principal objetivo de esta tarea es la identificación de salvaguardas eficaces y pertinentes que permitan mitigar el riesgo potencial que pueda afectar activos de información relevantes de la institución.

<table>
<tr><td colspan="2">SALVAGUARDA: Protecciones generales u horizontales
[H.tools.AV] Herramienta contra código dañino</td></tr>
<tr><td colspan="2">JUSTIFICACIÓN:
Los equipos de cómputo cuentan con una versión gratuita del antivirus Avast, cuyo tiempo de arranque es excesivo y el motor en segundo plano no es eficaz para máquinas de gama media-baja como con las que se cuenta en la institución.</td></tr>
<tr><td>ACTIVOS EN LOS QUE SE APLICA:
• Software [SW]</td><td>DIMENSIONES:
• Disponibilidad
• Integridad</td></tr>
<tr><td colspan="2">AMENAZAS MITIGADAS:
• E.8 Difusión de software dañino.
• E.20 Vulnerabilidades de los programas (software).
• E.21 Errores de mantenimiento / actualización de programas (software).
• I.5 Avería de origen físico o lógico.</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">SALVAGUARDA: Protección de los datos/información</td></tr>
</table>

<table>
<tr><td colspan="2">[D] Copias de Seguridad de los datos (backup)</td></tr>
<tr><td colspan="2">JUSTIFICACIÓN:
Siendo que para la institución los datos correspondientes a sus clientes directos, que vienen siendo los estudiantes, son de vital importancia, al igual que toda la información generada del Sistema de Gestión de Calidad, se escogió esta salvaguarda ya que en algunas ocasiones la información correspondiente a la gestión de calidad se almacena en dispositivos de almacenamiento propios de los empleados, y cuando éstos se dan de baja de su puesto de trabajo, ésta información en muchas ocasiones se pierde.</td></tr>
<tr><td>ACTIVOS EN LOS QUE SE APLICA:
Datos o Información [D]</td><td>DIMENSIONES:
Confidencialidad
Integridad</td></tr>
<tr><td colspan="2">AMENAZAS MITIGADAS:
E.19 Fugas de Información.
A.7 Uso no previsto.</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">SALVAGUARDA: Protección de los Servicios
[S.A] Aseguramiento de la disponibilidad</td></tr>
<tr><td colspan="2">JUSTIFICACIÓN:
Esta salvaguarda permite que el servicio que presta la institución de red wifi sea prestado con eficacia.</td></tr>
<tr><td>ACTIVOS EN LOS QUE SE APLICA:
Redes de Comunicaciones [COM]</td><td>DIMENSIONES:
Disponibilidad</td></tr>
<tr><td colspan="2">AMENAZAS MITIGADAS:
I.8 Fallo de servicios de comunicaciones
A.24 Denegación del servicio</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">SALVAGUARDA: Protección de los equipos
[HW] Protección de los equipos informáticos</td></tr>
<tr><td colspan="2">JUSTIFICACIÓN:
Se evidencia que algunos equipos informáticos como routers o switch no cuentan con la seguridad, ya que la puerta de ingreso no cuenta con su respectivo seguro, y cualquier persona que ingrese a las instalaciones en donde se encuentran podrían acceder a ellos.</td></tr>
<tr><td>ACTIVOS EN LOS QUE SE APLICA:
Hardware [HW]
Equipamiento auxiliar [AUX]</td><td>DIMENSIONES:
Integridad
Disponibilidad</td></tr>
<tr><td colspan="2">AMENAZAS MITIGADAS:
A.11 Acceso no autorizado.</td></tr>
<tr><td colspan="2"></td></tr>
</table>

SALVAGUARDA: Protección de los equipos [HW.CM] Cambios (actualizaciones y mantenimiento)	
JUSTIFICACIÓN: Esta salvaguarda tiene lugar debido a la respuesta de la encuesta en la que algunos operadores manifestaban la falta de mantenimiento de sus equipos de cómputo con regularidad. Además de la presencia de algunas goteras en la sala de tecnología.	
ACTIVOS EN LOS QUE SE APLICA: • Hardware [HW] • Equipamiento Auxiliar [AUX]	**DIMENSIONES:** • Integridad • Disponibilidad
AMENAZAS MITIGADAS: • N.2 Daños por agua. • I.5 Avería de origen lógico o físico. • E.253 Errores de mantenimiento / actualización de equipos (hardware).	
SALVAGUARDA: Protección de las comunicaciones [COM] Protección de las comunicaciones	
JUSTIFICACIÓN: Debido a que la organización no posee normativa para el uso de los servicios de internet, se produce en muchas ocasiones la caída del servicio en uno de los segmentos de la red wifi, también el acceso no autorizado al uso del servicio por personal externo de la institución debido a que uno de los segmentos se encuentra sin mecanismo de seguridad como contraseña.	
ACTIVOS EN LOS QUE SE APLICA: • Servicios Internos [SERVICE] • Redes de Comunicaciones [COM]	**DIMENSIONES:** • Disponibilidad • Trazabilidad • Autenticidad
AMENAZAS MITIGADAS: • A.7 Uso no previsto. • A.24 Denegación del servicio. • I.8 Fallo de servicios de comunicaciones. • A.11 Acceso no autorizado.	
SALVAGUARDA: Protección de Comunicaciones [COM.DS] Segregación de los redes en dominios	
JUSTIFICACIÓN: Esta salvaguarda permitirá que la red se segregue en dominios lógicos que permitirá que tendrá entre otras ventajas, autenticación de usuarios, limitación de instalación de software no autorizado, monitorización de tráfico y unificación de escritorios.	
ACTIVOS EN LOS QUE SE APLICA:	**DIMENSIONES:**

<table>
<tr><td>

- Servicios Internos [SERVICE]
- Redes de Comunicaciones [COM]
- Software [SW]

</td><td>

- Disponibilidad
- Trazabilidad
- Autenticidad

</td></tr>
<tr><td colspan="2">

AMENAZAS MITIGADAS:

- A.7 Uso no previsto.
- E.8 Difusión de software dañino.
- A.11 Acceso no autorizado.

</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">

SALVAGUARDA: Salvaguardas relativas al personal
[PS.AT] Formación y concientización

</td></tr>
<tr><td colspan="2">

JUSTIFICACIÓN:
Por medio de entrevistas realizadas al personal, se pudo evidenciar la falta de conocimientos con base en seguridad informática, como por ejemplo el desconocimiento de la implementación de mecanismos de seguridad, ingeniería social, etc. También se logró evidenciar que un gran porcentaje de usuarios de la plataforma de notas, no han cambiado nunca su contraseña, lo cual es una amenaza potencial para un ataque por ingeniería social.

</td></tr>
<tr><td>

ACTIVOS EN LOS QUE SE APLICA:

- Personal [P]
- Datos o Información [D]
- Servicios Internos [SERVICE]
- Soportes de información [MEDIA]

</td><td>

DIMENSIONES:

- Confidencialidad
- Autenticidad
- Integridad
- Trazabilidad

</td></tr>
<tr><td colspan="2">

AMENAZAS MITIGADAS:

- A.30 Ingeniería Social.
- A.5 Suplantación de Identidad.
- E.1 Errores de los usuarios.
- A.15 Modificación deliberada de la información.
- E.19 Fugas de Información.

</td></tr>
</table>

Tabla 8. Identificación de Salvaguardas necesarias para los activos de información

Fuente: Autor

4.2.2.2. Valoración de las salvaguardas

El objetivo de esta tarea es especificar la eficacia de las salvaguardas necesarias para los activos de información de la institución.

Para ello se tiene en cuenta el nivel de madurez de las salvaguardas como se define en la siguiente tabla:

EFICACIA	NIVEL	SIGNIFICADO
0%	L0	Inexistente
10%	L1	Inicial
50%	L2	Reproducible, pero intuitivo
90%	L3	Proceso definido
95%	L4	Gestionable y medible
100%	L5	Optimizado

Tabla 9. Eficacia y Madurez de las Salvaguardas

Fuente: Magerit V3 Libro 1. Método

SALVAGUARDA	ACTIVO	DIMENSIÓN					*ESTADO ACTUAL*
		[I]	[C]	[D]	[T]	[A]	
Protecciones generales u horizontales: [H.tools.AV] Herramienta contra código dañino	Software [SW]			X			L4
Protección de los datos/información: [D] Copias de Seguridad de los datos (backup)	Datos e información [D]	X	X				L2
Protección de los Servicios: [S.A] Aseguramiento de la disponibilidad	Redes de comunicaciones [COM]			X	X		L2
Protección de los equipos: [HW] Protección de los	Hardware [HW] Equipamiento Auxiliar [AUX]	X		X			L4

equipos informáticos							
Protección de los equipos: [HW.CM] Cambios (actualizaciones y mantenimiento)	Hardware [HW] Equipamiento Auxiliar [AUX]	X		X			L3
Protección de las comunicaciones: [COM] Protección de las comunicaciones	Servicios Internos [SERVICE] Redes de comunicaciones [COM]			X	X	X	L1
Protección de Comunicaciones: [COM.DS] Segregación de los redes en dominios	Servicios Internos [SERVICE] Redes de comunicaciones [COM] Software [SW]			X	X	X	L0
Salvaguardas relativas al personal: [PS.AT] Formación y concientización	Personal [P] Datos o Información [D] Servicios Internos [SERVICE] Soportes de Información [MEDIA]	X	X	X		X	L0

Tabla 10. Valoración de la eficacia y madurez de las salvaguardas

Fuente: Autor

4.2.3. Se estima el impacto y el riesgo al que están expuestos los activos del sistema

El objetivo de esta actividad es especificar la valoración del impacto que podría causar la materialización de una amenaza, y determinar el riesgo.

Para ello, esta actividad se divide en dos tareas: la determinación del riesgo potencial y del riesgo residual.

El riesgo potencial es todo aquel daño que una amenaza materializada podría causar en los activos de información relevantes de la organización.

El riesgo residual es aquel riesgo que queda sobre los activos de información, luego de haberse establecido un grupo de salvaguardas y aplicado el nivel de madurez o valoración de la eficacia de las salvaguardas.

4.2.3.1. Estimación del impacto

El objetivo de esta tarea es establecer el impacto potencial y residual.

El impacto es la medida del daño que pueda causar la materialización de una amenaza sobre un activo de información relevante de la organización.

El impacto potencial se determina teniendo en cuenta la valoración realizado tanto para los activos, como para las amenazas.

El impacto residual se determina teniendo en cuenta la valoración tanto de los activos como de las amenazas, así como también la eficacia y madurez de las salvaguardas establecidas.

La fórmula para el cálculo del impacto residual es:

$$\text{Impacto residual} = \text{impacto potencial} * (1- e^i)$$

Donde $e^i=0$ significa que las salvaguardas son ineficaces, por lo tanto el impacto es igual. Mientras que $e^i=1$ representa un conjunto de salvaguardas completamente eficaz, lo cual reduciría el impacto residual a cero.

