PROPUESTA DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA LA INSTITUCIÓN EDUCATIVA CELCO SAN LUCAS.

EDWIN ALBERTO NARANJO JIMÉNEZ

EDWIN GABRIEL ROA BOTIA

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

FACULTAD TECNOLOGICA

INGENIERIA EN TELMÁTICA

BOGOTÁ

2018

PROPUESTA DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA LA INSTITUCIÓN EDUCATIVA CELCO SAN LUCAS

EDWIN ALBERTO NARANJO JIMÉNEZ

EDWIN GABRIEL ROA BOTIA

Trabajo de grado presentado como requisito para optar al título de INGENIERÍA EN TELEMÁTICA

TUTOR:

MIGUEL ÁNGEL LEGUIZAMON PÁEZ

Ingeniero en Sistemas

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

FACULTAD TECNOLOGICA

INGENIERIA EN TELMÁTICA

BOGOTA

2018

Nota de aceptación

_____

_____

_____

_____

_____

Tutor

_____

Jurado

Bogotá D.C. 08 de agosto de 2018

AGRADECIMIENTOS

Como parte de este proceso damos gracias primeramente a Dios por permitirnos llegar hasta esta etapa, a nuestras familias que fueron el apoyo en el diario vivir, que comprendieron nuestros esfuerzos y dedicación en la meta que cultivábamos en nuestro día a día universitario.

A nuestros compañeros, docentes y a la Universidad Distrital que nos permitió hacer parte de un proceso educativo, en el cual, a parte de formar ingenieros, formo en nosotros unos profesionales íntegros y comprometidos con ser mejores personas cada día.

Un agradecimiento especial al tutor de este proyecto, el Ingeniero Miguel Ángel Leguizamón, que gracias a su empeño, dedicación y buena disposición para con nosotros permitió culminar esta etapa. Una persona que siempre se mostró dispuesto a atendernos y brindarnos los mejores consejos con base a su experiencia como docente y tutor en otros proyectos.

TABLA DE CONTENIDO

INTRODUCCIÓN *3*

1 PLANTEAMIENTO DEL PROBLEMA *4*

1.1 OBJETIVOS **5**

1.1.1 OBJETIVO GENERAL 5

1.1.2 OBJETIVOS ESPECIFICOS 5

1.2 MARCO TEORICO **6**

1.2.1 DESCRIPCIÓN ISO 27001 6

1.2.1.1 ¿QUÉ ES? 6

1.2.2 FASES DEL CICLO PHVA 7

1.2.3 ANTECEDENTES DE TRABAJOS 8

1.3 SOLUCIÓN TECNOLOGICA **9**

1.4 METODOLOGIA PHVA **10**

1.4.1 PLANIFICAR 10

1.4.2 HACER 10

1.4.3 VERIFICAR 10

1.4.4 ACTUAR 10

1.5 CRONOGRA DE ACTIVIDADES **11**

1.6 PRESUPUESTO DE LA IPLEMENTACIÓN **12**

1.7 ESTADO ACTUAL DE LA EMPRESA **12**

1.8 MARCO ESTRATÉGICO **13**

1.8.1 MISIÓN 13

1.8.2 VISIÓN 13

1.8.3 FILOSOFIA 13

2 DIAGNOSTICO *14*

2.1 SITUACION ACTUAL DE LA INSTITUCION **14**

2.1.1 ANALISIS INICIAL 14

2.1.2 CABLEADO ESTRUCTURADO 14

2.1.3 PERSONAL Y ESTRUCTURA ORGANIZACIONAL 14

2.1.4 INFORMACIÓN ACTIVOS 15

2.2 DIAGNOSTICO DE SEGURIDAD **22**

3 ANALISIS DE RIESGOS *22*

3.1 VALORACIÓN DE RIESGOS **22**

3.1.1 UNIVERSO DE VALORES 23

3.1.2 VALORACIÓN DE LOS ACTIVOS 23

3.1.3 MAPA DE RIESGOS 30

3.1.4 MATRIZ DE RIESGOS 31

3.1.5 PLAN DE TRATAMIENTO DE RIESGOS 34

3.2 CONTROLES PARA EL TRATAMIENTO DE RIESGOS **35**

4 PLANTEAMIENTO DEL SISTEMA DE SEGURIDAD *38*

4.1 ALCANCE. **38**

4.2 OBJETIVO **38**

4.3 METODOLOGIA..... 39

5 POLÍTICAS DE SEGURIDAD 39

5.1 JUSTIFICACIÓN. 39

5.2 PROPÓSITO. 40

5.3 ALCANCE. 40

5.4 ASPECTOS GENERALES. 40

5.5 RESPONSABILIDADES. 41

5.6 POLITICAS PARA MANEJO DE LA INFORMACIÓN. 41

5.7 POLÍTICAS DE SEGURIDAD PARA COMPUTADORES. 42

5.8 POLÍTICAS DE SEGURIDAD PARA LAS COMUNICACIONES. 44

5.8.1 PROPIEDAD DE LA INFORMACIÓN. 44

5.8.2 USO DE LOS SISTEMAS DE COMUNICACIÓN. 45

5.8.3 CONFIDENCIALIDAD Y PRIVACIDAD. 45

5.8.4 REENVÍO DE MENSAJES. 45

5.8.5 BORRADO DE MENSAJES. 46

5.9 POLÍTICAS DE SEGURIDAD PARA REDES. 46

5.9.1 MODIFICACIONES. 46

5.9.2 CUENTAS DE LOS USUARIOS. 46

5.10 CONTRASEÑAS Y EL CONTROL DE ACCESO. 47

6 SOFTWARE DE SEGURIDAD 48

6.1 SERVIDOR FIREWALL PFSENSE 48

6.1.1 SERVIDOR DHCP. 49

6.1.2 SERVIDOR PROXY. 49

6.2 SEGURIDAD Y ADMINISTRACIÓN WIFI 51

7 CONCLUSIONES 53

8 BIBLIOGRAFIA 54

LISTA DE TABLAS

Tabla 1 Presupuesto de la solución 12
Tabla 2 Inventario Activos 21
Tabla 3 Clasificación de los valores 23
Tabla 4 Valoración de activos 29
Tabla 6 Impacto en el negocio 30
Tabla 7 Probabilidad de afectación 30
Tabla 5 Mapa de Riesgos 31
Tabla 8 Matriz de riesgos 34
Tabla 9 Tratamiento de los Riesgos 35
Tabla 10 Dominios, objetivos y controles ISO 27002:2013 38

LISTA DE FIGURAS

Figura 1 Número de certificaciones por año de normas ISO 7
Figura 2 Ranking certificaciones para el año 2017 en América Latina 7
Figura 3 Cronograma de actividades 11
Figura 5 Configuración interfaz LAN y DHCP 49
Figura 6 SquidGuard 50
Figura 7 Categorías de la lista negra 50
Figura 8 Configuración de Filtrado MAC 51
Figura 9 Dispositivos Conectados 51

RESUMEN

La información se ha convertido en el recurso más valioso para el funcionamiento y evolución de las empresas e instituciones del mundo moderno, por tal razón las amenazas que afectan los sistemas de información cada vez son más complejas y difíciles de detectar a tiempo.

Asegurar la información, la integridad de los datos y la confidencialidad permitirá que los riesgos de afectación en la operación continua de las empresas sean mínimas. Este proyecto tiene como objeto la propuesta de un Sistema de Seguridad de la Información basándose en los lineamentos de la Norma ISO 27001 y siguiendo la metodología PHVA, iniciando con un análisis de la situación actual de la institución, identificación de vulnerabilidades, creación de controles, políticas de seguridad para finalmente implementar un software de seguridad perimetral que apoye los nivele de seguridad de la institución educativa CELCO San Lucas.

Palabras claves: SEGURIDAD INFORMÁTICA, INSTITUCIONES EDUCATIVAS, RIESGOS, POLÍTICAS DE SEGURIDAD, CONTROL DE ACCESO, VULNERABILIDADES, AMENAZAS.

ABSTRACT

The information has converted in the most valuable resource for the functioning and evolution of the companies and institutions of the modern world for this reason the threats that affect the information system every time are more elaborates and difficult of detect on time.

Ensure the information, the integrity of the dates and the confidentiality will allow that the threats that affect in the frequent operation of the companies will be minimum. This project has as a goal the proposition of a Security System of the information base on the guidelines of the ISO standard 27001 using the methodology PHVA (Plan, Check, Verify and Act), starting with an analysis of the current situation of the institutions, identification of the vulnerabilities, controls creation, safety politics and finally to implement a software of perimeter security whichtz support the security levels of the institution.

KEYWORDS:

COMPUTER SECURITY, EDUCATIONAL INSTITUTIONS, RISKS, SAFETY POLITICS, ACCESS CONTROL, VULNERABILITIES, THREATS.

INTRODUCCIÓN

El manejo de grandes volúmenes de información al interior de las instituciones, la constante evolución de la tecnología a nivel mundial y la necesidad de comunicación constante al interior y través de internet conllevan a grandes problemas de seguridad informática, los ataques externos constantes y software maliciosos más robustos ponen en manifiesto los problemas de seguridad que afectan la operación continua de las empresas, garantizar la confidencialidad de la información así como la integridad y disponibilidad de los datos son temas fundamentales y que deben ser atendidas de alguna manera si se desea crecer y evolucionar en el ámbito de la tecnología.

Celco San Lucas es una institución educativa que maneja grandes volúmenes de información estudiantil y cuenta con una infraestructura tecnológica suficiente para la adecuada prestación del servicio educativo, con este proyecto se desea proponer un sistema de seguridad que minimice los riesgos de pérdida, alteración y manipulación a información vital para el funcionamiento de la institución así como la adecuada administración de los recursos tecnológico al interior y mejorar sus procesos entre áreas administrativas, profesorado y estudiantes.

En la etapa de implementación se realizarán actividades de mejoramiento y puesta en marcha de mecanismos de seguridad que acompañados con las recomendaciones que se adjuntan en el presente documento permitirá de esta manera que los procesos sean optimizados y mejorados con el fin de minimizar impactos futuros.

1 PLANTEAMIENTO DEL PROBLEMA

El colegio Evangélico Luterano CELCO San Lucas actualmente presta los servicios de educación básica y secundaria a más de 1000 estudiantes y cuenta con una planta de 60 personas entre administrativos y profesores, la información del colegio posee datos educativos de más de 20 años, los cuales se almacenan de forma física en lugares destinados para el archivo y la otra parte se encuentra digitalizada desde el año 2008 en un software de gestión educativa llamado Sigecol, dicha información está en riesgo de recibir ataques informáticos y/o alteración, ya que al hacer un análisis documental e indagando con el personal administrativo no se cuenta con una documentación o políticas que minimicen o mitiguen los riesgos de la información que se maneja.

El actual software de seguridad (Untangle) es básico y no permite generar informes que le den valor al control de navegación de los estudiantes, los perfiles de usuarios (administrativos, docentes, estudiantes) no tienen una estructura adecuada según las actividades que realizan, no se cuenta con un mecanismo que permita recuperar los datos ,al no poseer controles y monitoreo activo que permita prever riesgos informáticos que afecten la integridad, confidencialidad y disponibilidad de los datos.

Al no contar con las políticas y mecanismos necesarios para el control, acceso y manipulación de la información, se pueden llegar a generar problemas de veracidad o alteración de los datos sensibles que son manejados por parte de funcionarios y estudiantes. Si se materializa alguno de estos riesgos la entidad podría entrar en un gasto para recuperar información afectada, (partiendo de que toda pueda ser recuperada) además de perder información educativa de muchos años que se podrían ver reflejados en los tiempos de respuesta de la institución.

¿De qué manera se puede aportar a la seguridad de la Información que maneja el Colegio Luterano CELCO San Lucas que minimice el riesgo de pérdida o alteración de datos institucionales?

1.1 OBJETIVOS

1.1.1 OBJETIVO GENERAL

Proponer un Sistema de Seguridad de la Información en el Colegio Evangélico Luterano CELCO San Lucas que permita reducir los problemas relacionados con la seguridad de la información con los que cuenta la institución.

1.1.2 OBJETIVOS ESPECIFICOS

- Hacer un diagnóstico de cómo se encuentra la seguridad de la información dentro de la institución educativa CELCO San Lucas

- Realizar un análisis de riesgos informáticos presentes en la institución basándose en la norma ISO 27001

- Plantear el Sistema de Gestión de Seguridad de la Información con los datos obtenidos en el diagnóstico y el análisis de riesgos realizado.

- Definir políticas para el manejo de la información garantizando la seguridad de la misma, teniendo en cuenta los perfiles que posee la institución (estudiante, profesor, administrativo).

- Implementar un software de seguridad que permita controlar y gestionar el acceso a contenido no deseado por parte de estudiantes y funcionarios

1.2 MARCO TEORICO

En los últimos años asegurar la información de una compañía se ha convertido en un tema fundamental y de vital importancia para la continuidad del negocio, para tal fin existen normas aceptadas internacionalmente que contienen los métodos y pautas para llegar a un modelo integral de un sistema de seguridad y manejo de la información, los más usados y reconocidos son las ISO/ IEC 27000 y para nuestro contexto específicamente la ISO 27001. "La ISO/IEC 27001 es un estándar para la seguridad de la información (Información technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission."

1.2.1 DESCRIPCIÓN ISO 27001

La familia de normas ISO / IEC 27000 ayuda a las organizaciones a mantener seguros los activos de información. El uso de esta familia de normas ayudará a la organización a administrar la seguridad de activos tales como información financiera, propiedad intelectual, detalles de los empleados o información que le haya sido confiada por terceros. ISO / IEC 27001 es el estándar más conocido en la familia que proporciona los requisitos para un sistema de gestión de seguridad de la información (ISMS).