4.2.3.1.1. Impacto Potencial

Como se mencionó anteriormente, para la realización de esta tarea se tendrá en cuenta el valor de los activos en las diferentes dimensiones (integridad, confidencialidad, integridad, trazabilidad y autenticidad), la valoración de la degradación que causan las amenazas sobre los activos de información relevantes en la organización, y de esta manera determinar el impacto que pueda causarse.

A continuación se muestra una escala en la que se clasifica el impacto:

NIVEL DE IMPACTO	VALOR CUANTITATIVO	COLOR
ALTO	10	
	9	
	8	
MEDIO	7	
	6	
	5	
	4	
BAJO	3	
	2	
	1	
	0	

Tabla 11. Clasificación del impacto potencial

Fuente: Autor

GRUPO DE ACTIVO	ACTIVO	DIMENSIONES				
		[I]	[C]	[D]	[T]	[A]
SERVICIOS INTERNOS [SERVICE]	Internet [INTERNET]			[7]	[5]	[5]
	Acceso a gestión de notas [EXT]	[5]	[7]	[1]	[1]	[3]
DATOS O INFORMACIÓN [D]	Contraseñas de acceso al sistema [PASSWORD]	[3]	[5]			[3]
	Copias de Seguridad [BACKUP]	[2]	[4]	[2]		
SOFTWARE [SW]	Antivirus [AV]			[3]		
	Office [OFFICE]			[4]		
	Sistema Operativo [SO]			[4]		
HARDWARE [HW]	Equipos de Cómputo [PC]	[5]		[6]		
	Equipos Portátiles [MOBILE]	[1]		[1]		
	Impresoras [PRINT]			[2]		
	Routers [ROUTER]			[4]	[4]	
	Switch [SWITCH]			[4]	[2]	
SOPORTES DE INFORMACIÓN [MEDIA]	Material Impreso [VR]	[7]	[5]	[7]		
	Memoria USB [BACKUP]		[4]	[1]		
EQUIPAMIENTO AUXILIAR [AUX]	UPS [UPS]			[3]		
	Aires Acondicionados [AC]			[3]		
	Rack [RACK]	[3]				
	Cableado [CABLING]			[3]		
REDES DE	Red Inalámbrica [WIFI]			[5]	[4]	

COMUNICACIONES [COM]	Red Local [LAN]			[6]	[4]	
INTALACIONES [I]	Edificio [BUILDING]			[7]		
PERSONAL [P]	Usuarios Internos [UI]		[7]	[5]		
	Administrador de Sistemas [ADM]		[5]	[2]		
	Operadores [OP]		[6]	[3]		

Tabla 12. Impacto Potencial sobre cada uno de los activos

Fuente: Autor

4.2.3.1.2. Impacto Residual

El impacto residual se calcula teniendo en cuenta el impacto potencial calculado sobre el activo y las salvaguardas establecidas para mitigar las amenazas sobre ese activo.

GRUPO DE ACTIVO	ACTIVO	DIMENSIONES				
		[I]	[C]	[D]	[T]	[A]
SERVICIOS INTERNOS [SERVICE]	Internet [INTERNET]			[0]	[0]	[0]
	Acceso a gestión de notas [EXT]	[1]	[1]	[0]	[0]	[0]
DATOS O INFORMACIÓN [D]	Contraseñas de acceso al sistema [PASSWORD]	[0]	[1]			[0]
	Copias de Seguridad [BACKUP]	[0]	[0]	[0]		
SOFTWARE [SW]	Antivirus [AV]			[0]		
	Office [OFFICE]			[1]		
	Sistema Operativo [SO]			[1]		
HARDWARE [HW]	Equipos de Cómputo [PC]	[1]		[1]		
	Equipos Portátiles [MOBILE]	[0]		[0]		
	Impresoras [PRINT]			[0]		
	Routers [ROUTER]			[0]	[0]	
	Switch [SWITCH]			[0]	[0]	
SOPORTES DE INFORMACIÓN [MEDIA]	Material Impreso [VR]	[5]	[1]	[1]		
	Memoria USB [BACKUP]		[0]	[0]		
EQUIPAMIENTO AUXILIAR	UPS [UPS]			[0]		
	Aires Acondicionados [AC]			[0]		

[AUX]	Rack [RACK]	[1]				
	Cableado [CABLING]			[0]		
REDES DE COMUNICACIONES [COM]	Red Inalámbrica [WIFI]			[1]	[0]	
	Red Local [LAN]			[1]	[0]	
INTALACIONES [I]	Edificio [BUILDING]			[7]		
PERSONAL [P]	Usuarios Internos [UI]		[3]	[1]		
	Administrador de Sistemas [ADM]		[1]	[1]		
	Operadores [OP]		[2]	[1]		

Tabla 13. Impacto Residual sobre cada uno de los activos

Fuente: Autor

4.2.3.2. Estimación del riesgo

Los objetivos de esta tarea son determinar tanto el riesgo potencial como residual al cual están expuestos los activos de información.

Para determinar el riesgo potencial al cual están expuestos los activos de información relevantes de la organización, se tendrá en cuenta la valoración que se hace sobre los activos en cada una de las dimensiones y la valoración de las amenazas.

El riesgo residual se determina teniendo en cuenta tanto el valor de los activos en cada una de las dimensiones, la valoración de las amenazas y la eficacia de las salvaguardas pertinentes para cada activo.

Para realizar el cálculo del riesgo residual se emplea la siguiente fórmula:

Riesgo residual = impacto residual * frecuencia residual

4.2.3.2.1. Riesgo potencial

Como se mencionó anteriormente, el riesgo potencial se determina teniendo en cuenta la valoración de los activos y de las amenazas. El riesgo es aquel daño que los activos de información podrían sufrir al materializarse una amenaza.

Para ello, se clasificará el riesgo teniendo en cuenta la siguiente escala de colores:

RIESGO	VALOR CUANTITATIVO	COLOR
ALTO	10	
	9	
	8	
	7	
MEDIO	6	
	5	
	4	
	3	
BAJO /DESPRECIABLE	2	
	1	
	0	

Tabla 14. Clasificación del Riesgo Potencial

Fuente: Autor

GRUPO DE ACTIVO	ACTIVO	DIMENSIONES				
		[I]	[C]	[D]	[T]	[A]
SERVICIOS INTERNOS [SERVICE]	Internet [INTERNET]			[7, 6]	[5, 6]	[5, 6]
	Acceso a gestión de notas [EXT]	[5, 4]	[7, 4]	[1, 4]	[1, 4]	[3, 4]
DATOS O INFORMACIÓN [D]	Contraseñas de acceso al sistema [PASSWORD]	[3, 2]	[5, 2]			[3, 2]
	Copias de Seguridad [BACKUP]	[2, 1]	[4, 1]	[2, 1]		
SOFTWARE [SW]	Antivirus [AV]			[3, 4]		
	Office [OFFICE]			[4, 4]		
	Sistema Operativo [SO]			[4, 4]		
HARDWARE [HW]	Equipos de Cómputo [PC]	[5, 5]		[6, 5]		
	Equipos Portátiles [MOBILE]	[1. 1]		[1, 1]		
	Impresoras [PRINT]			[2, 2]		
	Routers [ROUTER]			[4, 5]	[4, 5]	
	Switch [SWITCH]			[4, 4]	[2, 4]	
SOPORTES DE INFORMACIÓN [MEDIA]	Material Impreso [VR]	[7, 8]	[5, 8]	[7, 8]		
	Memoria USB [BACKUP]		[4, 2]	[1, 2]		
EQUIPAMIENTO AUXILIAR	UPS [UPS]			[3, 4]		
	Aires Acondicionados [AC]			[3, 4]		

[AUX]	Rack [RACK]	[3, 6]				
	Cableado [CABLING]			[3, 1]		
REDES DE COMUNICACIONES [COM]	Red Inalámbrica [WIFI]			[5, 7]	[4, 7]	
	Red Local [LAN]			[6, 4]	[4, 4]	
INTALACIONES [I]	Edificio [BUILDING]			[7, 0]		
PERSONAL [P]	Usuarios Internos [UI]		[7, 7]	[5, 7]		
	Administrador de Sistemas [ADM]		[5, 4]	[2, 4]		
	Operadores [OP]		[6, 5]	[3, 5]		

Tabla 15. Riesgo Potencial sobre cada uno de los activos

Fuente: Autor

4.2.3.2.2. Riesgo Residual

El riesgo residual es el resultado de la estimación de una amenaza cuando afecta a un activo de orden superior que depende de dicho activo. La siguiente tabla muestra los resultados obtenidos del riesgo residual acumulado, los resultados en rojo, son aquellos riesgos Altos.

GRUPO DE ACTIVO	ACTIVO	DIMENSIONES				
		[I]	[C]	[D]	[T]	[A]
SERVICIOS INTERNOS [SERVICE]	Internet [INTERNET]			[0, 2]	[0, 2]	[0, 2]
	Acceso a gestión de notas [EXT]	[1, 3]	[1, 3]	[0, 3]	[0, 3]	[0, 3]
DATOS O INFORMACIÓN [D]	Contraseñas de acceso al sistema [PASSWORD]	[0, 1]	[1, 1]			[0, 1]
	Copias de Seguridad [BACKUP]	[0, 0]	[0, 0]	[0, 0]		
SOFTWARE [SW]	Antivirus [AV]			[0, 2]		
	Office [OFFICE]			[1, 2]		
	Sistema Operativo [SO]			[1, 2]		
HARDWARE [HW]	Equipos de Cómputo [PC]	[1, 3]		[1, 3]		
	Equipos Portátiles [MOBILE]	[0, 0]		[0, 0]		
	Impresoras [PRINT]			[0, 1]		
	Routers [ROUTER]			[0, 3]	[0, 3]	
	Switch [SWITCH]			[0, 2]	[0, 2]	
SOPORTES DE INFORMACIÓN [MEDIA]	Material Impreso [VR]	[5, 6]	[1, 6]	[1, 6]		
	Memoria USB [BACKUP]		[0, 0]	[0, 0]		

EQUIPAMIENTO AUXILIAR [AUX]	UPS [UPS]			[0, 2]		
	Aires Acondicionados [AC]			[0, 2]		
	Rack [RACK]	[1, 3]				
	Cableado [CABLING]			[0, 0]		
REDES DE COMUNICACIONES [COM]	Red Inalámbrica [WIFI]			[1, 5]	[0, 5]	
	Red Local [LAN]			[1, 3]	[0, 3]	
INTALACIONES [I]	Edificio [BUILDING]			[7, 0]		
PERSONAL [P]	Usuarios Internos [UI]		[3, 5]	[1, 5]		
	Administrador de Sistemas [ADM]		[1, 3]	[1, 3]		
	Operadores As		[2, 3]	[1, 3]		