1.2.1.1 ¿QUÉ ES?

Un SGSI es un enfoque sistemático para administrar la información sensible de la compañía para que permanezca segura. Incluye personas, procesos y sistemas de TI mediante la aplicación de un proceso de gestión de riesgos. Puede ayudar a las pequeñas, medianas y grandes empresas en cualquier sector a mantener seguros los activos de información. A nivel mundial y año tras año se incrementa el número de empresas que cuentan con la certificación en la norma ISO 27001 (ver tabla 1.1) con un aumento del 21% con respecto al año 2015, por lo que podemos concluir que cada vez es más aceptado la ideología de una buena administración en seguridad de la información dentro de las compañías.

Al igual que otros estándares del sistema de gestión ISO, la certificación ISO / IEC 27001 es posible pero no obligatoria. Algunas organizaciones optan por implementar el estándar para beneficiarse de las mejores prácticas que contiene, mientras que otros deciden que también quieren certificarse para asegurar a los clientes y clientes que se han seguido sus recomendaciones. ISO no realiza la certificación.

Standard	Number of certificates in 2016	Number of certificates in 2015	Change	Change in %
ISO 9001**	1106356	1034180	72176	+7%
ISO 14001***	346189	319496	26693	+8%
ISO 50001	20216	11985	8231	+69%
ISO 27001	33290	27536	5754	+21%
ISO 22000	32139	32061	78	0
ISO/TS 16949	67358	62944	4414	+7%
ISO 13485	29585	26255	3330	+13%
ISO 22301	3853	3133	720	+23%
ISO 20000-1	4537	2778	1759	+63%
ISO 28000	356			
ISO 39001	478			
TOTAL	1,644,357	1,520,368		+8%

**ISO 9001:2008 (= 1025761) + ISO 9001:2015 (=80596)
***ISO 14001:2004 (=323023) + ISO 14001:2015 (=23167)

Figura 1 Número de certificaciones por año de normas ISO

Fuente: The ISO Survey of Management System Standard Certifications 2016

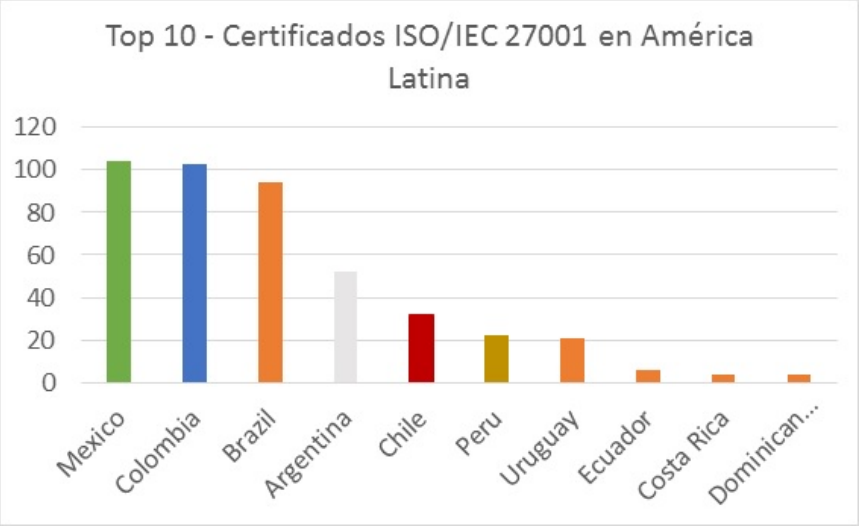


Figura 2 Ranking certificaciones para el año 2017 en América Latina

Fuente: http://www.datasec.com.uy/es/blog/certificados-isoiec-27001-emitidos-nivel-mundial

1.2.2 FASES DEL CICLO PHVA

Las siglas del ciclo o fórmula PHVA forman un acrónimo compuesto por las iniciales de las palabras Planificar, Hacer Verificar y Actuar. Cada uno de estos 4 conceptos corresponde a una fase o etapa del ciclo:

- Planificar: En la etapa de planificación se establecen objetivos y se identifican los procesos necesarios para lograr unos determinados resultados de acuerdo a las políticas de la organización. En esta etapa se determinan también los parámetros de medición que se van a utilizar para controlar y seguir el proceso.

- Hacer: Consiste en la implementación de los cambios o acciones necesarias para lograr las mejoras planteadas. Con el objeto de ganar en eficacia y poder corregir fácilmente posibles errores en la ejecución, normalmente se desarrolla un plan piloto a modo de prueba o testeo.

- Verificar: Una vez se ha puesto en marcha el plan de mejoras, se establece un periodo de prueba para medir y valorar la efectividad de los cambios. Se trata de una fase de regulación y ajuste.

- Actuar: Realizadas las mediciones, en el caso de que los resultados no se ajusten a las expectativas y objetivos predefinidos, se realizan las correcciones y modificaciones necesarias. Por otro lado, se toman las decisiones y acciones pertinentes para mejorar continuamente el desarrollo de los procesos.

1.2.3 ANTECEDENTES DE TRABAJOS

Los proyectos que se mencionan a continuación aportan de distintas maneras al desarrollo de la propuesta de un Sistema de gestión de seguridad de la Información para la institución educativa CELCO San Lucas:

PROPUESTA DE MODELO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN APLICADA A INSTITUCIONES EDUCATIVAS

Desarrollado por dos estudiantes de la Universidad Distrital Francisco José de Caldas para optar al título de Ingeniería en Telemática, este trabajo desarrolla una temática general de seguridad de la Información a instituciones educativas por lo que su aporte a la presente propuesta se basa en los siguientes criterios.

- Está desarrollado con base en la norma ISO 27001 y hace uso de la metodología PHVA, ambos planteamientos serán usados en la presente propuesta.

- Realiza una Investigación exhaustiva de los riesgos que se pueden presentar teniendo como referencia la información y el modelo de trabajo de las instituciones de educación básica y media.

- Permite identificar las debilidades dentro de la institución basándose en el diagnóstico y el análisis de riesgo desarrollado.

METODOLOGÍA PARA LA IMPLEMENTACIÓN DE UN SISTEMA INTEGRADO DE GESTIÓN CON LAS NORMAS ISO 9001, ISO 20000 e ISO 27001.

Desarrollado por los estudiantes DIANA MARCELA CORTES R. y ALIX VICTORIA ARDILA, para optar por el título de Especialistas en gerencia de procesos y calidad de la Universidad EAN.

Esta propuesta se basa en la integración y gestión de una serie de normas enfocadas en procesos de calidad, gestión y seguridad de la información, en los cuales se aborda la norma ISO 27001, que para el desarrollo de la presente propuesta es de gran ayuda

puesto que permite apoyarse en las técnicas o metodologías que fueron desarrolladas por los estudiantes para el desarrollo de su trabajo.

Al momento de analizar los resultados obtenidos en dicho trabajo, se puede dar marcha a la propuesta, ya que se tiene una base de cómo realizar los procesos, controles, requerimientos y levantamiento de información.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO 27001 Y 27002 PARA LA UNIDAD DE INFORMÁTICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE NARIÑO.

Desarrollado por los estudiantes YEZID CAMILO GUERRERO ANGULO y ROBERT MARCELO TABANGO GOYES Para optar por el título de ingenieros de sistemas de la Universidad de Nariño.

El manejo de información relacionada con bases de datos de estudiantes, aplicativos de notas y servicios institucionales son los aspectos principales que desarrollan los estudiantes de la Universidad de Nariño en la propuesta de SGSI basado en la ISO 27001 para optimizar y proteger la información, tomando parte de la metodología y estrategias utilizadas en dicho trabajo se tiene como base de partida la forma en que se debe actuar en la Institución Educativa CELCO San Lucas con la información que se quiere proteger y optimizar, así como la forma en que deben ser identificados los activos que forman parte de dicha infraestructura para medir el nivel de riesgo, vulnerabilidad y controles que se deben aplicar para la prevención de pérdida de información y acciones cuando un evento de seguridad se materialice.

1.3 SOLUCIÓN TECNOLOGICA

La implementación de una solución tecnológica en el Colegio CELCO san Lucas está basada en una serie de procedimientos enfocados al aseguramiento de información que se deben llevar a cabo para mitigar algún tipo de impacto o amenaza con los datos que cuenta la institución. Se parte de un análisis de riesgos de la seguridad actual de la red y equipos, lo que permite crear las políticas adecuadas para mitigar el riesgo y garantizar la confidencialidad, integridad, disponibilidad y autenticidad de la información, esto acompañado de un documento de buenas prácticas que complemente los procesos de seguridad.

El respaldo de la información sensible que se maneja en los módulos de notas, reportes y matrículas, así como los datos de administrativos y docentes se gestionará a través de un sistema de backup en la nube asociado al dominio educativo de cada una de las cuentas institucionales con la que cuenta cada funcionario.

La implementación y parametrización del software de seguridad (PFsense) permite poner en marcha las políticas establecidas, auditar los procesos de seguridad por medio de reportes de tráfico en la red, políticas de acceso y navegación en internet. Este Software es de tipo Free BSD y dentro de sus características está la de poder gestionar un servidor proxy(Squid), integración con servicios de active directory para la gestión de los usuarios existentes, manejo de listas de acceso (ACLs), configuración de reenvío de puertos para servicios específicos, priorización de servicios dependiendo de las necesidades de la institución, control de tráfico en internet a través de listas negras de contenido no deseado (pornografía, violencia, piratería).

1.4 METODOLOGIA PHVA

La metodología PHVA permite mantener la mejora continua de los procesos que soportan la seguridad de la información dentro de la institución, con esto se asegura un ciclo de desarrollo y mejora continua a los controles, políticas y objetivos dentro de la propuesta de un Sistema de Gestión de Seguridad de la Información para el Colegio Celco San Lucas.

1.4.1 PLANIFICAR

En esta primera etapa se planifican las tareas que se llevarán a cabo en cuanto a la asignación de roles y responsabilidades por parte de cada uno de los funcionarios según sus labores, partiendo de estas tareas se puede identificar los riesgos a los cuales se puede ver expuesta la información al ser manipulada por los usuarios.
Al tener claras las tareas y las asignaciones se puede medir el alcance y los objetivos que se están planificando, esto complementándolo con información acerca de recursos y equipamiento necesarios para el alcance de los objetivos planteados.

1.4.2 HACER

Al tener la planificación de las actividades a desarrollar se procede a generar los roles y perfiles de cada uno de los funcionarios que se encuentran en la institución partiendo de si son docentes, administrativos o estudiantes, luego de dicha labor se implementa y crea las políticas de seguridad, esto con herramientas de seguridad que se van a parametrizar y configurar según los recursos disponibles analizados en la etapa de planificación.

1.4.3 VERIFICAR

Para poder verificar que los objetivos que se plantearon y recopilaron se cumplen de manera adecuada se debe realizar un monitoreo que permita medir y revisar cada uno de los objetivos de seguridad y funcionamiento que se enumeraron en la fase de planificaron y hacer.
Los resultados obtenidos se deben reforzar con revisiones periódicas que permiten comprobar los requisitos planteados en la norma ISO 27001 que forma parte del sistema de gestión de seguridad de la información.
Cabe aclarar que las revisiones se deben reforzar con auditorías programadas dependiendo del estado actual en el que se encuentran los procesos y las dependencias que se desean auditar.

1.4.4 ACTUAR

Con los resultados obtenidos de las fases anteriores se hace necesario recopilar y analizar los datos para determinar el estado de la gestión de seguridad que se está desarrollando, posterior a identificar los problemas de seguridad encontrados se planifican e implementan las mejoras que permiten actuar sobre los puntos encontrados que requieran sean controlados o minimizados.