Tabla 16. Riesgo Residual sobre cada uno de los activos

Fuente: Autor

4.2.4. Interpretación de los resultados

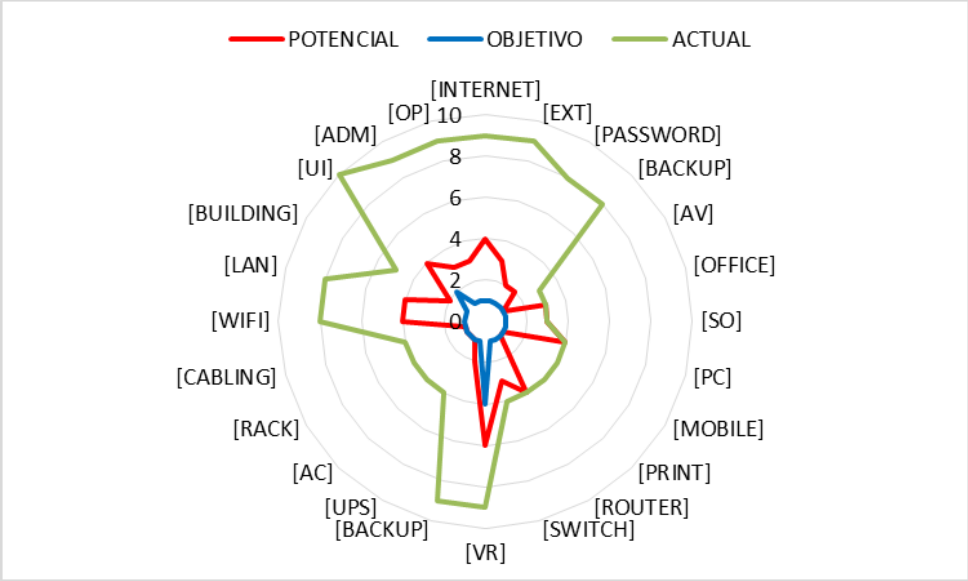


Figura 4. Identificación de riesgos

Fuente: Autor

Como resultado de la etapa de análisis de riesgos se genera la figura 4. Identificación de Riesgos. En la figura se puede evidenciar, que los activos que poseen un nivel de riesgo potencial más alto son:

- Internet [INTERNET]
- Sistema Operativo [SO]
- Equipos de cómputo [PC]
- Router [ROUTER]
- Material Impreso [VR]
- Red Inalámbrica [WIFI]
- Red Local [LAN]
- Usuario Interno [UI]

El objetivo de identificar los activos con mayor nivel de riesgo, es establecer estrategias que permitan mitigar ese riesgo en la siguiente fase, la cual es la Gestión de Riesgos.

4.3. GESTIÓN DE RIESGOS

Una vez realizado el proceso de análisis de riesgos, en la cual se establecieron los impactos de la materialización de una amenaza y los riesgos que puedan afectar los activos de información de la organización.

Ya habiéndose hecho una clasificación del riesgo, se procede a identificar el tratamiento eficaz, teniendo en cuenta la información de la siguiente tabla:

RIESGO	VALOR CUANTITATIVO	COLOR	TRATAMIENTO
ALTO	10		Crítico, atención urgente
	9		
	8		
	7		Grave, requiere atención
MEDIO	6		
	5		
	4		Apreciable, puede ser objeto de estudio para su tratamiento
	3		
BAJO /DESPRECIABLE	2		Asumible, no requiere acciones
	1		

	0		

Tabla 17. Clasificación de cada riesgo para su tratamiento

Fuente: Autor

4.3.1. Se elige una estrategia para mitigar impacto y riesgo

El objetivo de esta actividad es determinar los riesgos críticos, es decir, aquellos riesgos que pueden impactar a los activos de información de la institución de manera negativa.

Cabe resaltar que los activos de información relevantes para una organización siempre van a estar expuestos a riesgos, que puedan afectar su integridad, confidencialidad y disponibilidad. Es de vital importancia determinar cuáles de esos activos representan mayor valor para la organización, para de esta manera poder implementar las salvaguardas pertinentes, con el objetivo de minimizar la probabilidad de que una amenaza se materialice.

Una vez realiza la etapa de análisis de riesgos, la primera estrategia para la realización de esta actividad es la identificación de los riesgos críticos, los cuales se encuentran resumidos en la siguiente tabla:

GRUPO DE ACTIVO	ACTIVO	DIMENSIONES					NIVEL DE RIESGO
		[I]	[C]	[D]	[T]	[A]	
SERVICIOS INTERNOS [SERVICE]	Internet [INTERNET]			[0, 2]	[0, 2]	[0, 2]	Apreciable, puede ser objeto de estudio para su tratamiento
SOFTWARE [SW]	Sistema Operativo [SO]			[1, 2]			Apreciable, puede ser objeto de estudio para su tratamiento
HARDWARE [HW]	Equipos de Cómputo [PC]	[1, 3]		[1, 3]			Apreciable, puede ser objeto de estudio para su tratamiento
	Routers [ROUTER]			[0, 3]	[0, 3]		Apreciable, puede ser objeto de estudio para su tratamiento
SOPORTES DE INFORMACIÓN [MEDIA]	Material Impreso [VR]	[5, 6]	[1, 6]	[1, 6]			Grave, requiere atención
REDES DE	Red			[1, 5]	[0, 5]		Apreciable, puede ser objeto de

COMUNICACIONES [COM]	Inalámbrica [WIFI]						estudio para su tratamiento
	Red Local [LAN]			[1, 3]	[0, 3]		Apreciable, puede ser objeto de estudio para su tratamiento
PERSONAL [P]	Usuarios Internos [UI]		[3, 5]	[1, 5]			Apreciable, puede ser objeto de estudio para su tratamiento

Tabla 18. Identificación de Riesgos Críticos

Fuente: Autor

4.3.2. Se determinan las salvaguardas oportunas para el objetivo anterior

El objetivo de esta actividad es gestionar aquellos activos cuyos riesgos críticos fueron identificados en la etapa anterior.

- Internet [INTERNET]: este activo de información pertenece al grupo de Servicios Internos [SERVICE], los resultados obtenidos tras el análisis de riesgos fueron los siguientes:
    - La amenaza que mayor lo afecta es el A.7 Uso no previsto, la cual afecta la disponibilidad (0,2), la trazabilidad (0,2) y la autenticación (0,2). La materialización de esta amenaza podría afectar negativamente las actividades diarias de la organización, como por ejemplo, rendimiento del personal, ingreso a la página institucional, uso de e-mail, entre otras. Las medidas que podrían llevarse a cabo para reducir el riesgo potencial es:
        - La configuración de la conexión a internet mediante un servidor proxy, el cual le permitirá la restricción de acceso a páginas como redes sociales, descargar de programas no autorizados, es decir, que se restrinja solo a actividades laborales, y se prevenga la difusión de software dañino.

- Sistema Operativo [SO]: este activo de información pertenece al grupo de Software [SW], y los resultados obtenidos tras el análisis de riesgos fueron los siguientes:
    - La amenaza que afecta este activo de información es E.21 Errores de mantenimiento / actualización de programas (software), afectando la

disponibilidad (1,2). La materialización de esta amenaza podría afectar actividades propias de la organización como por ejemplo, la generación de informes, la digitación de procedimientos y formatos del Sistema de Gestión de Calidad, y la utilización de equipos en la sala de informática. Además, que la institución no cuenta con licencias para el uso del sistema operativo instalado en los equipos y en cualquier momento podría conllevar a inconvenientes de tipo legal. Las medidas que podrían llevarse a cabo para mitigar esta amenaza son:

- Un estudio de factibilidad en cuanto a la adquisición de un Campus Agreement, el cual es un programa que le permitirá a la Institución obtener el licenciamiento de manera legal de los servicios de Microsoft y de manera flexible en cuanto a costos.
- La instalación de parches y actualizaciones, una vez licenciado el software, estas características le garantizará al equipo características de seguridad que solo las actualizaciones pueden ofrecerle.

- Equipos de Cómputo [PC]: este activo de información pertenece al grupo de Hardware [HW], y los resultados obtenidos tras el análisis de riesgos fueron los siguientes:
  - La amenaza que mayor afecta a este activo es E.23 Errores de mantenimiento / actualización de equipos (hardware), afectando la integridad (1,3) y la disponibilidad (1,3). La materialización de esta amenaza podría afectar la ejecución de actividades propias de la organización como la generación de informes, las actividades relacionadas con el Sistema de Gestión de Calidad, y otras de tipo administrativo. Las medidas que podrían llevarse a cabo para mitigar esta amenaza son:
    - El resguardo contra algunas amenazas de tipo ambiental como por ejemplo, el agua.
    - Un cronograma de mantenimiento mensual, que permita una revisión constante preventivo.
    - Un programa de Gestión Tecnológica gestionable y medible, que permita identificar los requerimientos de tecnología de la institución, al igual que la asignación de recursos para el mismo.

- Routers [ROUTER]: este activo de información pertenece al grupo de Hardware [HW], y en cuanto a la realización del análisis de riesgos, se obtuvieron los siguientes resultados:

- La amenaza que mayor afecta a este activo es A.11 Acceso no autorizado, que podría afectar la disponibilidad (0,3) y la trazabilidad (0,3). La materialización de esta amenaza, podría afectar la prestación de algunos servicios internos, además podría estar expuesto a robos o a averías deliberadas. Las medidas que podrían llevarse a cabo para mitigar esta amenaza son:
  - La implementación de mecanismos de seguridad eficaces para el resguardo de estos activos, como por ejemplo, cerradura.
  - El cambio de la ubicación de algunos routers con el fin de evitar averías físicas.

- Material Impreso [VR]: este activo de información hace parte del grupo Soportes de información [MEDIA]. Los resultados del análisis de riesgos fueron los siguientes:
  - La amenaza que afecta en mayor grado a este activo es E.1 Errores de los usuarios, que podría afectar la integridad (5,6), confidencialidad (1,6) y disponibilidad (1,6). La materialización de esta amenaza podría afectar directamente el Sistema de Gestión de Calidad de la organización, ya que de la integridad de sus archivos, depende la confianza transmitida a los clientes, y también, la certificación de sus procesos por organismos externos. Las medidas que podrían llevarse a cabo para mitigar esta amenaza son:
    - La sistematización de algunos procedimientos y formatos de la gestión, que generen resultados automáticos, los cuales permitirá un análisis más eficaz de resultados.
    - La concientización y capacitación permanente a los empleados de la institución, con el fin de prevenir los errores constantes en el diligenciamiento de los formatos.

- Red inalámbrica [WIFI] y Red Local [LAN]: estos dos activos de información pertenecen al grupo de Redes de comunicaciones [COM], los resultados obtenidos en la etapa de análisis de riesgos es la siguiente:
  - Las amenazas que afectan en mayor medida estos dos activos de información es I.8 Fallo de servicios de comunicaciones y A.11 Acceso no autorizado, afectando la disponibilidad (1,5) y trazabilidad (0,5). La materialización de esta amenaza puede afectar algunos procesos y operaciones que realiza esta institución, además de no ofrecer el servicio de una manera óptima. Además, la institución se enfrenta a situaciones en donde personas externas a la organización acceden de manera directa al

servicio de red inalámbrica, lo cual podría ocasionar distribución de software dañino. Para ello se han establecido las siguientes medidas:

- Mantenimientos regulares tanto a la red inalámbrica como inalámbrica.
- Implementar una herramienta que permita el análisis del tráfico de la red.
- La implementación de un servidor de dominios para controlar los niveles de seguridad entre grupos de usuarios, el acceso a los servicios tales como la red inalámbrica, el control de la instalación de software no autorizado. Es decir, el objetivo es lograr una administración de la red tanto alámbrica como inalámbrica de la institución de manera centralizada, que brinde un método único de acceso identificando de esta manera a los usuarios no autorizados, garantizando la capacidad de la red.

- Usuarios Internos [UI]: este activo de información hace parte del grupo Personal [P], cuyos resultados obtenidos de la etapa de análisis de riesgos es las siguientes:
  - La amenaza que más afecta a este activo es A.30 Ingeniería social, influyendo en la confidencialidad (3,5) y disponibilidad (1,5). La amenaza tiene que ver con acciones relacionadas principalmente con la seguridad al ingreso de la plataforma de notas, ya que los usuarios manifiestan que no cumplen con el cambio de la contraseña para el ingreso del vortal. La materialización de esta amenaza conlleva grandes riesgos como por ejemplo, suplantación de identidad, revelación de información confidencial, pérdida de credibilidad y reputación de la institución, entre otras. Las acciones que podría implementarse para la mitigación de esta amenaza son:
    - Creación, comunicación e implementación de una política de contraseñas seguras y de otros mecanismos de seguridad con respecto a la prevención de la ingeniería social.
    - Crear un procedimiento gestionable y medible acerca de los incidentes de seguridad de la información ocurridos en la institución.

4.3.3. Se determina la calidad necesaria para dichas salvaguardas

El objetivo de esta actividad es establecer el nivel de eficacia de las salvaguardas planteadas en la actividad anterior.

SALVAGUARDA	ACTIVO	DIMENSIÓN					ESTADO DESEABLE	
		[I]	[C]	[D]	[T]	[A]		
Protecciones generales u horizontales: [H.tools.AV] Herramienta contra código dañino	Software [SW]			X			L5	Optimizado
Protección de los datos/información: [D] Copias de Seguridad de los datos (backup)	Datos e información [D]	X	X				L4	Gestionable y Medible
Protección de los Servicios: [S.A] Aseguramiento de la disponibilidad	Redes de comunicaciones [COM]			X	X		L4	Gestionable y Medible
Protección de los equipos: [HW] Protección de los equipos informáticos	Hardware [HW] Equipamiento Auxiliar [AUX]	X		X			L5	Optimizado
Protección de los equipos: [HW.CM] Cambios (actualizaciones y mantenimiento)	Hardware [HW] Equipamiento Auxiliar [AUX]	X		X			L4	Gestionable y Medible
Protección de las comunicaciones: [COM] Protección de las comunicaciones	Servicios Internos [SERVICE] Redes de comunicaciones [COM]			X	X	X	L4	Gestionable y Medible
Protección de Comunicaciones: [COM.DS] Segregación de los redes en dominios	Servicios Internos [SERVICE] Redes de comunicaciones [COM] Software [SW]			X	X	X	L5	Optimizado

Salvaguardas relativas al personal: [PS.AT] Formación y concientización	Personal [P] Datos o Información [D] Servicios Internos [SERVICE] Soportes de Información [MEDIA]	X	X	X		X	L4	Optimizado

Tabla 19. Eficacia deseable de las salvaguardas establecidas

Fuente: Autor

4.3.4. Plan de Seguridad (Estrategias de Mejora)

El objetivo de esta actividad del proyecto, es establecer un plan de seguridad, es decir, unas estrategias de mejora que permita materializar los resultados obtenidos en la gestión de riesgos.

Las tareas a realizar en esta actividad son, la identificación de proyectos de seguridad, el plan de ejecución y la ejecución. Como se estableció en la planeación de este proyecto, no se va a llevar a cabo la ejecución del plan de seguridad, puesto que éste Plan de Seguridad se plantea ante la alta gerencia de la Institución, y la decisión de implementarlo total o parcialmente, es única y exclusivamente de ellos.

4.4. POLÍTICAS DE SEGURIDAD

Como objetivo de esta tarea está el establecer un Programa de Seguridad o Estrategias de Mejora de Seguridad, que le permita a la organización mitigar el impacto y la probabilidad de ocurrencia que pueda causar una amenaza sobre un activo de información relevante de la organización.

4.4.1. Plan de Seguridad

- **Políticas de Seguridad para el Uso de Internet:**

  - El servicio de internet es provisto por la Gestión administrativa de la Institución, y por tanto, debe ser utilizado única y exclusivamente para fines organizacionales, y el desempeño de las funciones asignadas.
  - Los usuarios de los equipos de cómputo de la institución tienen completamente prohibido la descarga e instalación de software no autorizado.
  - Quedan estrictamente prohibidas las redes de todo tipo como, redes sociales, sitios con contenido sexual, sitios con contenidos que inciten a la violencia de cualquier tipo, descarga de software ilegal o sitios que generen un consumo elevado de recursos de red como streaming.
  - La institución tiene la facultad de bloquear cualquier tipo de tráfico de red no autorizado o por usuarios no autorizados.
  - Es de completa responsabilidad del usuario, cualquier tipo de daño ocasionado por contenidos no apropiados y no autorizados.

- **Políticas de Seguridad para el Uso de Aplicaciones:**

  - Se prohibirá completamente la instalación de software de cualquier índole.
  - Los usuarios deberán verificar la información que almacenan en dispositivos de almacenamiento externos, con el fin de prevenir infecciones con software dañino en los equipos de cómputo de propiedad de la institución.
  - Estudio de factibilidad de adquisición de licenciamiento de software tanto de sistema operativo como de ofimática. Los usuarios no usarán copias no

autorizadas de software, ni tampoco harán uso personal de licencias o software de tipo propietario de la institución.

- La actualización e instalación de parches de seguridad, será responsabilidad única y exclusivamente de la Gestión Administrativa de la Institución.

- **Políticas de Seguridad para la Gestión de Equipos de Cómputo y otro tipo de Hardware:**

  - Cada equipo de cómputo que haga parte del inventario de la Institución Educativa Domingo Savio, tendrá un usuario responsable que se especificará en la hoja de vida de los equipos.
  - Los usuarios responsables de los equipos no podrán mover, trasladar, dar de baja, desconectar / agregar periféricos, ya que esto será competencia de personal autorizado.
  - Solo el personal idóneo y autorizado puede llevar a cabo mantenimientos, reparaciones e instalación de software y hardware de los equipos de cómputo.
  - Queda completamente prohibido el consumo tanto de alimentos como de bebidas durante el uso de equipos de cómputo de la institución. De igual forma, es de responsabilidad del usuario, mantener el equipo de cómputo en un ambiente libre de humedad, polvo, y garantizar un entorno limpio para el activo. En caso de ocurrir un daño producido por las acciones anteriormente mencionadas o por negligencia del empleado, éste está en la obligación de cubrir los gastos de reparación de la máquina.
  - Se establecerá un programa mensual de mantenimiento preventivo y correctivo de los equipos de cómputo, que pueda ser gestionable y medible.
  - Se instaurará programa de Gestión Tecnológica gestionable y medible, que permita identificar los requerimientos de tecnología de la institución, al igual que la asignación de recursos para el mismo.
  - Implementación de mecanismos de seguridad eficientes para el resguardo de activos de información, en el caso de racks, la revisión y seguridad de este equipamiento auxiliar.

- **Políticas de Seguridad para Resguardo y Protección de la Información:**

    - El resguardo de la información se hará en dos ubicaciones: local y fuera de sitio. La primera se realizará en los equipos de cómputo de la organización, el segundo resguardo se hará en almacenamiento en la nube con cuentas propias de la institución, en donde los usuarios y contraseñas sean administrados por rectoría. La frecuencia del respaldo será cada semana.
    - Para el caso de la información crítica de la organización, los empleados que tengan acceso a ella, tendrán que resguardar esta información mínimo con frecuencia diaria, tanto en la ubicación local o de su equipo, como en una cuenta propia de la institución en la nube.
    - La documentación impresa relacionada con el Sistema de Gestión de Calidad estará completamente rotulada, discriminada por Proceso, y tendrá como ubicación las oficinas de la Institución, resguardadas de amenazas ambientales, como humedad, fuego, entre otras.

- **Políticas de Seguridad Referentes al Personal:**

    - Establecer, documentar y comunicar roles de responsabilidad con respecto a la seguridad de la información que incluya:
        - Verificación de antecedentes a candidatos de empleo, contratistas y terceros.
        - La clasificación de la información a la que tenga acceso cada empleado.
        - Establecimiento de cláusulas de confidencialidad, términos y condiciones en el documento del contrato.
        - Proceso formal disciplinario para empleados que generen incidentes graves de seguridad.
    - Un programa de capacitación y formación con relación a seguridad de la información con el fin de prevenir incidentes de seguridad ocasionados por Ingeniería social.
    - Establecer una política formal, gestionable y medible para la gestión de contraseñas de usuarios para el ingreso a la plataforma de notas.

5. CONCLUSIONES

Las conclusiones que se pudieron obtener al desarrollar el presente proyecto fueron las siguientes:

Se cumplieron todos los objetivos propuestos en el presente proyecto, teniendo en cuenta que a través de la aplicación de la metodología MAGERIT se estableció unas Políticas de Seguridad, cuyo fin era determinar una serie de estrategias que le permitieran a la institución estar preparados ante incidentes o eventualidades relacionadas con la seguridad de la información.

Se realizó el proceso de identificación y clasificación de activos relevantes de la institución, determinando su dependencia y su valoración. Con ello se logró determinar los activos de información con los cuales se continuó a la etapa de análisis de riesgos.