1.5 CRONOGRA DE ACTIVIDADES

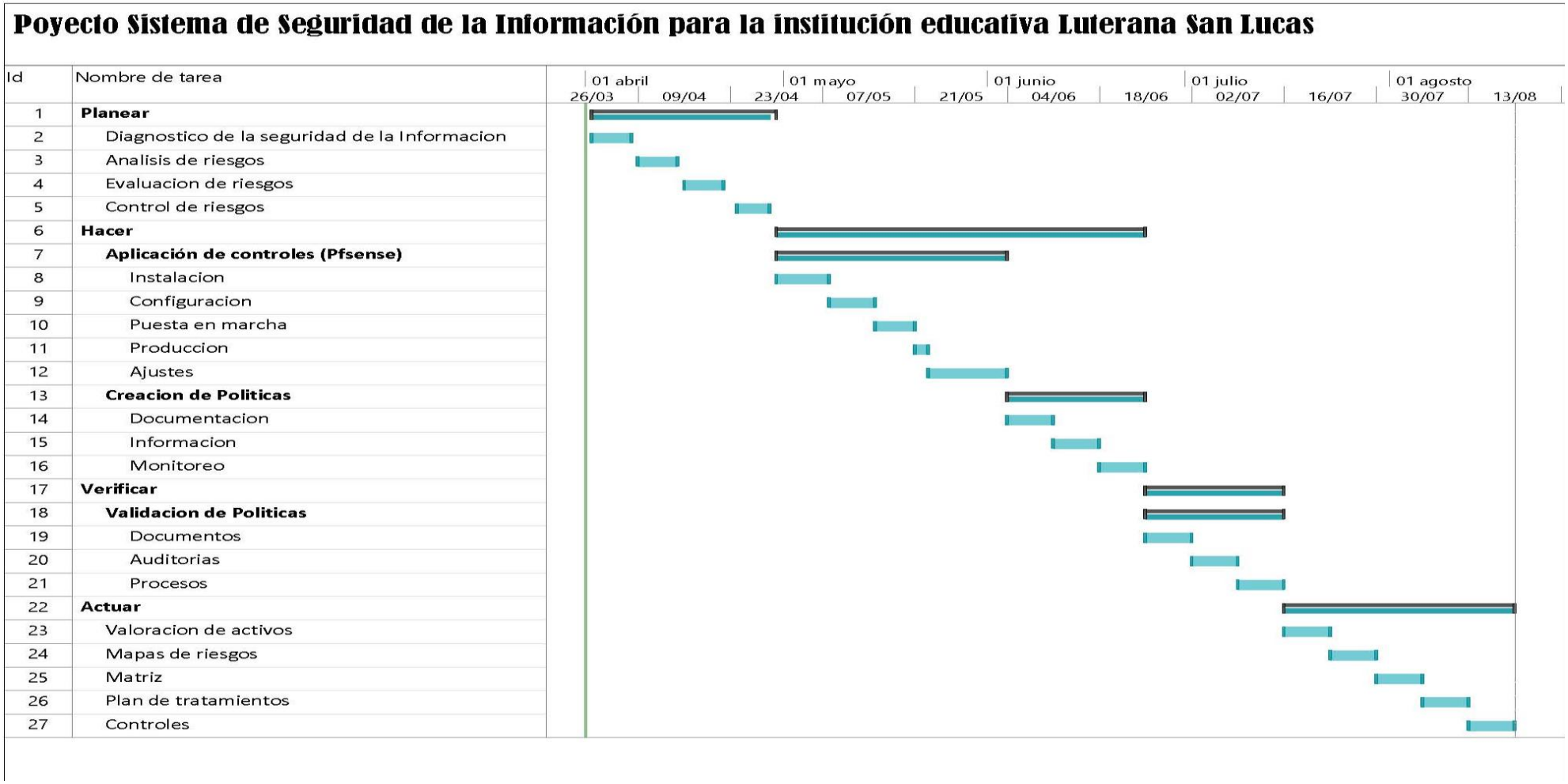


Figura 3 Cronograma de actividades

Fuente: Cronograma Autores

1.6 PRESUPUESTO DE LA IPLEMENTACIÓN

Asesoría y gastos por la implementación				
Tipo	**Descripción**	**Valor-Hora**	**Cantidad**	**Total**
Tutor 1	Asesorías para la realización del proyecto, referente a la metodología.	$ 50,000	150	$ 7,500,000
Estudiantes	Estudiantes que desarrollan e implementan el SGSI (2)	$ 40,000	12 horas semanales	$ 9,600,000
Factibilidad y recursos técnicos				
Computadores (servidores)	Equipo para la implementación del software de seguridad (Pfsense)	$ 2,500,000	1	$ 2,500,000
Computadores (portátiles)	Equipos para parametrización del software, pruebas de monitoreo y tráfico	$ 1,600,000	2	$ 3,200,000
Total, Recursos Humanos				$ 17,100,000
Total, Recursos Técnicos				$ 5,700,000
Total, otros recursos				$ 300,000
Total, Recursos Imprevistos (10%)				$ 2,310,000
Costo total implementación				***$ 25,410,000***

Tabla 1 Presupuesto de la solución

Fuente: Autores

1.7 ESTADO ACTUAL DE LA EMPRESA

El colegio evangélico luterano de Colombia (CELCO San Lucas), es una institución educativa ubicada en la ciudad de Bogotá en la calle 35 a sur # 78i 21, en la cual se encarga de brindar acceso a la educación a estudiantes en los ciclos de básica primaria, básica secundario y media superior a una población de más de 1000 estudiantes. En su parte administrativa cuenta con 16 funcionarios, servicios generales 8, el personal docente está compuesto por 36 profesionales encargados de impartir la educación y formación en todo el ciclo educativo que ofrece el colegio.

En la actualidad la empresa no cuenta con un sistema ni buenas prácticas en seguridad de la información, su infraestructura tecnológica esta soporta por un cuarto de comunicaciones que se encuentra en condiciones confusas en cuanto etiquetado y ordenamiento, ya que allí confluyen todas las redes de comunicaciones de la empresa, pero se es difícil identificar una conexión especifica si se necesitara.

Las redes de comunicación de la empresa están divididas en dos segmentos, el primero cuenta con la red de los funcionarios administrativos y el acceso a internet se hace por el proveedor UNE, el segundo segmento se encuentran los equipos de salas de sistemas , los puntos de red de cada salan desde el cual acceden los decentes con equipos suministrados por la institución, y la solución wifi con la cuenta el colegio en cada una de sus zonas, esta red se encuentra sin ningún control ni monitoreo en cuanto a restricciones de tráfico y navegabilidad y seguridad por parte de acceso de cada uno de los usuarios que hacen uso de ella.

1.8 MARCO ESTRATÉGICO

1.8.1 MISIÓN

El Colegio “CELCO SAN LUCAS “, como institución educativa de la Iglesia Luterana está comprometido con la misión de Dios, que proclama integralmente el evangelio de nuestro señor Jesucristo para la liberación y salvación del ser humano y la creación, Y conforme a ella brinda a sus estudiantes una formación Diversificada, Integral, Evangelizadora, Socializadora, Personalizada, Agradable y de Proyección, basada en principios éticos cristianos.

1.8.2 VISIÓN

Es un centro de formación que propende en fortalecer a hombres y mujeres capacitados para transformar su entorno. Es el espacio en el que una nueva generación se alista para tomar los lugares de influencia. Es el lugar donde se encaminan niños, niñas y adolescentes a una plenitud de vida, al punto que ellos se sientan realizados y nosotros satisfechos de la labor cumplida y la meta alcanzada.

1.8.3 FILOSOFIA

Somos una Institución Educativa Evangélica luterana, fundada en la doctrina bíblica que proclama en forma integral el Evangelio de Jesucristo para reconciliar al hombre con Dios, con su Prójimo y consigo mismo. La Iglesia Evangélica Luterana desde la Reforma resumió la fe cristiana evangélica en las consignas: Sola escritura, Solo Cristo, Sola Gracia, Sola Fe, desde las cuales el colegio CELCO San Lucas guía la labor pastoral y educativa.

2 DIAGNOSTICO

2.1 SITUACION ACTUAL DE LA INSTITUCION

Iniciaremos con un análisis de la situación actual del colegio Celco San Lucas, enfocándonos en identificar los puntos de seguridad vulnerables, con esto se obtiene una idea clara de la infraestructura tecnológica, Cableado estructurado, Estado de los equipos, Centros de datos, equipos de comunicación y más adelante facilitara el análisis de los riesgos y la aplicación de políticas enfocadas en la seguridad informática.

2.1.1 ANALISIS INICIAL

El Colegio Luterano San Lucas fue fundado por la Iglesia que lleva su nombre en el año 1974 para servir a la comunidad de ciudad Kennedy y sus alrededores, bajo un convenio con el distrito de Bogotá inicio como un Jardín infantil, no fue sino hasta 1992 que inicio con el grado primero y desde entonces la institución ha hecho un esfuerzo constante para tener una infraestructura tecnológica que permita impartir educación de calidad a sus alumnos, hace algunos años el Colegio realizo una ampliación estructural en la que se instalaron salones computacionales más grandes y en donde fue necesario realizar adecuaciones tecnológicas nuevas pero que permitieron tener una infraestructura mucho más robusta.

2.1.2 CABLEADO ESTRUCTURADO

Actualmente la institución tiene un lugar dedicado para resguardar los equipos de comunicaciones, este lugar está ubicado a la entrada principal de la institución debajo de la escalera que lleva a los salones de primaria, en este sitio se encuentran los equipos de comunicaciones de los dos proveedores de internet (etb y claro), el firewall de seguridad, servidor de aplicaciones y concentra todo el cableado del colegio, planta telefónica, está protegido por una puerta con láminas que funciona como persiana ideal para que se ventile, una chapa de seguridad y dos ventiladores de pared, a partir de este punto se desprende el backbone que alimenta las salas de sistemas ubicadas en el 5 piso del bloque de bachillerato, el cableado es categoría 6, el rack de telecomunicaciones se encuentra bastante desorganizado y no están identificados correctamente los equipos de comunicación, este lugar se considera el centro de datos principal del instituto.

2.1.3 PERSONAL Y ESTRUCTURA ORGANIZACIONAL

La institución educativa en su estructura organizacional cuentas con empleados en la cual la rectora se encuentra a la cabeza del organigrama jerárquico de la institución, la parte administrativa consta del área de contabilidad integrada por tres personas, el área de sistemas, secretaria y rectoría por una persona en cada área, la parte de iglesia está compuesta por dos personas que son la capellana y el pastor. El área de servicios generales se cuenta con 5 personas, el área de seguridad cuenta con 4 personas, los servicios de enfermería y salud ocupacional por una persona al igual que los servicios de mantenimiento.

En el nivel educativo encontramos a los 36 docentes que imparten sus clases en los ciclos de básica primaria, básica secundaria y media superior, tiene como jefes inmediatos a los coordinadores de convivencia y académica, el apoyo para el manejo de casos que requieran manejo especial se realiza por medio del psicólogo del colegio.

2.1.4 INFORMACIÓN ACTIVOS

Se deben identificar todos y cada uno de los activos que hacen parte de la infraestructura tecnológica del instituto para posteriormente hacer una valoración y priorizar los equipos o servicios críticos para la prestación del servicio educativo del Colegio, según el estándar ISO 27005:2008, se definen seis distintos tipos específicos de activos:

- Dato: Información que se genera, envía, recibe y gestionan dentro de la organización. Dentro de este tipo, podemos encontrar distintos documentos que la institución educativa gestiona dentro de sus procesos.

- Aplicación: Todo aquel software que se utilice como soporte en los procesos.

- Servicio: Son los servicios que alguna área de la organización suministra a otra área o entidades externas a la misma.

- Tecnología: Es todo el hardware donde se maneje la información y las comunicaciones.

- Instalación: Es cualquier lugar donde se alojan los activos de información. Este lugar o ambiente puede estar ubicado dentro de la organización tanto como fuera de la misma.

- Equipamiento auxiliar: Son los activos que no se hallan definidos en ninguno de los anteriores tipos.

Con base en los seis tipos de activos nombrados anteriormente se usó la base de datos de equipos tecnológicos de la institución como referencia para crear la siguiente tabla.

ITEM	TIPO	DESCIPCIÓN	RESPONSABLE
1	**COMPUTADOR**	PROCESADOR INTEL CELERON (430) 1,8 GHZ, 1GB MEMORIA RAM DDR2, 250 GB DISCO DURO	CONSUELO PRECIADO
2	**MONITOR**	14 PULGADAS	CONSUELO PRECIADO
3	**COMPUTADOR**	COMPUTADOR CON PROCESADOR INTEL CELERON (E5200) 2,5 GHZ, 4GB MEMORIA RAM DDR2, 250 GB DISCO DURO	JANNETH COLMENARES
4	**IMPRESORA**	MULTIFUNCIONAL HP LASERJET M2727NF	JANNETH COLMENARES
5	**MONITOR**	MONITOR DE 19"	JANNETH COLMENARES
6	**MONITOR**	19 PULGADAS	NUBIA GUALDRON
7	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 4 GB DDR3	NUBIA GUALDRON
8	**IMPRESORA**	IMPRESORA EPSON L800 RECARGA DE TINTAS	NUBIA GUALDRON
9	**TELÉFONO ANALOGO**	TELÉFONO ANÁLOGO PANASONIC	NUBIA GUALDRON

ITEM	TIPO	DESCIPCIÓN	RESPONSABLE
10	**VIDEO BEAM**	COLOR GRIS PLATEADO	JOHN ROJAS
11	**COMPUTADOR**	Janus CORE I3 (2100) A 3,1 GHZ, 4 GB RAM, 1TB GB DISCO DURO	JOHN ROJAS
12	**PARLANTE**	PARLANTE DE GRAVES, DOS PARLANTES PEQUEÑOS, CONTROL DE VOLUMEN, CONEXIÓN AURICULARES	JOHN ROJAS
13	**VIDEO BEAM**	COLOR NEGRO, CON ESTUCHE, CABLE DE PODER	JOHN ROJAS
14	**IMPRESORA**	LASER ML 2240	ALBERTO CEPEDA
15	TELEFONO	PANASONIC KX-TS500 LXB	ALBERTO CEPEDA
16	**COMPUTADOR**	CON PROCESADOR INTEL CELERON (430) 1,8 GHZ, 2GB MEMORIA RAM DDR2, 500 GB DISCO DURO	ALBERTO CEPEDA
17	**IMPRESORA**	LASERJET 2014N BLANCA	DIANA VERA
18	**TELEFONO**	ANALOGO NEGRO	DIANA VERA
19	**TELEFONO**	ANALOGO NEGRO	JESUS GAMBOA
20	**IMPRESORA**	IMPRESORA HP LASERJET 1102W NEGRA	JESUS GAMBOA
21	**MONITOR**	16 PULGADAS NEGRO	JESUS GAMBOA
22	**COMPUTADOR**	CON BOART N68S PROCESADOR AMD SEMPROM (130) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3	JESUS GAMBOA
23	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	DEPARTAMENTO DE SISTEMAS
24	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3	DEPARTAMENTO DE SISTEMAS
25	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	DEPARTAMENTO DE SISTEMAS
26	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR4	DEPARTAMENTO DE SISTEMAS
27	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	DEPARTAMENTO DE SISTEMAS
28	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR5	DEPARTAMENTO DE SISTEMAS
29	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	DEPARTAMENTO DE SISTEMAS
30	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR6	DEPARTAMENTO DE SISTEMAS
31	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	DEPARTAMENTO DE SISTEMAS
32	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR7	DEPARTAMENTO DE SISTEMAS
33	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	DEPARTAMENTO DE SISTEMAS
34	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR8	DEPARTAMENTO DE SISTEMAS
35	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	DEPARTAMENTO DE SISTEMAS
36	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR9	DEPARTAMENTO DE SISTEMAS
37	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ,	DEPARTAMENTO DE SISTEMAS

ITEM	TIPO	DESCIPCIÓN	RESPONSABLE
		DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	
38	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR10	DEPARTAMENTO DE SISTEMAS
39	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	DEPARTAMENTO DE SISTEMAS
40	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR11	DEPARTAMENTO DE SISTEMAS
41	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	DEPARTAMENTO DE SISTEMAS
42	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR12	DEPARTAMENTO DE SISTEMAS
43	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	DEPARTAMENTO DE SISTEMAS
44	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	DEPARTAMENTO DE SISTEMAS
45	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR13	DEPARTAMENTO DE SISTEMAS
46	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	DEPARTAMENTO DE SISTEMAS
47	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR14	DEPARTAMENTO DE SISTEMAS
48	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	DEPARTAMENTO DE SISTEMAS
49	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR15	DEPARTAMENTO DE SISTEMAS
50	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	DEPARTAMENTO DE SISTEMAS
51	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR16	DEPARTAMENTO DE SISTEMAS
52	**COMPUTADOR**	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	DEPARTAMENTO DE SISTEMAS
53	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
54	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
55	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
56	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
57	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
58	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS

ITEM	TIPO	DESCIPCIÓN	RESPONSABLE
59	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
60	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
61	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
62	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
63	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
64	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
65	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
66	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
67	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
68	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
69	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
70	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
71	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
72	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
73	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
74	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
75	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
76	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
77	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
78	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
79	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
80	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
81	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
82	**MONITOR**	19 PULGADAS LED MARCA JANUS	DEPARTAMENTO DE SISTEMAS
83	**COMPUTADOR PORTATIL**	PLATEADO, MARCA HP 69309 PROCESSDRO INTEL CORE DOS DUO 2 GB MEMORIA RAM, CON CARGADOR	DEPARTAMENTO DE SISTEMAS
84	**COMPUTADOR PORTATIL**	PLATEADO, MARCA HP 69309 PROCESSDRO INTEL CORE DOS DUO 2 GB MEMORIA RAM, CON CARGADOR	DEPARTAMENTO DE SISTEMAS
85	**COMPUTADOR PORTATIL**	PLATEADO, MARCA HP 69309 PROCESSDRO INTEL CORE DOS DUO 2 GB MEMORIA RAM, CON CARGADOR	DEPARTAMENTO DE SISTEMAS
86	**COMPUTADOR PORTATIL**	PLATEADO, MARCA HP 69309 PROCESSDRO INTEL CORE DOS DUO 2 GB MEMORIA RAM, CON CARGADOR	DEPARTAMENTO DE SISTEMAS
87	**COMPUTADOR PORTATIL**	PLATEADO, MARCA HP 69309 PROCESSDRO INTEL CORE DOS DUO 2 GB MEMORIA RAM, CON CARGADOR	DEPARTAMENTO DE SISTEMAS
88	**COMPUTADOR PORTATIL**	PLATEADO, MARCA HP 69309 PROCESSDRO INTEL CORE DOS DUO 2 GB MEMORIA RAM, CON CARGADOR	DEPARTAMENTO DE SISTEMAS
89	SWITCH	24 PUERTOS TP_LINK TL-SG1024, SERIAL 10CA0600349	DEPARTAMENTO DE SISTEMAS
90	SWITCH	SWITCH 24 PUERTOS TP_LINK TL-SG1024 SERIAL 10CA0600350	DEPARTAMENTO DE SISTEMAS
91	SWITCH	SWITCH 48 PUERTOS TP_LINK TL-SG1048	DEPARTAMENTO DE SISTEMAS
92	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG52716NZ	MARTIN BARAJAS

ITEM	TIPO	DESCIPCIÓN	RESPONSABLE
93	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG527200S	JENNY LEON
94	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG527287N	ANGELA BOHORQUEZ
95	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG52728CH	CESAR PAREDES
96	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG52728GL	ANYUL STEAK FIGUEROA
97	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG52728YX	SANDRA FORERO
98	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG52729BC	MANUEL GERARDO ACOSTA
99	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG5272BG1	MARLENY MONTOYA
100	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG5272C50	DIEGO OLAVE
101	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG5271Y8X	YENNY SABRINA LIZCANO
102	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG527208N	JOSE BOLAÑOS
103	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG5272881	DIANA VERA
104	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG52728CX	LUISA FERANDA PORRAS
105	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG52728QK	MARTHA DIAZ
106	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG5272960	CAROLINA VARON
107	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG52729BY	ANDRES CAMILO MENDEZ
108	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG5272BG5	CINDY BLANCO / ENED GARCIA
109	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG5272CR1	ALEJANDRO CIFUENTES
110	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG5271ZN3	SANDRA PALACIOS
111	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG527208Z	LEIDY LINARES
112	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG527288H	LISA SAENZ
113	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG52728FD	DIEGO CELY
114	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG52728QS	OLGA LEAL
115	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG527297T	SANDRA TAMAYO
116	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG52729W6	PASTOR JOHN ROJAS
117	**COMPUTADOR PORTATIL**	HP 240 G4 SERIAL 5CG5272BQP	MARIA FERNANDA MORENO
118	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4902608	JENNY LEON
119	VIDEO BEAM	EPSON POWERLITE SERIALU43K4902771	HENRRY ROJAS
120	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4902806	ANGELA BOHORQUEZ
121	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4902819	ANYUL STEAK FIGUEROA
122	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4903299	SABRINA LIZCANO
123	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4903375	ALEJANDRO CIFUENTES
124	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4903446	DIEGO OLAVE
125	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4903487	GERARDO ACOSTA
126	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4903545	JEFFERSSON CORTES
127	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4902751	PATRICIA MARTINEZ
128	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4902792	EDWIN NARANJO / ASTRID BERNAL
129	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4902816	EDWIN NARANJO / ASTRID BERNAL
130	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4902823	SANDRA TAMAYO
131	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4903346	CINDY BLANCO

ITEM	TIPO	DESCIPCIÓN	RESPONSABLE
132	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4903389	CESAR PAREDES
133	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4903452	WILLIAM GARZON
134	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4903497	JOSE BOLAÑOS
135	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4903556	MARTIN BARAJAS
136	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4902754	MARISOL RUBIO
137	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4902805	JOHN ROJAS
138	VIDEO BEAM	EPSON POWERLITE SERIAL U43K49022818	OLGA LEAL
139	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4902824	ASTRID BERNAL
140	VIDEO BEAM	EPSON POWERLITE SERIAL U43K49023352	IGLESIA
141	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4903428	SANDRA FORERO
142	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4903459	CAROLINA VARON
143	VIDEO BEAM	EPSON POWERLITE SERIAL U43K4903504	DIEGO CELY
144	DVR	VIDEO GRABADOR DAHUA HCVR5116HS3 2J50A1DPAPFZ2YZ	DEPARTAMENTO SISTEMAS
144	**DVR**	VIDEO GRABADOR nahua HCVR5116HS3 serial 2J50A1DPAPF633N	DEPARTAMENTO DE SISTEMAS
145	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
146	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
147	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
148	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
149	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
150	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
151	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
152	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
153	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
154	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
155	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
156	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
157	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
158	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
159	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
160	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
161	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
162	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
163	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
164	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
165	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
166	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
167	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
168	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
169	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS

ITEM	TIPO	DESCIPCIÓN	RESPONSABLE
170	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
171	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
172	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
173	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
174	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
175	CAMARA	ANALOGA HIKVISION	DEPARTAMENTO DE SISTEMAS
177	SERVICIO	Internet fibra óptica UNE 20MB	DEPARTAMENTO DE SISTEMAS
178	SERVICIO	internet ETB 150MBV Fibra Óptica	DEPARTAMENTO DE SISTEMAS
179	SERVICIO	página web	DEPARTAMENTO DE SISTEMAS
180	SERVICIO	telefonía	DEPARTAMENTO DE SISTEMAS
181	APLICACIÓN	Sigecol	DEPARTAMENTO DE SISTEMAS
182	APLICACIÓN	dhs	DEPARTAMENTO DE SISTEMAS
183	APLICACIÓN	pfsense	DEPARTAMENTO DE SISTEMAS
184	APLICACIÓN	unifi controler	DEPARTAMENTO DE SISTEMAS
185	SERVIDOR	servidor Sigecol procesador Intel Core i7 6200 8 GB Memoria RAM, 1 TB Disco Duro	DEPARTAMENTO DE SISTEMAS
186	SERVIDOR	seguridad pfsense procesador Intel Core i3 2100 4 GB memoria RAM 1TB Disco duro	DEPARTAMENTO DE SISTEMAS
187	PLANTA	telefonía Panasonic kx-tes824	DEPARTAMENTO DE SISTEMAS
188	INSTALACIÓN	centro de computo	DEPARTAMENTO DE SISTEMAS
189	INSTALACIÓN	UPS de 15 KVA	DEPARTAMENTO DE SISTEMAS
190	INSTALACIÓN	Ups de 10 KVA	DEPARTAMENTO DE SISTEMAS
191	ACCES POINT	ubiquiti uap ac pro	DEPARTAMENTO DE SISTEMAS
192	ACCES POINT	ubiquiti uap ac pro	DEPARTAMENTO DE SISTEMAS
193	ACCES POINT	ubiquiti uap ac pro	DEPARTAMENTO DE SISTEMAS
194	ACCES POINT	ubiquiti uap ac pro	DEPARTAMENTO DE SISTEMAS
195	ACCES POINT	ubiquiti uap ac pro	DEPARTAMENTO DE SISTEMAS
196	ACCES POINT	ubiquiti uap ac pro	DEPARTAMENTO DE SISTEMAS
197	ACCES POINT	ubiquiti uap ac pro	DEPARTAMENTO DE SISTEMAS
198	CONTROLADORA WIFI	ubiquiti cloud key Controler	DEPARTAMENTO DE SISTEMAS

Tabla 2 Inventario Activos

Fuente: Base de Datos Activos CELCO San Lucas

La tabla enumera el tipo de activo, la descripción y el área o persona responsable, adicional se identificaron y enumeraron los servicios, aplicaciones e infraestructura para obtener una base de datos consistentes de los equipos que son parte de la infraestructura tecnológica.

2.2 DIAGNOSTICO DE SEGURIDAD

La Institución actualmente no cuenta con un sistema de seguridad de la información definido, esto conlleva a que los datos del colegio estén en un nivel de riesgo muy alto de recibir ataques informáticos, pérdida o alteración de la información. La identificación de activos, servicios e infraestructura del colegio, así como el análisis del personal administrativo y docente permitió encontrar los siguientes puntos críticos:

- Falta de conocimiento en temas de seguridad del personal administrativo y docente.
- Ausencia de políticas documentadas para el manejo de equipos, accesos y redes.
- Muy poco seguimiento y trazabilidad de incidentes de seguridad.
- Instalaciones sin controles de acceso.
- Falta de seguridad en los equipos.
- Controles de navegación insuficientes para salas de sistemas.
- No existe una valoración de activos que permita identificar los dispositivos vitales para la operación del colegio.
- No tiene un proceso de backup documentado donde se asegure la información vital de la institución.

Con base en los anteriores puntos de seguridad identificados se ve la necesidad de plantear un Sistema de Gestión de Seguridad de la Información que este alineado con los procesos de cada una de las áreas de la institución, reduzca los niveles de riesgo y permita la normal operación del servicio de educación que imparten.

3 ANALISIS DE RIESGOS

3.1 VALORACIÓN DE RIESGOS

Luego de realizar un diagnóstico de la situación actual del Instituto, la valoración de activos es un paso fundamental para iniciar con un análisis de riesgos, aquí se identifican los puntos críticos que podrían afectar la operación del colegio, para tal fin se creó una tabla con tres criterios de valoración, la disponibilidad, integridad y la confidencialidad cada uno con un rango de valores que van desde el numero 0 hasta el número 3 y su correspondiente descripción.

CRITERIO	VALOR	DESCRIPCION
Disponibilidad	1	No Aplica / No es relevante
	2	Debe estar disponible al menos un 50% del tiempo
	3	Debe estar disponible siempre
Integridad	1	No Aplica / No es relevante
	2	Tiene que estar correcto y completo al menos un 50%
	3	Tiene que estar correcto y completo un 100%
Confidencialidad	1	No Aplica / No es relevante
	2	Los daños serian relevantes y el incidente implicaría varias áreas
	3	Los daños serian catastróficos, la reputación e imagen la de institución se vería comprometida

Figura 4 Valoración de riesgos

Fuente: Autores

3.1.1 UNIVERSO DE VALORES

La sumatoria de los criterios de disponibilidad, integridad y confidencialidad estará en un rango del 0 a 9, para facilitar la identificación de los activos más críticos visualmente se creó la siguiente tabla de colores.

VALOR	CRITICO
0	
1	Bajo
2	Bajo
3	Bajo
4	Medio
5	Medio
6	Medio
7	Alto
8	Alto
9	Alto

Tabla 3 Clasificación de los valores

Fuente: Autores

3.1.2 VALORACIÓN DE LOS ACTIVOS

Ahora tomaremos cada uno de los activos y se le asignara un valor según el criterio de Integridad, disponibilidad y criticidad, la sumatoria de estos 3 ítems dará un número que se identificara con el color de la tabla de "clasificación de valores" y esto determina su criticidad para el instituto.