El análisis de riesgos de la institución permitió determinar que como toda organización, se presentan brechas de seguridad que pueden repercutir negativamente en los activos de información relevantes, por lo tanto, fue una etapa determinante del proyecto para poder establecer las estrategias de mejora. Por medio de diferentes técnicas de recolección de información se determinaron algunas amenazas relevantes como:

- La inexistencia de una política de contraseñas seguras para la autenticación en la plataforma de notas de la institución.
- Las contraseñas para el ingreso a la plataforma institucional de publicación de notas, no son confidenciales, lo cual puede ocasionarle a la institución problemas de seguridad de la información.
- Ubicación inadecuada de equipos de comunicaciones, y de igual forma, mecanismos de seguridad inexistentes en algunos gabinetes de red.
- Los respaldos de información realizados por algunos empleados en medios de almacenamientos propios del empleado, por lo que cuando abandonan su puesto de trabajo, la institución se ha visto perjudicada por la pérdida de información, generalmente concerniente al Sistema de Gestión de Calidad.

Como resultado de la ejecución de este proyecto, la alta gerencia de la Institución Educativa Domingo Savio, obtuvo un informe técnico en donde se presentaron elementos importantes encontrados, así como también se estableció una Política de Seguridad aplicable para la organización, que le permita mitigar el impacto y la probabilidad de ocurrencia que pueda causar una amenaza sobre un activo de información crítico de la institución. Cabe destacar, que por políticas de la institución, la implementación de loa política de seguridad queda a completa disposición de la alta gerencia.

6. RECOMENDACIONES

Se recomienda capacitación y concientización acerca de la Seguridad de la Información a los empleados de la organización, ya que muchas de las brechas de seguridad encontradas, se deben a la falta de conocimiento sobre seguridad de algunos de los empleados.

Se sugiere establecer, documentar y medir un procedimiento para el tratamiento de incidentes de seguridad que involucren los activos de información. Además, que este procedimiento permita una revisión periódica de amenazas y riesgos que se puedan materializar. Todo ello, articulado con el Sistema de Gestión de Calidad con el que cuenta la institución.

De igual forma, se sugiere el establecimiento del departamento de informática, como parte de los procesos de apoyo de la organización, en el cual se puedan gestionar los incidentes de seguridad, los programas de mantenimiento y todo lo relacionado con los activos de información de la institución.

REFERENCIAS

A GÓMEZ VIEITES, Seguridad en Equipos Informáticos, RA-M, A Editorial, 2014.

ANDRÉS, A., & GÓMEZ, L. (2009). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes.

G.R.S.R.M.R.D.J. Escrivá Gascó, Seguridad Informática, Macmillan Iberia, S.A., 2013.

CONGRESO DE LA REPÚBLICA (2009). Ley 1273: De la protección de la información y los datos. Recuperado de: http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf

ISACA (2010). Metodologías y Normas para el análisis de riesgos: ¿Cuál debo aplpicar? Recuperado de: http://www.isaca.org/chapters7/Monterrey/Events/Documents/20100302%20Metodolog%C3%ADas%20de%20Riesgos%20TI.pdf

INSTITUCIÓN EDUCATIVA DOMINGO SAVIO (2016) Plan Educativo Institucional PEI. Recuperado de: www.colegiodomingosavio.edu.co

ISO (2016) ISO 31000 – Gestión de Riesgos: Recuperado de: http://www.iso.org/iso/home/standards/iso31000.htm

MINISTERIO DE ADMINISTRACIÓN PÚBLICAS (2012). MAGERIT- Versión 3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: Libro 1 - Método. Recuperado de: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

MINISTERIO DE ADMINISTRACIÓN PÚBLICAS (2012). MAGERIT- Versión 3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: Libro 2 – Catálogo de Elementos. Recuperado de: https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

SECURITY ART WORK (2012) Introducción al análisis de riesgos – Metodologías (II). Recuperado de: https://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+deGesti%C3%B2n+de+Riesgos.pdf

ANEXOS

A. Carta de Presentación a la Empresa

Florencia, febrero 3 de 2017

Hna. María Eva Zarta Santos

Rectora Institución Educativa Domingo Savio

L.C

Cordial Saludo

La presente carta tiene como objetivo solicitar el debido permiso para la ejecución del proyecto “Análisis de Riesgos de Seguridad de la Información utilizando la metodología MAGERIT a la Institución Educativa Domingo Savio en la ciudad de Florencia – Caquetá, como opción de grado de Especialista en Seguridad Informática de la Universidad Nacional Abierta y a Distancia, de la estudiante Adriana Paredes Salinas con cédula de ciudadanía 1078748025 de Acevedo Huila.

Cabe resaltar que toda la información utilizada para la ejecución del proyecto anteriormente mencionado, tendrá tratamiento confidencial, y los resultados obtenidos serán presentados a usted para su análisis y aprobación.

De antemano, agradezco la atención prestada y el apoyo brindado.

Cordialmente,

Adriana Paredes Salinas

(Original Firmada)

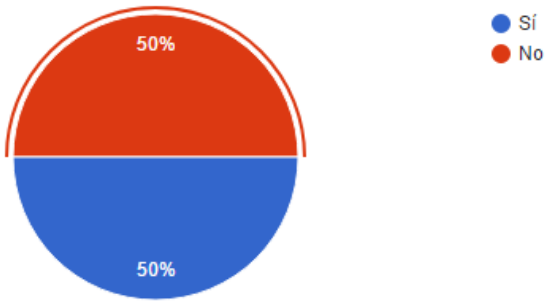
B. Resultados obtenidos de las Encuestas Realizadas

Para la recolección de la información inicial se realizaron dos encuestas dirigidas al personal de la Institución, los resultados obtenidos fueron los siguientes:

Encuesta 1: Análisis de Riesgos en Seguridad Informático a la Institución Educativa Domingo Savio

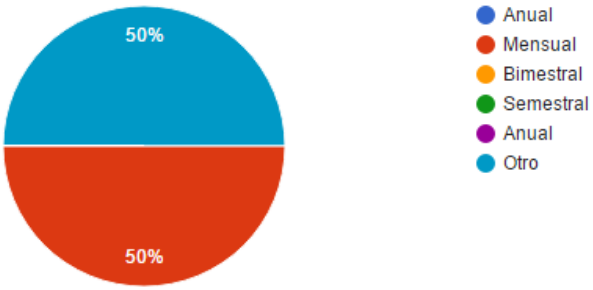
Dirigida a: rectoría, gestión académica, de convivencia, contable y administrativa.

1. ¿Su computador recibe mantenimiento de manera periódica?



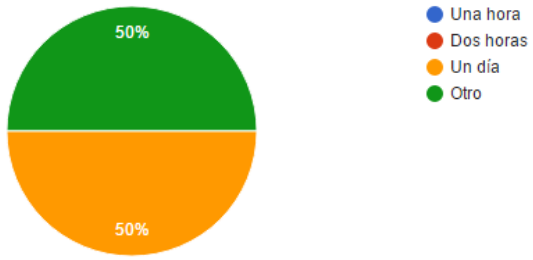
Análisis: el 50% de los empleados encuestados respondieron que reciben mantenimiento a su equipo de cómputo de manera periódica y el 50% respondió que no.

2. ¿Cada cuánto se realiza mantenimiento a su computador?



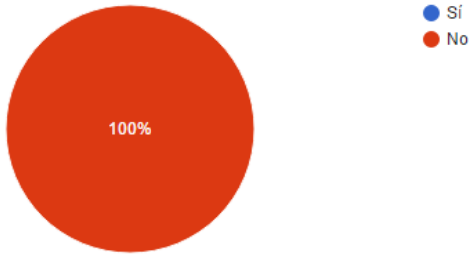
Análisis: el 50% de los empleados respondieron que reciben el mantenimiento a su equipo de manera extra, y el 50% que lo reciben de manera mensual.

3. En caso de daño ¿Qué tiempo se demoran en arreglarlo?



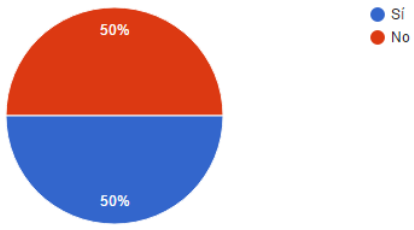
Análisis: el 50% respondieron que lo reciben en un día y el otro 50% respondió que lo reciben en otro tiempo no estipulado.

4. ¿Existe determinado algún periodo de tiempo para el cambio de equipos de cómputo?



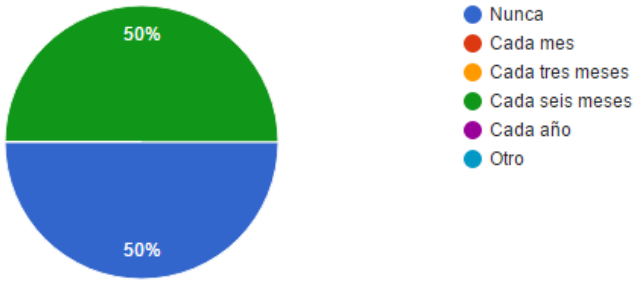
Análisis: el 100% de los empleados respondieron que no existe un tiempo determinado para el cambio de los equipos de cómputo.

5. ¿Su computador cuenta con contraseña?



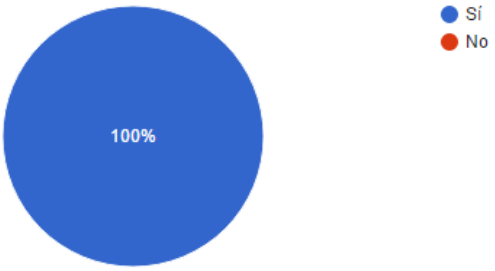
Análisis: el 50% respondieron que su equipo no cuenta con protección de contraseña y el otro 50% que si cuenta con este tipo de protección.

6. ¿Con qué frecuencia cambia su contraseña?



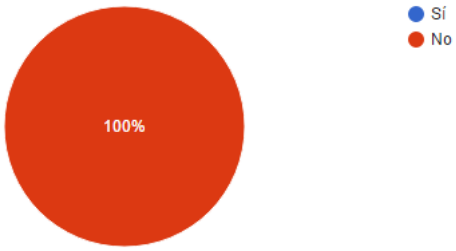
Análisis: el 50% respondieron que su contraseña la cambia cada seis meses y el otro 50% nunca cambia su contraseña.

7. ¿Tiene acceso a internet?



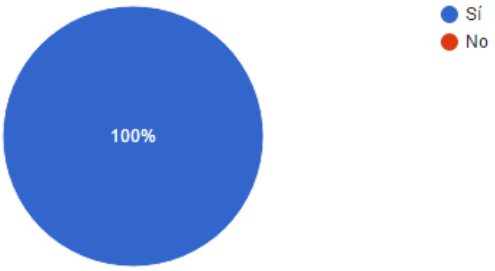
Análisis: el 100% de los usuarios manifestaron que cuentan con el servicio de internet.