10	*ACTIVO*	CARACTERISTICAS	CRITERIO			VALOR TOTAL	CRITICIDA
			INTEG	DISPON	CONFD		
1	*COMPUTADOR*	PROCESADOR INTEL CELERON (430) 1,8 GHZ, 1GB MEMORIA RAM DDR2, 250 GB DISCO DURO	3	3	3	9	
2	*MONITOR*	14 PULGADAS	1	1	1	3	
3	*COMPUTADOR*	COMPUTADOR CON PROCESADOR INTEL CELERON (E5200) 2,5 GHZ, 4GB MEMORIA RAM DDR2, 250 GB DISCO DURO	1	2	1	4	
4	*IMPRESORA*	MULTIFUNCIONAL HP LASERJET M2727NF	1	2	1	4	
5	*MONITOR*	MONITOR DE 19"	1	1	1	3	
6	*MONITOR*	19 PULGADAS	1	1	1	3	
7	*COMPUTADOR*	JANUS BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 4 GB DDR3	1	1	1	3	
8	*IMPRESORA*	IMPRESORA EPSON L800 RECARGA DE TINTAS	1	2	1	4	
9	*TELÉFONO ANALOGO*	TELÉFONO ANÁLOGO PANASONIC	1	1	1	3	
10	*VIDEO BEAM*	COLOR GRIS PLATEADO	1	1	1	3	
11	*COMPUTADOR*	Janus CORE I3 (2100) A 3,1 GHZ, 4 GB RAM, 1TB GB DISCO DURO	3	3	3	9	
12	*PARLANTE*	PARLANTE DE GRAVES, DOS PARLANTES PEQUEÑOS, CONTROL DE VOLUMEN, CONEXIÓN AURICULARES	1	1	1	3	
13	*VIDEO BEAM*	COLOR NEGRO, CON ESTUCHE, CABLE DE PODER	2	2	1	5	

10	ACTIVO	CARACTERISTICAS	CRITERIO			VALOR TOTAL	CRITICIDA
			INTEG	DISPON	CONFD		
14	*IMPRESORA*	LASER ML 2240	1	2	1	4	
15	*TELEFONO*	PANASONIC KX-TS500 LXB	1	1	1	3	
16	*COMPUTADOR*	CON PROCESADOR INTEL CELERON (430) 1,8 GHZ, 2GB MEMORIA RAM DDR2, 500 GB DISCO DURO	1	2	3	6	
17	*IMPRESORA*	LASERJET 2014N BLANCA	1	2	1	4	
18	*TELEFONO*	ANALOGO NEGRO	1	1	1	3	
19	*TELEFONO*	ANALOGO NEGRO	1	1	1	3	
20	*IMPRESORA*	IMPRESORA HP LASERJET 1102W NEGRA	1	2	1	4	
21	*MONITOR*	16 PULGADAS NEGRO	1	1	1	3	
22	*COMPUTADOR*	CON BOART N68S PROCESADOR AMD SEMPROM (130) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3	1	2	1	4	
23	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	1	1	1	3	
24	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3	1	1	1	3	
25	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	1	1	1	3	
26	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR4	1	1	1	3	
27	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	1	1	1	3	
28	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR5	1	1	1	3	
29	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	1	1	1	3	
30	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR6	1	1	1	3	
31	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	1	1	1	3	
32	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR7	1	1	1	3	
33	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	1	1	1	3	
34	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR8	1	1	1	3	
35	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	1	1	1	3	
36	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR9	1	1	1	3	
37	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL	1	1	1	3	

10	*ACTIVO*	CARACTERISTICAS	CRITERIO			VALOR TOTAL	CRITICIDA
			INTEG	DISPON	CONFD		
		CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,					
38	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR10	1	1	1	3	
39	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	1	1	1	3	
40	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR11	1	1	1	3	
41	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	1	1	1	3	
42	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR12	1	1	1	3	
43	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	1	1	1	3	
44	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	1	1	1	3	
45	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR13	1	1	1	3	
46	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	1	1	1	3	
47	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR14	1	1	1	3	
48	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	1	1	1	3	
49	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR15	1	1	1	3	
50	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	1	1	1	3	
51	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR16	1	1	1	3	
52	*COMPUTADOR*	JANUS CON BOART ELITE GROUP H61M PROCESADOR INTEL CELERON (G550) A 2,6 GHZ, DISCO DURO DE 500GB, MEMORIA RAM DE 2 GB DDR3,	1	1	1	3	
53	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
54	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
55	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
56	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
57	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
58	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
59	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	

10	*ACTIVO*	CARACTERISTICAS	CRITERIO			VALOR TOTAL	CRITICIDA
			INTEG	DISPON	CONFD		
60	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
61	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
62	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
63	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
64	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
65	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
66	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
67	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
68	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
69	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
70	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
71	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
72	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
73	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
74	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
75	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
76	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
77	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
78	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
79	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
80	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
81	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
82	*MONITOR*	19 PULGADAS LED MARCA JANUS	1	1	1	3	
83	*COMPUTADOR PORTATIL*	PLATEADO, MARCA HP 69309 PROCESSDRO INTEL CORE DOS DUO 2 GB MEMORIA RAM, CON CARGADOR	2	2	3	7	
84	*COMPUTADOR PORTATIL*	PLATEADO, MARCA HP 69309 PROCESSDRO INTEL CORE DOS DUO 2 GB MEMORIA RAM, CON CARGADOR	2	3	3	8	
85	*COMPUTADOR PORTATIL*	PLATEADO, MARCA HP 69309 PROCESSDRO INTEL CORE DOS DUO 2 GB MEMORIA RAM, CON CARGADOR	2	3	2	7	
86	*COMPUTADOR PORTATIL*	PLATEADO, MARCA HP 69309 PROCESSDRO INTEL CORE DOS DUO 2 GB MEMORIA RAM, CON CARGADOR	3	3	2	8	
87	*COMPUTADOR PORTATIL*	PLATEADO, MARCA HP 69309 PROCESSDRO INTEL CORE DOS DUO 2 GB MEMORIA RAM, CON CARGADOR	2	3	2	7	
88	*COMPUTADOR PORTATIL*	PLATEADO, MARCA HP 69309 PROCESSDRO INTEL CORE DOS DUO 2 GB MEMORIA RAM, CON CARGADOR	3	3	2	8	
89	*SWITCH*	24 PUERTOS TP_LINK TL-SG1024, SERIAL 10CA0600349	3	3	3	9	
90	*SWITCH*	SWITCH 24 PUERTOS TP_LINK TL-SG1024 SERIAL 10CA0600350	3	3	3	9	
91	*SWITCH*	SWITCH 48 PUERTOS TP_LINK TL-SG1048	3	3	3	9	
92	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG52716NZ	1	2	1	4	
93	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG527200S	1	2	1	4	
94	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG527287N	1	2	1	4	

10	*ACTIVO*	CARACTERISTICAS	CRITERIO			VALOR TOTAL	CRITICIDA
			INTEG	DISPON	CONFD		
95	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG52728CH	1	2	1	4	
96	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG52728GL	1	2	1	4	
97	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG52728YX	1	2	1	4	
98	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG52729BC	1	2	1	4	
99	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG5272BG1	1	2	1	4	
100	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG5272C50	1	2	1	4	
101	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG5271Y8X	1	2	1	4	
102	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG527208N	1	2	1	4	
103	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG5272881	1	2	1	4	
104	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG52728CX	1	2	1	4	
105	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG52728QK	1	2	1	4	
106	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG5272960	1	2	1	4	
107	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG52729BY	1	2	1	4	
108	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG5272BG5	1	2	1	4	
109	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG5272CR1	1	2	1	4	
110	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG5271ZN3	1	2	1	4	
111	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG527208Z	1	2	1	4	
112	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG527288H	1	2	1	4	
113	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG52728FD	1	2	1	4	
114	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG52728QS	1	2	1	4	
115	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG527297T	1	2	1	4	
116	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG52729W6	1	2	1	4	
117	*COMPUTADOR PORTATIL*	HP 240 G4 SERIAL 5CG5272BQP	1	2	1	4	
118	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4902608	1	1	1	3	
119	*VIDEO BEAM*	EPSON POWERLITE SERIALU43K4902771	1	1	1	3	
120	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4902806	1	1	1	3	
121	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4902819	1	1	1	3	
122	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4903299	1	1	1	3	
123	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4903375	1	1	1	3	
124	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4903446	1	1	1	3	
125	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4903487	1	1	1	3	
126	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4903545	1	1	1	3	
127	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4902751	1	1	1	3	
128	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4902792	1	1	1	3	
129	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4902816	1	1	1	3	
130	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4902823	1	1	1	3	
131	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4903346	1	1	1	3	
132	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4903389	1	1	1	3	
133	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4903452	1	1	1	3	

10	*ACTIVO*	CARACTERISTICAS	CRITERIO			VALOR TOTAL	CRITICIDA
			INTEG	DISPON	CONFD		
134	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4903497	1	1	1	3	
135	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4903556	1	1	1	3	
136	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4902754	1	1	1	3	
137	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4902805	1	1	1	3	
138	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K49022818	1	1	1	3	
139	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4902824	1	1	1	3	
140	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K49023352	1	1	1	3	
141	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4903428	1	1	1	3	
142	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4903459	1	1	1	3	
143	*VIDEO BEAM*	EPSON POWERLITE SERIAL U43K4903504	1	1	1	3	
144	*DVR*	VIDEO GRABADOR DAHUA HCVR5116HS3 2J50A1DPAPFZ2YZ	2	3	3	8	
145	*DVR*	VIDEO GRABADOR dahua HCVR5116HS3 serial 2J50A1DPAPF633N	2	3	2	7	
146	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
147	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
148	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
149	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
150	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
151	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
152	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
153	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
154	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
155	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
156	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
157	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
158	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
159	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
160	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
161	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
162	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
163	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
164	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
165	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
166	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
167	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
168	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
169	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
170	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
171	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
172	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	

10	*ACTIVO*	CARACTERISTICAS	CRITERIO			VALOR TOTAL	CRITICIDA
			INTEG	DISPON	CONFD		
173	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
174	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
175	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
176	*CAMARA*	ANALOGA HIKVISION	1	2	1	4	
177	*SERVICIO*	Internet fibra óptica UNE 20MB	3	3	3	9	
178	*servicio*	internet ETB 150MBV Fibra Óptica	3	3	3	9	
179	*servicio*	página web	1	1	1	3	
180	*servicio*	telefonía	3	3	2	8	
181	*aplicación*	Sigecol	3	3	3	9	
182	*aplicación*	dhs	3	2	2	7	
183	*aplicación*	pfsense	3	3	3	9	
184	*aplicación*	unifi controler	1	1	1	3	
185	*servidor*	servidor Sigecol procesador Intel Core i7 6200 8 GB Memoria RAM, 1 TB Disco Duro	3	3	3	9	
186	*servidor*	seguridad pfsense procesador Intel Core i3 2100 4 GB memoria RAM 1TB Disco duro	3	3	3	9	
187	*planta*	telefonía Panasonic kx-tes824	3	3	3	9	
188	*Instalación*	centro de computo	3	3	3	9	
189	*Instalación*	UPS de 15 KVA	2	2	2	6	
190	*instalación*	Ups de 10 KVA	2	2	2	6	
191	*Acces point*	ubiquiti uan ac pro	1	2	1	4	
192	*Acces point*	ubiquiti uan ac pro	1	2	1	4	
193	*Acces point*	ubiquiti uan ac pro	1	2	1	4	
194	*Acces point*	ubiquiti uan ac pro	1	2	1	4	
195	*Acces point*	ubiquiti uan ac pro	1	2	1	4	
196	*Acces point*	ubiquiti uan ac pro	1	2	1	4	
197	*Acces point*	ubiquiti uan ac pro	1	2	1	4	
198	*Controladora wifi*	ubiquiti cloud key Controler	1	1	1	3	

Tabla 4 Valoración de activos

Fuente: Autores

3.1.3 MAPA DE RIESGOS

El mapa de riesgos permite hacer una clasificación haciendo un cruce entre los niveles de impacto y la probabilidad de afectación, para realizar una ponderación de estas variables se deben tener dos tablas, una con la probabilidad de afectación y otra con el impacto en el negocio, para ambas tablas se asignan 5 niveles iniciando desde muy alto y finalizando en muy bajo.

Probabilidad de Afectación	Interpretación
Muy Alta	Es casi seguro que la amenaza afectará la vulnerabilidad.
Alta	Es probable que la amenaza afectará la vulnerabilidad.
Media	Es posible que la amenaza afectará la vulnerabilidad.
Baja	Es improbable que la amenaza afectará la vulnerabilidad.
Muy Baja	Es impensable que la amenaza afectará la vulnerabilidad.

Tabla 5 Impacto en el negocio

Fuente: Autores

Impacto en el Negocio	Interpretación
Muy Alto	Afecta a toda la institución educativa o por más de una semana las operaciones del instituto.
Alto	Afecta varias áreas en particular o hasta en 72 horas las operaciones del instituto.
Medio	Afecta a un área en particular o hasta en 24 horas las operaciones del instituto.
Bajo	Afecta a un usuario en particular o hasta en 6 horas las operaciones del instituto.
Muy Bajo	Tiene un efecto nulo o muy pequeño en las operaciones del instituto educativo.