8. ¿Tiene restricción para ingresar a páginas de internet?



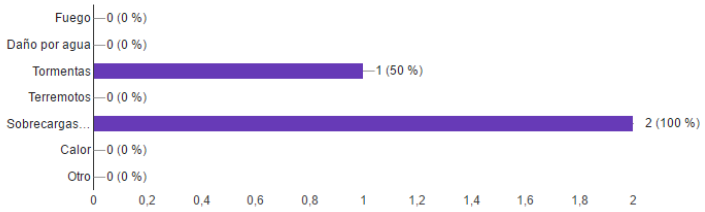
Análisis: el 100% de los usuarios manifestaron que no existen restricciones para el servicio de internet.

9. ¿Su computador tiene instalado un antivirus o antispyware?



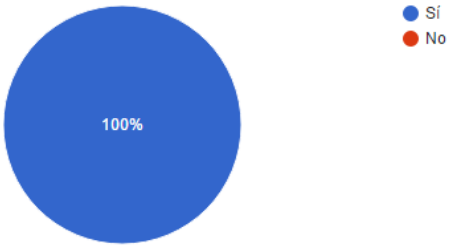
Análisis: el 100% de los usuarios manifestaron que tienen instalada una protección antivirus.

10. ¿La institución se ha visto afectada por amenazas naturales? Marque las que se han presentado (Puede escoger varias opciones):



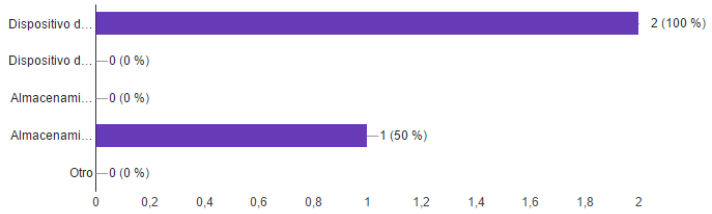
Análisis: los usuarios manifestaron que en la institución se han presentado amenazas naturales como tormentas y sobrecargas de energía.

11. ¿Realiza copias de seguridad de la información propia de la institución que se encuentra a su cargo?



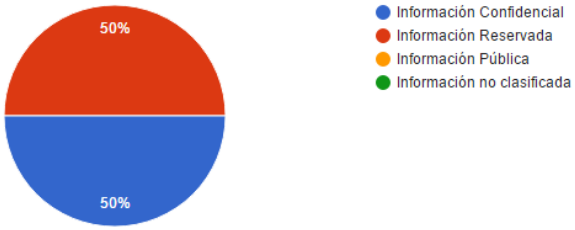
Análisis: el 100% de los usuarios manifestaron que si realiza copias de seguridad de información correspondiente a la institución.

12. ¿En dónde realiza las copias de seguridad (Puede escoger varias opciones)?



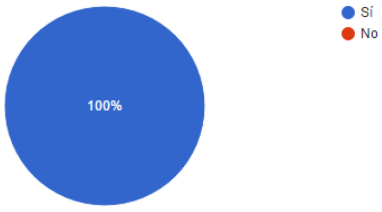
Análisis: los empleados manifestaron que realizan copias de seguridad de la información de la organización en dispositivos de almacenamiento propios de la institución y en almacenamiento en la nube.

13. ¿Qué tipo de información se almacena en su equipo de cómputo?



Análisis: los empleados manifestaron que almacenan tanto información reservada como confidencial en sus equipos de cómputo.

14. ¿Existen un procedimiento documentado y definido para reportar fallas en los sistemas informáticos (red de comunicaciones, equipos de cómputo, software contable, etc.?

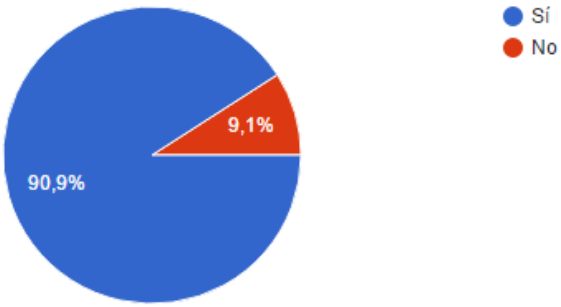


Análisis: el 100% de los empleados manifestaron que si existe un procedimiento para reportar fallas e incidentes informáticos.

Encuesta 2: Análisis de Riesgos en Seguridad Informático a la Institución Educativa Domingo Savio

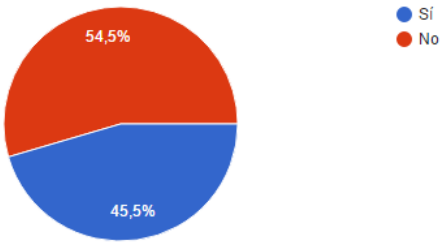
Dirigida a: docentes.

1. ¿Sabes qué es un hacker?



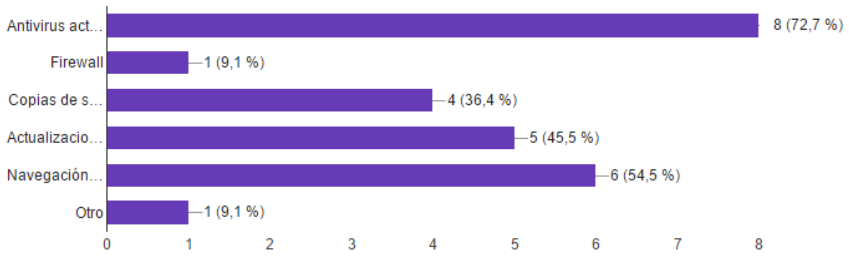
Análisis: el 90,9% de los encuestados manifiestan que sí saben que es un hacker y el 9,1% manifiestan que no lo saben.

2. ¿Estás informado acerca de los mecanismos de seguridad a tener en cuenta para evitar el ingreso no autorizado a su equipo de cómputo?



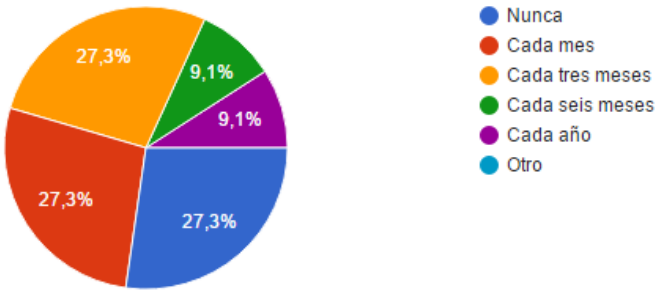
Análisis: el 45,5% de los docentes manifiestan que está informado acerca de mecanismos de seguridad a tener en cuenta para garantizar la seguridad de su equipo de cómputo, mientras que el 54,5% manifiesta que no.

3. ¿Qué mecanismos de seguridad implementas en tu equipo de cómputo (Puede escoger varias opciones)?



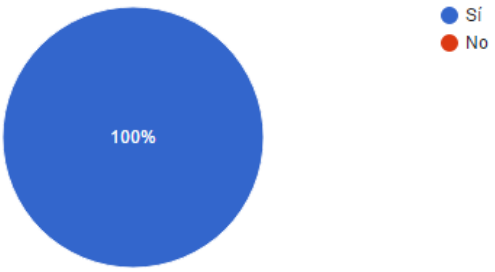
Análisis: los empleados manifiestan que utilizan mecanismos de seguridad como antivirus actualizado, firewall, copias de seguridad, actualizaciones automáticas y navegación segura.

4. ¿Con qué frecuencia cambias la contraseña de ingreso al Sistema de Información de notas de la institución?



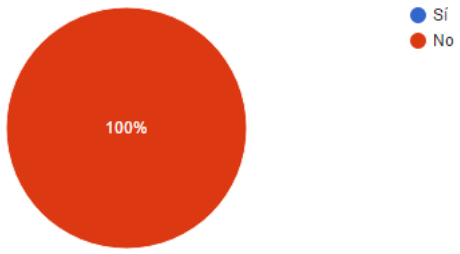
Análisis: de los resultados obtenidos, el 27,3% nunca ha cambiado la contraseña, 27,3% la cambian cada mes, el 27,3% la cambian cada tres meses, el 9,1% la cambian cada seis meses y el 9,1% la cambian cada año.

5. ¿Tiene acceso a internet en la institución?



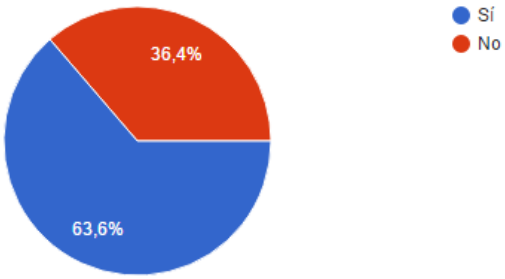
Análisis: el 100% de los usuarios manifestaron que cuentan con el servicio de internet.

6. ¿Tiene restricción para ingresar a páginas de internet en la institución?



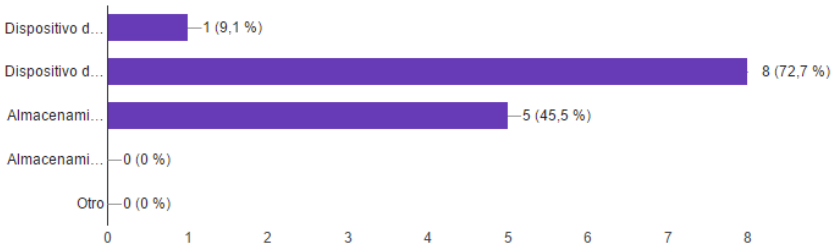
Análisis: el 100% de los usuarios manifestaron que no existen restricciones para el servicio de internet.

7. ¿Realiza copias de seguridad de la información propia de la institución que se encuentra a su cargo?



Análisis: el 63,6% manifiestan que si realizan copias de seguridad y el 36,4% dicen que no realizan copias de seguridad de la información de la institución.

8. ¿En dónde realiza las copias de seguridad (Puede escoger varias opciones?



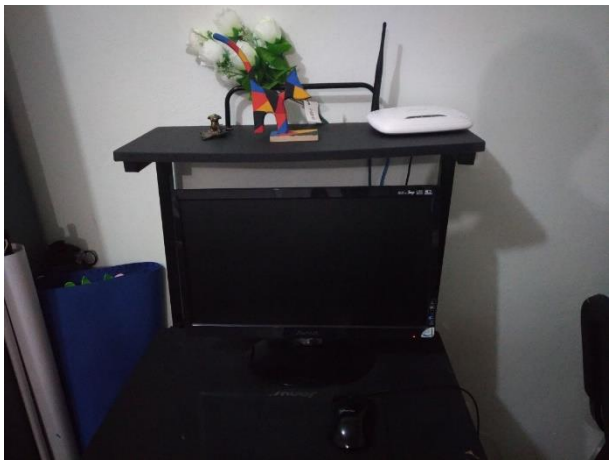
Análisis: los docentes manifiestan que realizan copias de seguridad de la información tanto en dispositivos de la institución como propios y en cuentas en la nube.