Tabla 6 Probabilidad de afectación

Fuente: Autores

El cruce de las dos tablas genera una nueva clasificación de riesgos que tiene los siguientes niveles:

- Bajo: El riesgo tiene muy poca probabilidad de ocurrencia y su impacto es mínimo en el negocio
- Moderado: El riesgo tiene una probabilidad de ocurrencia medio-baja y su impacto podría afectar una persona en específico.
- Relevante: El riesgo tiene una probabilidad de ocurrencia media y su impacto podría afectar varias personas o un área entera.
- Alto: El riesgo tiene una probabilidad de ocurrencia alta y su impacto podría afectar varias áreas.
- Crítico: El riesgo tiene una probabilidad de ocurrencia muy alta y su impacto podría afectar la operación del instituto.

Impacto en el Negocio	Probabilidad de Afectación				
	Muy Baja	Baja	Media	Alta	Muy Alta
Muy alto	Relevante	Relevante	Alto	Critico	Critico
Alto	Relevante	Relevante	Alto	Alto	Critico
Medio	Moderado	Moderado	Relevante	Alto	Critico
Bajo	Bajo	Bajo	Bajo	Moderado	Relevante
Muy Bajo	Bajo	Bajo	Bajo	Bajo	Moderado

Tabla 7 Mapa de Riesgos

Fuente: Autores

3.1.4 MATRIZ DE RIESGOS

Teniendo definido los niveles de riesgos que dependerán de las tablas de Probabilidad de afectación y el Impacto en el Negocio se enumeran cada uno de los activos identificados como equipos, servicios e infraestructura y se identifican los niveles de riesgos para cada uno para posteriormente aplicar las políticas y controles necesarios para mitigar la ocurrencia de riesgos haciendo énfasis en los niveles alto y crítico.

ITEM	DESCRIPCION	CANTIDAD	TIPO	VULNERABILIDAD	NIVEL AMENAZA	NIVEL AFECTACION	IMPACTO	NIVEL DE RIESGO
1	EQUIPOS ADMINISTRATIVOS	5	INFORMATICO	Falta de cierre de sesión al momento de salir de la estación de trabajo	Manipulación de información	Media	Muy Bajo	Bajo
			FISICO	Sensibilidad de golpes o caídas	Destrucción de equipos o medios de comunicación	Alta	Muy Bajo	Bajo
			INFORMATICO	Virus Informáticos	Destrucción de información	Alta	Muy Bajo	Bajo
			FISICO	Falla en los dispositivos físicos del equipo	Avería de origen físico o lógico	Media	Muy Bajo	Bajo
2	EQUIPOS PROFESORES	26	INFORMATICO	Falta de cierre de sesión al momento de salir de la estación de trabajo	Manipulación de información	Media	Muy Bajo	Bajo
			FISICO	Sensibilidad de golpes o caídas	Destrucción de equipos o medios de comunicación	Alta	Muy Bajo	Bajo
			INFORMATICO	Virus Informáticos	Destrucción de información	Alta	Muy Bajo	Bajo
			FISICO	Falla en los dispositivos físicos del equipo	Avería de origen físico o lógico	Media	Muy Bajo	Bajo
3	EQUIPOS SALAS DE SISTEMAS	60	INFORMATICO	Falta de cierre de sesión al momento de salir de la estación de trabajo	Manipulación de información	Media	Muy Bajo	Bajo
			FISICO	Sensibilidad de golpes o caídas	Destrucción de equipos o medios de comunicación	Alta	Muy Bajo	Bajo
			INFORMATICO	Virus Informáticos	Destrucción de información	Alta	Muy Bajo	Bajo

ITEM	DESCRIPCION	CANTIDAD	TIPO	VULNERABILIDAD	NIVEL AMENAZA	NIVEL AFECTACION	IMPACTO	NIVEL DE RIESGO
			FISICO	Falla en los dispositivos físicos del equipo	Avería de origen físico o lógico	Media	Muy Bajo	Bajo
4	MONITORES	60	FISICO	Sensibilidad a la humedad, polvo y al calor	Polvo, Corrosión, Temperaturas	Muy Bajo	Muy Bajo	Bajo
			FISICO	Sensibilidad de golpes o caídas	Destrucción de equipos o medios de comunicación	Media	Media	Relevante
5	IMPRESORAS	3	USUARIO	Uso inapropiado de los equipos	Destrucción de equipos o medios de comunicación	Bajo	Medio	Moderado
			INFORMATICO	Interceptación de información	Suplantación y Manipulación de información	Muy Bajo	Medio	Moderado
			FISICO	Falla en los dispositivos físicos del equipo	Avería de origen físico o lógico	Alta	Medio	Alto
6	SWITCH 24 PUERTOS TP_LINK TL-SG1024	4	INFORMATICO	Interceptación de información	Suplantación y Manipulación de información	Media	Muy Alto	Alto
			FISICO	Acceso indebido	Manipulación de Configuración.	Media	Muy Alto	Alto
			USUARIO	Administración de red inadecuada.	Fallo de Servicio de comunicaciones	Media	Muy Alto	Alto
7	EPSON POWERLITE SERIAL U43K4902608	26	USUARIO	Uso inapropiado de los equipos	Destrucción de equipos o medios de comunicación	Alta	Muy Bajo	Bajo
			FISICO	Sensibilidad de golpes o caídas	Destrucción de equipos o medios de comunicación	Alta	Muy Bajo	Bajo
8	VIDEO GRABADOR DVR	2	FISICO	Acceso indebido	Manipulación de Configuración.	Media	Muy Bajo	Bajo
			FISICO	Manipulación de equipos y conexiones de personas no autorizadas y/o capacitadas	Manipulación de los equipos.	Media	Muy Bajo	Bajo
9	ANALOGA HIKVISION	31	FISICO	Manipulación de equipos y conexiones de personas no autorizadas y/o capacitadas	Manipulación de los equipos.	Alta	Muy Bajo	Bajo
10	INTERNET FIBRA OPTICA UNE 20MB	1	Físico	Falla en la prestación del servicio	Fallo de Servicio de comunicaciones	Media	Muy Alto	Alto
			FISICO	Manipulación de equipos y conexiones de personas no autorizadas y/o capacitadas	Manipulación de los equipos.	Media	Muy Alto	Alto
			INFORMATICO	Ataques externos a través de Internet	Denegación de Servicios	Muy Alto	Muy Alto	Critico

ITEM	DESCRIPCION	CANTIDAD	TIPO	VULNERABILIDAD	NIVEL AMENAZA	NIVEL AFECTACION	IMPACTO	NIVEL DE RIESGO
			USUARIO	Administración de red inadecuada.	Fallo de Servicio de comunicaciones	Bajo	Muy Alto	Relevante
			INFORMATICO	Saturación de ancho de banda	Fallo de Servicio de comunicaciones	Alto	Muy Alto	Critico
11	INTERNET ETB 150MBV FIBRA OPTICA	1	Físico	Falla en la prestación del servicio	Fallo de Servicio de comunicaciones	Media	Muy Alto	Alto
			FISICO	Manipulación de equipos y conexiones de personas no autorizadas y/o capacitadas	Manipulación de los equipos.	Media	Muy Alto	Alto
			INFORMATICO	Ataques externos a través de Internet	Denegación de Servicios	Muy Alto	Muy Alto	Critico
			USUARIO	Administración de red inadecuada.	Fallo de Servicio de comunicaciones	Bajo	Muy Alto	Relevante
			INFORMATICO	Saturación de ancho de banda	Fallo de Servicio de comunicaciones	Bajo	Muy Alto	Relevante
12	PAGINA WEB	1	INFORMATICO	Falta de mecanismos de autenticación e identificación de usuarios	Abuso o forzado de derechos	Bajo	Medio	Moderado
			INFORMATICO	Phishing	Suplantación de la identidad del usuario	Alto	Medio	Alto
			INFORMATICO	Ataques externos a través de Internet	Denegación de Servicios	Alto	Medio	Alto
			FISICO	Falla en la prestación del servicio	Fallo de Servicio de comunicaciones	Muy Bajo	Medio	Moderado
13	TELEFONIA	1	FISICO	Manipulación de equipos y conexiones de personas no autorizadas y/o capacitadas	Manipulación de los equipos.	Media	Alto	Alto
			FISICO	Falla en la prestación del servicio	Fallo de Servicio de comunicaciones	Bajo	Alto	Relevante
			FISICO	Falla en los dispositivos físicos del equipo	Avería de origen físico o lógico	Alto	Alto	Alto
14	SIGECOL	1	INFORMATICO	Falla en los datos respaldados.	Perdida de Información	Bajo	Muy Alto	Relevante
14	SIGECOL	1	INFORMATICO	Exposición al público de documentos o datos	Escapes de información confidencial	Bajo	Muy Alto	Relevante
			INFORMATICO	Conexión de equipo y/o usuario no autorizado.	Suplantación de la identidad del usuario	Media	Muy Alto	Alto
			FISICO	Falla en los dispositivos físicos del equipo	Avería de origen físico o lógico	Alto	Muy Alto	Critico

ITEM	DESCRIPCION	CANTIDAD	TIPO	VULNERABILIDAD	NIVEL AMENAZA	NIVEL AFECTACION	IMPACTO	NIVEL DE RIESGO
15	DHS	1	INFORMATICO	Falla en los datos respaldados.	Perdida de Información	Bajo	Muy Alto	Relevante
			INFORMATICO	Exposición al público de documentos o datos	Escapes de información confidencial	Bajo	Muy Alto	Relevante
			INFORMATICO	Conexión de equipo y/o usuario no autorizado.	Suplantación de la identidad del usuario	Media	Muy Alto	Alto
			FISICO	Falla en los dispositivos físicos del equipo	Avería de origen físico o lógico	Alto	Muy Alto	Critico
16	PFSENSE	1	FISICO	Control de acceso inadecuado.	Manipulación de los equipos.	Media	Muy Alto	Alto
			INFORMATICO	Conexión de equipo y/o usuario no autorizado.	Suplantación de la identidad del usuario	Media	Muy Alto	Alto
			FISICO	Falla en los dispositivos físicos del equipo	Avería de origen físico o lógico	Alto	Muy Alto	Critico
17	UNIFI CONTROLER	1	INFORMATICO	Conexión de equipo y/o usuario no autorizado.	Suplantación de la identidad del usuario	Bajo	Medio	Moderado
			FISICO	Falla en los dispositivos físicos del equipo	Avería de origen físico o lógico	Alto	Medio	Alto
18	CENTRO DE COMPUTO	1	FISICO	Control de acceso inadecuado.	Manipulación de los equipos.	Media	Muy Alto	Alto
			FISICO	Protección física inadecuada de los equipos tecnológicos.	Avería de origen físico o lógico	Media	Muy Alto	Alto
			FISICO	Control de acceso inadecuado.	Manipulación de los equipos.	Media	Muy Alto	Alto
19	UPS DE 10 y 15 KVA	2	FISICO	Susceptibilidad a variaciones en el voltaje	Perdida de suministro de energía	Bajo	Muy Alto	Relevante
			FISICO	Sensibilidad a la humedad, polvo y al calor	Polvo, Corrosión, Temperaturas	Bajo	Muy Alto	Relevante
20	UBIQUITI UAP AC PRO	7	FISICO	Manipulación de equipos y conexiones de personas no autorizadas y/o capacitadas	Manipulación de los equipos.	Bajo	Bajo	Bajo

Tabla 8 Matriz de riesgos

Fuente: Autores

3.1.5 PLAN DE TRATAMIENTO DE RIESGOS

Luego de definir los niveles de riesgos respecto a las vulnerabilidades de cada activo y las amenazas que puedan afectar su integridad, confidencialidad o disponibilidad; se definió un criterio de aceptación del riesgo el cual determina si el riesgo es aceptable o si requiere de algún tratamiento.

A continuación, se presenta el plan de tratamiento de los riesgos:

Nivel de Riesgo	Política para la toma de Acciones
Crítico	Riesgo no aceptable
Alto	Riesgo no deseable
Relevante	Riesgo aceptable
Moderado	Riesgo aceptable
Bajo	Riesgo aceptable

Tabla 9 Tratamiento de los Riesgos

Fuente: Autores

Para el tratamiento de los riesgos cuyo nivel sea “Crítico”, “Alto” o “Relevante” se debe recurrir a la implementación de ciertos controles y políticas de manejo obligatorias para reducir la probabilidad que dichos riesgos identificados se materialicen. Finalmente, se aplicarán normas de tratamiento para los niveles de riesgos “Moderado” y “Bajo” ya que se considera que la institución puede convivir con dichos riesgos y no afectará de manera considerable la operación normal del servicio educativo.

3.2 CONTROLES PARA EL TRATAMIENTO DE RIESGOS

Los controles que se han seleccionado para el tratamiento de los riesgos son los que se detallan en el estándar ISO 27001, el cual contiene una lista de los objetivos de control relevantes para todas las organizaciones en general. Cabe resaltar que dichos controles siguen lineamientos generales y que se mostrarán controles adaptados a la realidad organizacional de la Institución CELCO San Lucas

Todos los controles o políticas detallados contribuyen a la mitigación de los riesgos identificados y, en su mayoría, deberán ser desarrollados y promovidos por la rectora y junta directiva de la institución.

Estos controles y políticas de seguridad son los siguientes:

Categoría de seguridad	Nombre del control	Número de dominio, objetivo de control y control en ISO 27002:2013	Descripción	Riesgos a controlar	Adaptación a la entidad educativa
SEGURIDAD FÍSICA Y AMBIENTAL.	Ubicación y protección del equipo	Dominio 11, Objetivo 11.2, control 11.2.1	El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.	ITEM 1-2-3,5,6,7,8,10 ,11,13,18	Los equipos electrónicos críticos deberán estar ubicados de tal manera que ayudarán a reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.
	Seguridad en el cableado	Dominio 11, Objetivo 11.2, control 11.2.3	El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la intercepción o daño.	ITEM 4,8,10,11,1 8	El cableado eléctrico y de las telecomunicaciones que llevan data o sostienen los servicios de información del instituto deberán ser protegidos mediante tubos u otros controles

Categoría de seguridad	Nombre del control	Número de dominio, objetivo de control y control en ISO 27002:2013	Descripción	Riesgos a controlar	Adaptación a la entidad educativa
SEGURIDAD FÍSICA Y AMBIENTAL.	Mantenimiento de equipo	Dominio 11, Objetivo 11.2, control 11.2.4	El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.	ITEM 1,2,3,5,7,8, 19,20	Los equipos deberán pasar por mantenimiento 1 vez cada 4 meses para asegurar la continuidad de los sistemas y demás aplicativos que dan soporte a los procesos críticos
	Equipo de usuario desatendido	Dominio 11, objetivo 11.2, control 11.2.8	Se debe requerir que los usuarios se aseguren de dar la protección apropiada al equipo desatendido	ITEM 1,2,5,7,8	Todos los usuarios de la institución deberán estar al tanto de los requerimientos de seguridad y los procedimientos para proteger su respectivo equipo desatendido, así como sus responsabilidades para implementar dicha protección
	Política de pantalla y escritorio limpio	Dominio 11, objetivo 11.2, control 11.2.9	Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.	ITEM 1 y 2	La política de escritorio limpio y pantalla limpia que la institución proporcione deberá tomar en cuenta las clasificaciones de información, requerimientos legales y contractuales y los correspondientes riesgos y aspectos culturales de la organización
CONTROL DE ACCESOS	Política de control de accesos.	Dominio 9, objetico 9.1, control 9.1.1	Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.	ITEM 1,2,3,8,12,14,15,16,17	Se deberá formular una política relacionada con el uso de las redes y los servicios de la red, de tal manera que los usuarios de la institución sólo deberán tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.
	Gestión de contraseñas de usuario.	Dominio 9, objetivo 9.4, control 9.4.3	Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.	ITEM 1,2,8,10,11, 12,14,15,16	El área de Sistemas deberá proporcionar políticas para las contraseñas de los distintos sistemas de información que se posean. Estas políticas deberán seguir buenas prácticas de seguridad en la selección y uso de claves.
	Restricción de acceso a la información	Dominio 9, objetivo 9.4, control 9.4.1	El acceso a información de estudiantes e información sensible de la organización se debe manejar de acuerdo a perfiles y políticas de seguridad	ITEM 1,2,3,14,15, 16	Los coordinadores, administradores del sistema de gestión estudiantil y software contable manejaran la información hasta donde su perfil lo permita para garantizar la integridad de los datos.

Categoría de seguridad	Nombre del control	Número de dominio, objetivo de control y control en ISO 27002:2013	Descripción	Riesgos a controlar	Adaptación a la entidad educativa
CONTROL DE ACCESOS	Gestión de contraseñas de usuario	Dominio 9, objetivo 9.4, control 9.4.3	El uso de contraseñas es obligatorio para cada uno de los funcionarios administrativos para acceso a la plataforma DHS y Sigecol, los docentes al módulo de notas deben ser únicas y el manejo de ellas es responsabilidad exclusiva de cada usuario	ITEM 1,2,8,12,13, 14,15,16,17	Dependiendo del rol de cada funcionario y docente el manejo de las contraseñas es obligatorio para realizar trazabilidad de los procesos que se realizan en el software con los que cuenta la institución
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	Asignación de responsabilidades para la seguridad de la información.	Dominio 6. objetivo 6.1, control 6.1.1	Cada usuario será responsable de la información que maneje según el área asignada, el mal manejo de la misma será responsabilidad exclusiva de quien se encuentre como custodio.	ITEM 1,2,8,12,14, 15,16	La información que manejan personal docente y administrativo deberá ser controlada para que el mismo no sea manipulado por personal ajeno a la institución.
	Seguridad de la información en la gestión de proyectos	Dominio 6, objetivo 6.1, control 6.1.5	Al trabajar con entidades Gubernamentales o distritales se deben seguir las directrices de la institución para el manejo de la información y tratamiento de datos	ITEM 1,2,14,15	Con las entidades de secretaria de educación y ministerio de educación la información de estudiantes debe ser manejada respecto a las políticas de la institución y la ley de protección de datos
GESTIÓN DE ACTIVOS.	Devolución de activos	Dominio 8. objetivo 8.1, control 8.1.4	Se establecerá un procedimiento para la recepción de activos que sean devueltos por parte de funcionarios administrativos o docentes	ITEM 1,2,5,7,8	Al momento del retiro de un funcionario de la institución se verificará las condiciones en las cuales hace entrega de los activos que les fueron asignados para el desempeño de su labor.
	Gestión de soportes extraíbles	Dominio 8. objetivo8.3, control 8.3.1	En áreas específicas se generará políticas sobre el uso y cuidado de medios extraíbles utilizados para intercambio de información.	ITEM 1,2,14,15	Los medios extraíbles que se asignan a determinados docentes y funcionarios para la presentación de trabajos e informes se deben gestionar según las políticas internas para evitar manipulación y perdida de información de dichos medios
RELACION CON PROVEEDORES	Supervisión y revisión de los servicios prestados por terceros	Dominio 15, Objetivo 15.2, control 15.2.1	El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.	ITEM 10,11,13,18	Los equipos electrónicos críticos deberán ser protegidos de fallas de energía y otras interrupciones causadas por fallas en los servicios eléctricos o de telecomunicaciones
SEGURIDAD EN LA OPERATIVA	Copias de seguridad de la información.	Dominio 12 Objetivo 12.3 Control 12.3.1	Todos los dispositivos que manejen información deben tener un respaldo de backup para recuperación de la misma	ITEM 1,2,8,12,13, 14,15 16,17	El área de sistemas debe generar las tareas de backups y su periocidad dependiendo de la importancia y tamaño de la información y asegurar que sean confiables
	Registros de actividad del administrador y operador del sistema.	Dominio 12 Objetivo 12.4 Control 12.4.3	Toda modificación, cambio y configuración nueva debe ser registrado en una bitácora de control de cambios	ITEM 1-2-3-5-8-10-11-12-13-14-15-16-17	Mantener el registro de cambios actualizado para tener un control de nuevas configuraciones realizadas a los dispositivos que generen cambios significativos.

Categoría de seguridad	Nombre del control	Número de dominio, objetivo de control y control en ISO 27002:2013	Descripción	Riesgos a controlar	Adaptación a la entidad educativa
GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	Notificación de puntos débiles de la seguridad.	Dominio 16 Objetivo 16.1 Control 16.1.3	Identificar puntos inseguros de toda la infraestructura tecnológica	ITEM 1-2-3-4-6-10-11-13-14-15-16-18	Notificar todo suceso que pueda presentar un hueco de seguridad y realizar el respectivo registro para llevar un control de los sucesos
	Recopilación de evidencias.	Dominio 16 Objetivo 16.1 Control 16.1.7	Levantamiento de pruebas sobre incidentes de la seguridad de la información	ITEM 1-2-3-4-6-10-11-13-14-15-16-18	Registros fotográficos, software, video y todo material probatorio que ayude analizar los incidentes de seguridad presentados
CUMPLIMIENTO.	Cumplimiento de las políticas y normas de seguridad.	Dominio 18 Objetivo 18.2 Control 18.2.2	Realizar seguimientos periódicos al cumplimiento de las políticas creadas dentro del sistema de gestión de la seguridad	ITEM 1-2-3-8-10-11-12-14-15-16-17	Asignar auditores internos que garanticen el cumplimiento de las políticas, normas y directrices
	Protección de datos y privacidad de la información personal.	Dominio 18 Objetivo 18.1 Control 18.1.4	Mantener seguros las Bases de Datos que contengan información personal sensible de padres, estudiantes y personal administrativo	ITEM 1-14-15	Generar las configuraciones necesarias para garantizar la seguridad de estas Base de datos según lo estipulado en la ley de protección de datos personales

Tabla 10 Dominios, objetivos y controles ISO 27002:2013

Fuente: Autores

4 PLANTEAMIENTO DEL SISTEMA DE SEGURIDAD

Después de realizar el análisis de riesgos para la institución educativa CELCO san Lucas, se debe plantear un sistema de seguridad en el cual se especifiquen las políticas que se deben aplicar, así como las metodologías, alcances y seguimientos de las mismas.

4.1 ALCANCE.

El sistema de seguridad que se plantea aplica para todas las áreas y procesos de la institución educativa, todo proceso nuevo o que se modifique debe entrar a formar parte del sistema de seguridad que se plantea, de esta manera se garantiza la continuidad y retroalimentación del sistema de gestión de seguridad de la información.

4.2 OBJETIVO

Con el Sistema que se plantea lo que se pretende es garantizar la continuidad del negocio tanto en los procesos internos, así como en el core del negocio que para el caso de la institución educativa CELCO san Lucas es la de brindar educación desde los ciclos de básica primaria hasta la educación media superior.

De otra parte, se pretende concientizar a todo el personal que forma parte de la institución sobre el adecuado manejo de la información, las normas y parámetros que se deben seguir para el manejo de la misma, así como minimiza el impacto de una ocurrencia y los riesgos que ello conlleva, lo anterior garantizando los aspectos claves en el manejo y seguridad de la información garantizando la disponibilidad, integridad y confidencialidad.

4.3 METODOLOGIA

Posterior a realizar la planificación del sistema de gestión de seguridad de la información, se procede a realizar la implementación de los diferentes procedimientos y herramientas que ayudaran a generar las políticas para el control de activos, información y procesos de la institución educativa CELCO San Lucas.

Generar un cronograma de cumplimiento de las propuestas planteadas es de vital importancia ya que desde este punto se puede monitorear el cumplimiento por parte del personal que está sujeto a las políticas de seguridad, esto ayudara a que la ocurrencia de uno de los riesgos planteados en el análisis anterior no se presente.

Si después de realizar los procedimientos anteriores la materialización de uno de los riesgos que se generaron en la matriz de riesgos llegara a presentarse, se debe contar con las herramientas necesarias para minimizar el impacto, dichas herramientas deben estar enfocadas a que la pérdida, manipulación o alteración de la información sea en el mínimo grado posible.

El que un riesgo y/o amenaza se haya materializado se debe hacer el respectivo seguimiento para determinar donde se pudo haber generado la falla y los posibles responsables para que con las medidas adecuadas se tomen los correctivos necesarios y evitar que se vuelva a presentar.

5 POLÍTICAS DE SEGURIDAD

5.1 JUSTIFICACIÓN.

La información de las Bases de Datos y los equipos informáticos son recursos importantes y vitales para el funcionamiento de la institución educativa sin ellos el servicio de educación que se presta podría ser afectado y por tal razón la Junta directiva y Rector tienen el deber de preservarlos, protegerlos y actualizarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, suplantación, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales.

La información perteneciente a la Institución debe protegerse de acuerdo a su valor e importancia. Se emplean medidas de seguridad sin importar cómo la información se guarda (en papel o en forma electrónica), o como se procesa (PCs, servidores, correo

de voz, etc.), o cómo se transmite (correo electrónico, conversación telefónica). Tal protección incluye restricciones de acceso a los usuarios de acuerdo a su cargo.

Las distintas áreas están en el deber y en la responsabilidad de consagrar tiempo y recursos suficientes para asegurar que los activos de información estén suficientemente protegidos. Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos.

En todo caso cada año el Comité administrativo llevará a cabo un análisis de riesgos y se revisarán las políticas de seguridad. Así mismo, se preparará cada año un informe para la Junta Directiva y Rectoría que muestre el estado actual de la Institución en cuanto a seguridad informática y las políticas aplicadas.

A todo el personal administrativo, profesores y estudiantes se les debe proporcionar adiestramiento, información, y advertencias para que ellos puedan proteger y manejar apropiadamente los recursos informáticos de la Institución. Debe hacerse hincapié en que la seguridad informática es una actividad tan vital para la Institución como lo son la contabilidad y la nómina.

La finalidad de las políticas de seguridad que se describen más adelante es proporcionar instrucciones específicas sobre cómo mantener más seguros tanto los computadores (conectados o no en red), como la información guardada en ellos. La violación de dichas políticas puede acarrear medidas disciplinarias e incluso el despido.

5.2 PROPÓSITO.

El propósito de esta política es establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de la información de la Institución al estar conectada a redes de computadoras, a compartir archivos, al manejo de correo electrónico, a la modificación general de los archivos, con o sin intención.

5.3 ALCANCE.

Esta política se aplica a personal administrativo, profesorado, estudiantes y demás personal que haga uso de la infraestructura tecnología del Colegio.

5.4 ASPECTOS GENERALES.

Es deber de la Institución prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información propietaria. Además, es su deber proteger la información que pertenece a otras empresas o personas y que le haya sido confiada.

5.5 RESPONSABILIDADES.

Los siguientes entes son responsables, en distintos grados, de la seguridad en la Institución:

El **Comité Administrativo** está compuesto por la Rectora, representante legal, el Pastor de la Institución y el Revisor. Este Comité está encargado de elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a seguridad en informática y telecomunicaciones con el apoyo del Ingeniero de Sistemas. También es responsable de coordinar los planes de contingencia y prevención de desastres. Durante sus reuniones el Comité efectuará la evaluación y revisión de la situación de la Institución en cuanto a seguridad informática, incluyendo el análisis de incidentes ocurridos y que hayan afectado de alguna manera la seguridad.