C. Evidencia Fotográfica

En las anteriores imágenes se evidencia la ubicación no segura de dos routers inalámbricos.

Evidencia de averías físicas de algunos equipos de cómputo.

En las anteriores fotografías se evidencia protección contra incendios, tanto para elementos tecnológicos como para elementos comunes.

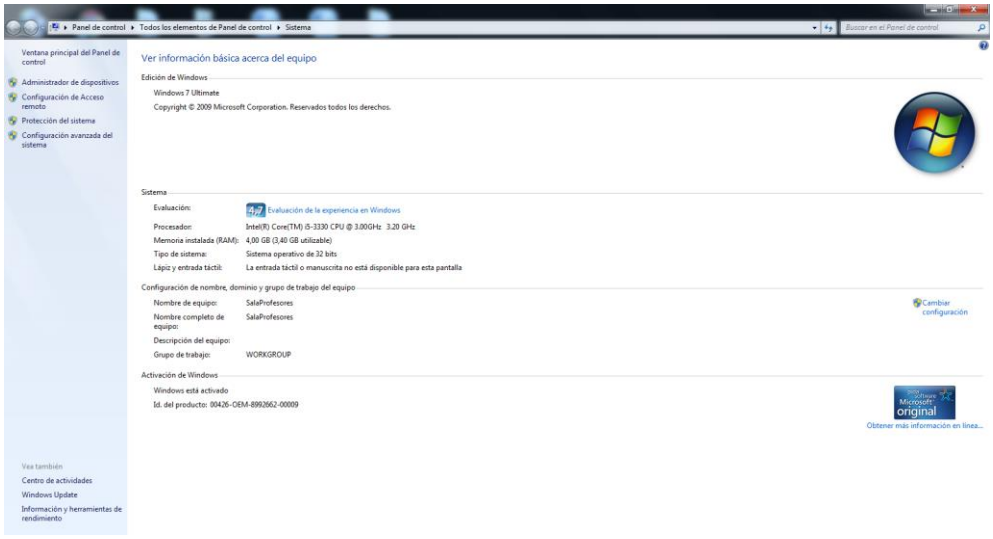


En las anteriores fotografías se evidencia el fácil acceso a equipos auxiliares como routers y switch.

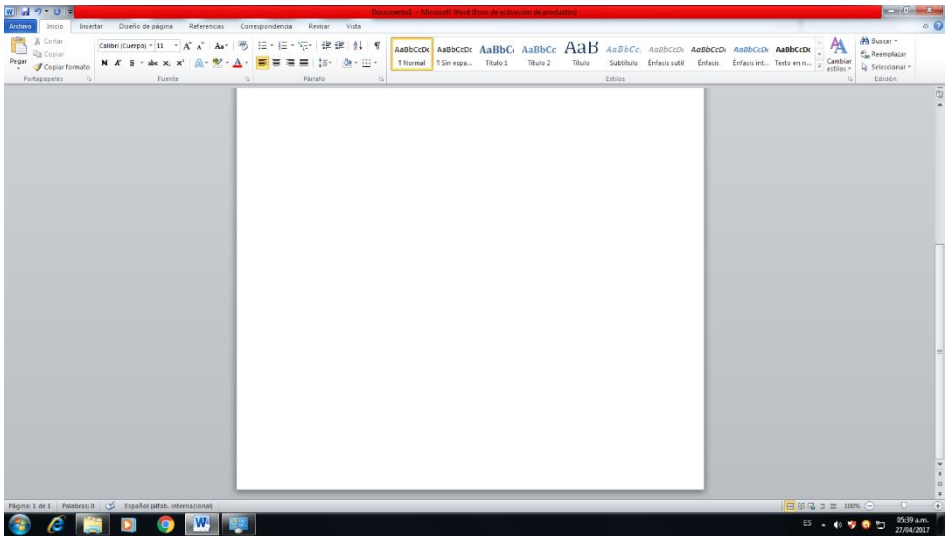
En esta fotografía se puede observar el fácil acceso a parte del cableado.

Rack de comunicaciones con su debida protección.

D. Licenciamiento



Como se muestra en la figura anterior, este pantallazo fue tomado de una de los equipos de la institución, el cual muestra que el sistema operativo se encuentra activado, pero la organización no cuenta con las debidas licencias. La siguiente imagen muestra como el software de ofimática solicita su activación, y debido a que la insittución no cuenta con su licencia podría dejar de funcionar en algún momento.



E. Hoja de Vida de Activos de información relevantes de la organización

ACTIVO: Servicios Internos [SERVICE]		
CÓDIGO: [INTERNET]	NOMBRE: Internet	
DESCRIPCIÓN: Es el servicio de internet prestado por el operador Claro con una velocidad de 30 megas.		
PROPIETARIO: Institución Educativa Domingo Savio		
RESPONSABLE: Proveedor Externo		
TIPO: Servicios.		
VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	N/A	No aplica.
[C]	N/A	No aplica.
[D]	3	Probablemente cause la interrupción de actividades propias de la organización.
[T]	3	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente.
[A]	3	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente.
DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN
[WIFI]	1	Inferior
[LAN]	1	Inferior

ACTIVO: Servicios Internos [SERVICES]	
CÓDIGO: [EXT]	NOMBRE: Acceso a gestión de notas.
DESCRIPCIÓN: Es el servicio que permite el ingreso al sistema de gestión de notas de la institución, contratada a un proveedor externo a la organización.	
PROPIETARIO: Institución Educativa Domingo Savio	
RESPONSABLE: Administrador de Sistemas (Ing. Oscar Eduardo Espinosa)	
TIPO: Servicios.	

VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	8	Probablemente afecte gravemente a un grupo de individuos.
[C]	8	Probablemente quebrante seriamente la ley o algún reglamento de protección de datos personales.
[D]	9	Probablemente cause una interrupción seria de las actividades propias de la organización.
[T]	7	Probablemente causa un grave incidente de seguridad o dificulte la investigación de incidentes graves.
[A]	6	Probablemente causa de una merma en la seguridad o dificulte la investigación de un incidente.

DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN
[PASSWORD]	1	Inferior

ACTIVO: DATOS O INFORMACIÓN [D]	
CÓDIGO: [PASSWORD]	NOMBRE: Contraseñas de acceso al sistema
DESCRIPCIÓN: Son las claves o contraseñas de acceso a la plataforma de notas, cuya asignación inicial es el mismo nombre de usuario, lo que corresponde al número de cédula de ciudadanía del usuario del sistema, ya sea docente o administrador (coordinación académica, secretaría).	
PROPIETARIO: Usuario del sistema	
RESPONSABLE: Usuario del Sistema	
TIPO: Datos o Información	

VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	7	Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
[C]	9	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística.
[D]	N/A	No aplica.
[T]	N/A	No aplica.
[A]	4	Probablemente afecte a un grupo de individuos.

DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN
[EXT]	1	Superior

ACTIVO: DATOS O INFORMACIÓN [D]	
CÓDIGO: [BACKUP]	NOMBRE: Copias de Seguridad.
DESCRIPCIÓN: Hace referencia a los respaldos de información propios de la institución, que corresponde a información de sus clientes y de sus procesos.	
PROPIETARIO: Institución Educativa Domingo Savio	
RESPONSABLE: Usuarios internos, operadores y administrador del sistema.	
TIPO: Datos o Información	

VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	7	Probablemente afecte a un grupo de individuos.
[C]	7	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general.
[D]	1	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local).
[T]	N/A	No aplica.
[A]	N/A	No aplica.

DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN
[MEDIA]	1	Inferior

ACTIVO: SOFTWARE [SW]		
CÓDIGO: [AV]	NOMBRE: Antivirus	
DESCRIPCIÓN: Es la protección contra virus que se encuentra instalado en los equipos de cómputo de la Institución Educativa Domingo Savio, el cual es la versión gratuita de Avast.		
PROPIETARIO: Institución Educativa Domingo Savio		
RESPONSABLE: Operadores		
TIPO: Software		
VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	N/A	No aplica.
[C]	N/A	No aplica.
[D]	3	Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente.
[T]	N/A	No aplica.
[A]	N/A	No aplica.
DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN
[PC]	1	Inferior

ACTIVO: SOFTWARE [SW]	
CÓDIGO: [OFFICE]	NOMBRE: Office
DESCRIPCIÓN: Es el suite de ofimática que se emplea para la edición de documentos básicos de oficina, se encuentra instalado el Microsoft Office 2010 sin licencia de activación.	
PROPIETARIO: Institución Educativa Domingo Savio	
RESPONSABLE: Operadores	
TIPO: Software	

VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	N/A	No aplica.
[C]	N/A	No aplica.
[D]	3	Probablemente cause interrupción de actividades propias de la Organización.
[T]	N/A	No aplica.
[A]	N/A	No aplica.

DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN
[PC]	1	Inferior

ACTIVO: SOFTWARE [SW]		
CÓDIGO: [SO]	NOMBRE: Sistema Operativo	
DESCRIPCIÓN: El sistema operativo con el cuenta la institución instalado en sus equipos de cómputo es Windows 7, pero no se encuentra activado.		
PROPIETARIO: Institución Educativa Domingo Savio		
RESPONSABLE: Operadores		
TIPO: Software		
VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	N/A	No aplica.
[C]	N/A	No aplica.
[D]	3	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.
[T]	N/A	No aplica.
[A]	N/A	No aplica.
DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN
[PC]	1	Inferior

ACTIVO: HARDWARE [HW]		
CÓDIGO: [PC]	NOMBRE: Equipos de Escritorio	
DESCRIPCIÓN: Son todos aquellos equipos de cómputo de escritorio, máquinas gama media, que se utilizan para el procesamiento de información relacionada con las operaciones propias de la institución como generación de informes, gestión académica, gestión adminsitrativa y gestión contable.		
PROPIETARIO: Institución Educativa Domingo Savio		
RESPONSABLE: Usuario interno, operadores.		
TIPO: Hardware		
VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	5	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local.
[C]	N/A	No aplica.
[D]	5	Probablemente impediría la operación efectiva de más de una parte de la Organización.
[T]	N/A	No aplica.
[A]	N/A	No aplica.
DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN
[SW]	1	Inferior

ACTIVO: HARDWARE [HW]	
CÓDIGO: [MOBILE]	NOMBRE: Equipos Portátiles
DESCRIPCIÓN: Son todos aquellos equipos de cómputo portátiles, máquinas gama baja, que se utilizan para el procesamiento de información relacionada algunas operaciones auxiliares propias de la institución.	
PROPIETARIO: Institución Educativa Domingo Savio	
RESPONSABLE: Usuario interno, operadores.	
TIPO: Hardware	

VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	1	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local).
[C]	N/A	No aplica.
[D]	1	Pudiera impedir la operación efectiva de una parte de la Organización
[T]	N/A	No aplica.
[A]	N/A	No aplica.

DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN
[SW]	1	Inferior

ACTIVO: HARDWARE [HW]		
CÓDIGO: [PRINT]	NOMBRE: Impresoras	
DESCRIPCIÓN: Son los equipos que se utilizan para la impresión de archivos.		
PROPIETARIO: Institución Educativa Domingo Savio		
RESPONSABLE: Usuario interno, operadores.		
TIPO: Hardware		
VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	N/A	No aplica.
[C]	N/A	No aplica.
[D]	1	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local).
[T]	N/A	No aplica.
[A]	N/A	No aplica.
DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN
[SW]	1	Inferior

ACTIVO: HARDWARE [HW]		
CÓDIGO: [ROUTER]	NOMBRE: Routers	
DESCRIPCIÓN: Son aquellos dispositivos que se utilizan para la trasmisión de datos en la red wifi pública de la institución.		
PROPIETARIO: Institución Educativa Domingo Savio		
RESPONSABLE: Usuario interno, operadores.		
TIPO: Hardware		
VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	N/A	No aplica.
[C]	N/A	No aplica.
[D]	1	Pudiera causar la interrupción de actividades propias de la Organización.
[T]	7	Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
[A]	N/A	No aplica.
DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN
[SW]	1	Inferior

ACTIVO: HARDWARE [HW]		
CÓDIGO: [SWITCH]	NOMBRE: Switch	
DESCRIPCIÓN: Son aquellos dispositivos de red para la inteconexión lógica de otros equipos de cómputo.		
PROPIETARIO: Institución Educativa Domingo Savio		
RESPONSABLE: Usuario interno, operadores.		
TIPO: Hardware		
VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	N/A	No aplica.
[C]	N/A	No aplica.
[D]	5	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local.
[T]	3	Probablemente cause la interrupción de actividades propias de la Organización.
[A]	N/A	No aplica.
DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN
[SW]	1	Inferior

ACTIVO: SOPORTES DE INFORMACIÓN [MEDIA]	
CÓDIGO: [VR]	NOMBRE: Material Impreso
DESCRIPCIÓN: Es toda aquella información que se encuentra en papel y que corresponde a datos relacionados con los clientes, con las operaciones propias de la información, e información relacionada con el Sistema de Gestión de Calidad de la Institución.	
PROPIETARIO: Institución Educativa Domingo Savio	
RESPONSABLE: Coordinadores de convivencia y académica, líderes de gestiones, operadores.	
TIPO: Soportes de Información	

VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	3	Probablemente afecte a un individuo
[C]	6	Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.
[D]	3	Probablemente cause la interrupción de actividades propias de la Organización.
[T]	N/A	No aplica.
[A]	N/A	No aplica.

DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN
[EXT]	1	Inferior

ACTIVO: SOPORTES DE INFORMACIÓN [MEDIA]		
CÓDIGO: [BACKUP]	NOMBRE: Memoria USB	
DESCRIPCIÓN: Es un dispositivo de almacenamiento en donde se almacena información propia de la gestión administrativa y financiera.		
PROPIETARIO: Institución Educativa Domingo Savio		
RESPONSABLE: Operadores.		
TIPO: Soportes de Información		
VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	N/A	No aplica.
[C]	4	Probablemente quebrante leyes o legislaciones.
[D]	3	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local).
[T]	N/A	No aplica.
[A]	N/A	No aplica.
DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN
[EXT]	1	Inferior

ACTIVO: EQUIPAMIENTO AUXILIAR [AUX]		
CÓDIGO: [UPS]	NOMBRE: UPS	
DESCRIPCIÓN: Son los dispositivos de soporte eléctrico con los que cuenta la institución.		
PROPIETARIO: Institución Educativa Domingo Savio		
RESPONSABLE: Gestión administrativa.		
TIPO: Equipamiento Auxiliar		
VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	N/A	No aplica.
[C]	N/A	No aplica.
[D]	3	Probablemente cause la interrupción de actividades propias de la Organización.
[T]	N/A	No aplica.
[A]	N/A	No aplica.
DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN
[PC]	1	Inferior

ACTIVO: EQUIPAMIENTO AUXILIAR [AUX]	
CÓDIGO: [AC]	NOMBRE: Aires Acondicionados
DESCRIPCIÓN: Es el equipamiento para la regulación climática de los equipos de cómputo.	
PROPIETARIO: Institución Educativa Domingo Savio	
RESPONSABLE: Gestión Administrativa	
TIPO: Equipamiento Auxiliar	

VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	N/A	No aplica.
[C]	N/A	No aplica.
[D]	1	Pudiera impedir la operación efectiva de una parte de la Organización.
[T]	N/A	No aplica.
[A]	N/A	No aplica.

DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN
[PC]	1	Inferior

ACTIVO: EQUIPAMIENTO AUXILIAR [AUX]		
CÓDIGO: [RACK]	NOMBRE: Rack	
DESCRIPCIÓN: Son las estructuras metálicas que albergan equipos de comunicaciones como los switch y hubs. La institución cuenta con tres racks distribuídos en la sala de profesores, la sala de informática y la oficina de contabilidad. Cabe resaltar, que es de vital importancia un mecanismo de seguridad que permita que los racks se encuentren debidamente cerrados.		
PROPIETARIO: Institución Educativa Domingo Savio		
RESPONSABLE: Gestión Administrativa		
TIPO: Equipamiento Auxiliar		
VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	7	Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
[C]	N/A	No aplica.
[D]	N/A	No aplica.
[T]	N/A	No aplica.
[A]	N/A	No aplica.
DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN
[ROUTER]	1	Inferior
[SWITCH]	1	Inferior

ACTIVO: EQUIPAMIENTO AUXILIAR [AUX]		
CÓDIGO: [CABLING]	NOMBRE: Cableado	
DESCRIPCIÓN: Es el cableado que se encuentra dentro del edificio y que constituyen una red interna de comunicaciones.		
PROPIETARIO: Institución Educativa Domingo Savio		
RESPONSABLE: Gestión Administrativa		
TIPO: Equipamiento Auxiliar		
VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	N/A	No aplica.
[C]	N/A	No aplica.
[D]	3	Probablemente cause la interrupción de actividades propias de la Organización.
[T]	N/A	No aplica.
[A]	N/A	No aplica.
DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN
[PC]	1	Inferior

ACTIVO: REDES DE COMUNICACIONES [COM]	
CÓDIGO: [WIFI]	NOMBRE: Red Inalámbrica
DESCRIPCIÓN: Conexión inalámbrica la cual consta de tres routers inalámbricos ubicados en la zona de preescolar, pasillo del segundo piso y sala de profesores. Esta red se encuentra fragmentada en cuatro sectores: administrativos que cuenta con código de acceso, docentes que cuenta con código de acceso, estudiantes la cual se encuentra abierta al público y contabilidad que cuenta con código de acceso.	
PROPIETARIO: Institución Educativa Domingo Savio	
RESPONSABLE: Gestión administrativa	
TIPO: Redes de Comunicaciones	

VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	N/A	No aplica.
[C]	N/A	No aplica.
[D]	1	Pudiera impedir la operación efectiva de una parte de la Organización.
[T]	7	Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
[A]	N/A	No aplica.

DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN
[INTERNET]	1	Inferior

ACTIVO: REDES DE COMUNICACIONES [COM]		
CÓDIGO: [LAN]	NOMBRE: Red Local	
DESCRIPCIÓN: Conexión de red por medio de cableado, cuenta con 35 puntos de red.		
PROPIETARIO: Institución Educativa Domingo Savio		
RESPONSABLE: Gestión Administrativa		
TIPO: Red de Comunicaciones		
VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	N/A	No aplica.
[C]	N/A	No aplica.
[D]	5	Probablemente impediría la operación efectiva de más de una parte de la Organización.
[T]	7	Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
[A]	N/A	No aplica.
DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN
[INTERNET]	1	Inferior

ACTIVO: INSTALACIONES [L]		
CÓDIGO: [BUILDING]	NOMBRE: Edificio	
DESCRIPCIÓN: Los activos de información más importantes de la organización se encuentran ubicados en un único edificio ubicado en la Calle 25 Carrera 10 Esquina Barrio Torasso en la ciudad de Florencia Caquetá.		
PROPIETARIO: Institución Educativa Domingo Savio		
RESPONSABLE: Gestión Administrativa		
TIPO: Instalaciones		
VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	N/A	No aplica.
[C]	N/A	No aplica.
[D]	9	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones.
[T]	N/A	No aplica.
[A]	N/A	No aplica.
DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN

ACTIVO: PERSONAL [P]		
CÓDIGO: [UI]	NOMBRE: Usuarios Internos	
DESCRIPCIÓN: Los usuarios internos son todas aquellas personas que se benefician de los servicios que ofrece la organización, como son docentes, adminsitrativos y personal operativo.		
PROPIETARIO: Institución Educativa Domingo Savio		
RESPONSABLE: Gestión de Talento Humano		
TIPO: Personal		
VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	N/A	No aplica.
[C]	6	Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.
[D]	3	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local).
[T]	N/A	No aplica.
[A]	N/A	No aplica.
DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN

ACTIVO: PERSONAL [P]	
CÓDIGO: [ADM]	NOMBRE: Administrador de sistemas
DESCRIPCIÓN: Es aquella persona encargada de adminsitrar la plataforma de gestión de notas institucional, además de realizar la gestión de incidentes de activos informáticos.	
PROPIETARIO: Institución Educativa Domingo Savio	
RESPONSABLE: Gestión de Talento Humano	
TIPO: Personal	

VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	N/A	No aplica.
[C]	6	Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.
[D]	3	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local).
[T]	N/A	No aplica.
[A]	N/A	No aplica.

DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN

ACTIVO: PERSONAL [P]	
CÓDIGO: [OP]	NOMBRE: Operadores
DESCRIPCIÓN: Es aquel personal que se dedica a las operaciones propias de la institución, como gestión administrativa, gestión académica y secretaría.	
PROPIETARIO: Institución Educativa Domingo Savio	
RESPONSABLE: Gestión de Talento Humano	
TIPO: Personal	

VALORACIÓN		
DIMENSIÓN	VALOR	JUSTIFICACIÓN
[I]	N/A	No aplica.
[C]	6	Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.
[D]	3	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local).
[T]	N/A	No aplica.
[A]	N/A	No aplica.

DEPENDENCIA DE ACTIVOS INFERIORES (Hijos)		
ACTIVO	GRADO	JUSTIFICACIÓN