El **Ingeniero de Sistemas** es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la institución, todo esto en coordinación con la Rectora del Colegio. También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además, debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

También es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes.

Establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra.

Los **usuarios** son responsables de cumplir con todas las políticas de la Institución relativas a la seguridad informática y en particular:

5.6 POLITICAS PARA MANEJO DE LA INFORMACIÓN.

Estas políticas están enfocadas a mantener la seguridad de la información de la institución, aplica para todas las áreas que manejen o tengan acceso a información crítica para la compañía, su cumplimiento es obligatorio y el no acatarlas acarrearan sanciones disciplinarias, a continuación se describe cada una:

- Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
- No divulgar información confidencial de la Institución a personas no autorizadas.
- No permitir y no facilitar el uso de los sistemas informáticos de la Institución a personas no autorizadas.

- No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo en la Institución.

- Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.

- Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.

- Reportar inmediatamente a su jefe inmediato o al área de sistemas, , o la persona autorizada, cualquier evento que pueda comprometer la seguridad de la Institución y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

5.7 POLÍTICAS DE SEGURIDAD PARA COMPUTADORES.

Los computadores de la Institución sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.

- Los equipos asignados a personal Administrativo y Profesores sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos, no aplica para equipos de sala de sistemas los cuales si pueden ser usados para temas de ocio.

- Debe respetarse y no modificar la configuración de hardware y software establecida por el Área de sistemas o la persona autorizada.

- No se permite fumar, comer o beber mientras se está usando un PC.

- Deben usarse protectores contra picos de voltaje y en los servidores deben usarse fuentes de poder interrumpibles (UPS).

- Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

- Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de vigilantes y cerradura con llave.

- Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.

- No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la institución se requiere una autorización escrita.

- La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.
- Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto.

- Si un PCs tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso por usuario adicional al que se usa para ingresar al equipo y es deber del usuario preservar la integridad de dicha información.

- Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.

- No está permitido llevar al sitio de trabajo computadores portátiles ajenos a la institución y en caso de ser necesario se requiere solicitar la autorización correspondiente.

- Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PCs que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la LAN del instituto educativo.

- A menos que se indique lo contrario, los usuarios deben asumir que todo el software del Colegio está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

- Los usuarios no deben copiar a un medio removible (como una USB), el software o los datos residentes en las computadoras del Instituto, sin la aprobación previa de la Rectora o la persona autorizada.

- No pueden extraerse datos fuera de la sede de la Institución sin la aprobación previa de la Rectora y la supervisión del Ingeniero de sistemas. Esta política es particularmente pertinente a aquellos que usan portátiles o equipos que están conectados a Internet.

- Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente y poner la PC en cuarentena hasta que el problema sea resuelto.

- Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos. Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otros departamentos de la institución.

- No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Ingeniero de sistemas, Rectoría, o la persona autorizada.

- Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el Ingeniero de sistemas, Rectoría, o la persona autorizada.

- Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.

- No deben usarse USBs u otros medios de almacenamiento en cualquier computadora de la institución a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos, esto aplicaría para equipos Administrativos y Profesores.

- Periódicamente debe hacerse el respaldo de los datos guardados en PCs y servidores y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación de la institución deben guardarse en otro lugar que no sea instalaciones del Colegio.

- Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño. Para sistemas multiusuario y sistemas de comunicaciones, el Administrador de cada uno de esos sistemas es responsable de hacer copias de respaldo periódicas.

- Siempre que sea posible, deba eliminarse información confidencial de los computadores y unidades de disco duro antes de que les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de un representante de la institución.

- No deben salirse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial de la institución.

5.8 POLÍTICAS DE SEGURIDAD PARA LAS COMUNICACIONES.

5.8.1 PROPIEDAD DE LA INFORMACIÓN.

Con el fin de mejorar la productividad, la Institución promueve el uso responsable de las comunicaciones de forma electrónica, en particular el teléfono, el correo electrónico e internet. Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, se deben considerar como propiedad de la Institución y no propiedad de los usuarios de los servicios de comunicación.

5.8.2 USO DE LOS SISTEMAS DE COMUNICACIÓN.

Los sistemas de comunicación de la Institución generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del empleado ni con las actividades de la Institución. Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión. La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la Institución y en tal sentido deben usarse las horas no laborables.

5.8.3 CONFIDENCIALIDAD Y PRIVACIDAD.

Los recursos, servicios y conectividad disponibles vía Internet abren nuevas oportunidades, pero también introducen nuevos riesgos. Los empleados y funcionarios de la Institución no deben interceptar las comunicaciones o divulgar su contenido. Tampoco deben ayudar a otros para que lo hagan. La Institución se compromete a respetar los derechos de sus empleados y estudiantes, incluyendo su privacidad. También se hace responsable del buen funcionamiento y del buen uso de sus redes de comunicación y para lograr esto, ocasionalmente es necesario interceptar ciertas comunicaciones.

Es política de la Institución no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones pueden ocasionalmente ser supervisado en caso de ser necesario para actividades de mantenimiento, seguridad o auditoría. Puede ocurrir que el personal técnico vea el contenido de un mensaje de un empleado individual durante el curso de resolución de un problema.

De manera consistente con prácticas generalmente aceptadas, la Institución procesa datos estadísticos sobre el uso de los sistemas de comunicación.

5.8.4 REENVÍO DE MENSAJES.

Tomando en cuenta que cierta información está dirigida a personas específicas y puede no ser apta para otros, dentro y fuera de la Institución, se debe ejercer cierta cautela al remitir los mensajes. En todo caso no debe remitirse información confidencial de la Institución sin la debida aprobación.

5.8.5 BORRADO DE MENSAJES.

Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.

5.9 POLÍTICAS DE SEGURIDAD PARA REDES.

5.9.1 MODIFICACIONES.

Todos los cambios en los equipos de red de la Institución, incluyendo la instalación de nuevo software, el cambio de direcciones IP, la reconfiguración de routers y switchs, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

5.9.2 CUENTAS DE LOS USUARIOS.

- Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta. La solicitud de una nueva cuenta o el cambio de privilegios deben ser hecha por escrito y debe ser debidamente aprobada.

- No debe concederse una cuenta a personas que no sean empleados de la Institución o hagan parte de ella a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días. Privilegios especiales, tal como la posibilidad de modificar o barrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.

- No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Ingeniero de Sistemas, la Rectora, o la persona autorizada determine que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto). Si hace falta una conexión remota durante un periodo más largo, entonces se debe usar un sistema de autenticación más robusto basado contraseñas dinámicas, o tarjetas inteligentes.

- Se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad, en cualquier caso debe registrarse en la bitácora todos los cambios de ID.

- Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Ingeniero de Sistemas, la Rectora, o la persona autorizada debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones. Cuando un empleado es despedido o renuncia a la institución, debe desactivarse su cuenta antes de que deje el cargo.

5.10 CONTRASEÑAS Y EL CONTROL DE ACCESO.

- El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.

- Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.

- Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.

- La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

- Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.

- Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, para el acceso remoto a los recursos informáticos de la Institución,

la combinación del ID de usuario y una contraseña fija no proporciona suficiente seguridad, por lo que se recomienda el uso de un sistema de autenticación más robusto basado en contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.

- Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El periodo recomendado de tiempo es de 15 minutos. El re-establecimiento de la sesión requiere que el usuario proporcione se autentique mediante su contraseña (o utilice otro mecanismo, por ejemplo, tarjeta inteligente o de proximidad).

- Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la Institución, pudiendo ser causal de despido.

- Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.

- Los archivos de bitácora que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dichos archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoría. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.

- Los servidores de red y los equipos de comunicación (Teléfonos, Routers, etc.) deben estar ubicados en lugares apropiados, protegidos contra daños y robo.

6 SOFTWARE DE SEGURIDAD

6.1 SERVIDOR FIREWALL PFSENSE

Pfsense es una herramienta con características de firewall y Router de tipo Open Source bajo distribución de FreeBSD, la cual se instaló en un equipo específico para la administración de las configuraciones de la red interna de la institución educativa San Lucas.
Dentro de las características más relevantes que presente la herramienta y que fueron adaptadas a las necesidades de la institución encontramos las siguientes:

6.1.1 SERVIDOR DHCP.

En esta parte se generó un nuevo esquema de direccionamiento teniendo en cuenta el número de usuarios que acceden a los servicios de la red interna (aproximadamente 800 usuarios), dicho direccionamiento se realizó con una dirección ip clase B, la cual comprende un rango de direccionamiento que va desde la dirección 128.0.0.0 hasta la dirección 191.255.255.25. Para el caso de la institución educativa San Lucas se generó el esquema a partir de la dirección 172.16.0.0 con una máscara de red 255.255.0.0, la cual permite generar direccionamiento hasta para un máximo de 65534 host.

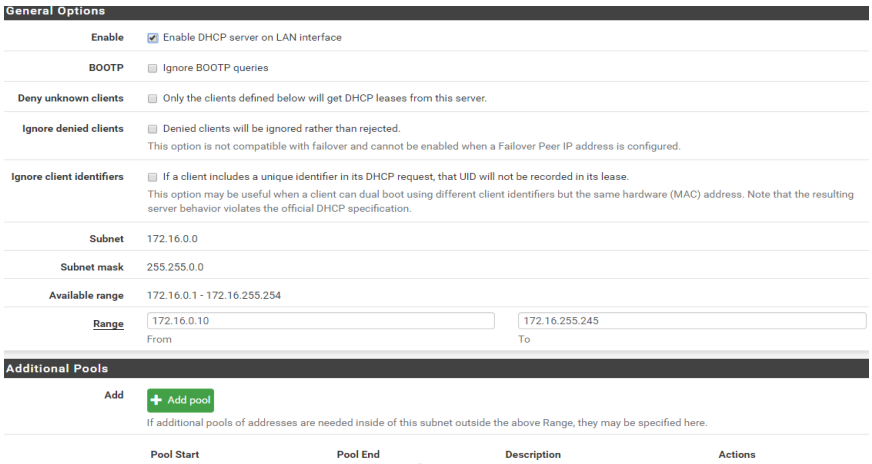


Figura 4 Configuración interfaz LAN y DHCP

Fuente: Software de seguridad Implementado en la institución

6.1.2 SERVIDOR PROXY.

En este segmento se hace bastante énfasis ya que a partir de este servicio se desprenderán las políticas de navegabilidad y acceso por parte de los usuarios de la red del colegio san Lucas a los servicios de internet, cabe aclarar que este servicio está siendo aplicado a los usuarios de la solución wifi, los usuarios de salas de sistemas y equipos suministrados al personal docente. La red cuenta con un servicio contratado de 150MB de fibra óptica suministrado por el proveedor ETB, el cual dispone de una dirección ip pública para ser gestionada en los servicios internos de la organización.

Dentro de este servicio se desprende una serie de paquetes o configuraciones que complementan la seguridad de la navegabilidad como lo son la utilidad SquidGuard, que es en el que se realizan las configuraciones y filtrados de contenido en internet, permite generar una serie de restricciones en páginas no aptas para los estudiantes y el personal docente.

Dicha herramienta se basa en una serie de listas negras con categorías previamente establecidas las cuales se configuran para generar bloqueo para los usuarios que traten de acceder a ellas.

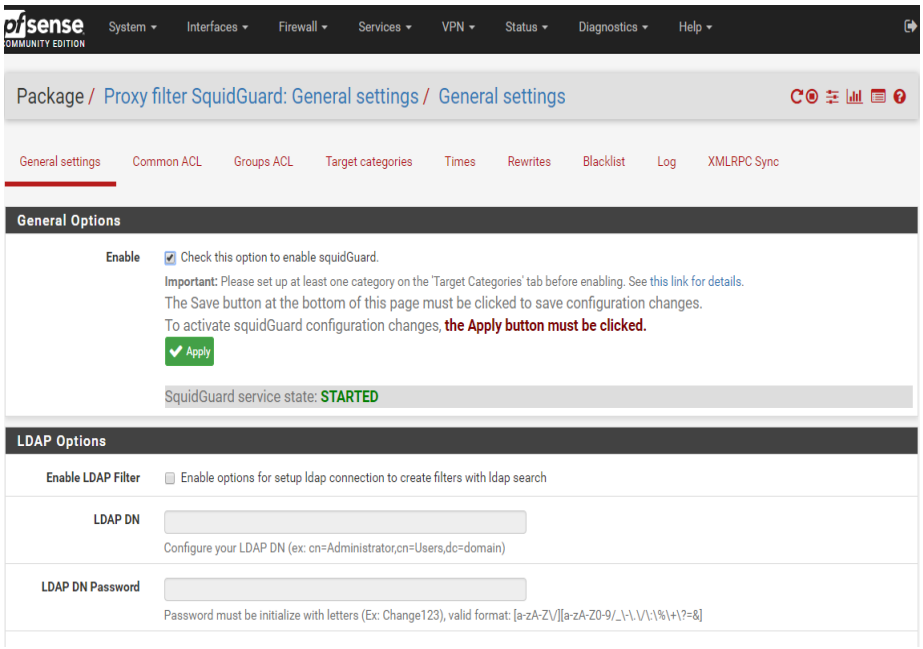


Figura 5 SquidGuard

Fuente: Software de seguridad Implementado en la institución

Para aplicar políticas de navegación el servidor SquidGuard siempre debe estar el servicio activo (Ver figura 8) si se realizan configuraciones nuevas al filtrado web se deben aplicar dese la ventana general de opciones.

Las listas negras (Ver figura 10) son bases de datos que se encuentran disponibles en Internet donde se definen categorías según el contenido o servicio que presta la página, dichas categorías se pueden configurar para que según la selección sea permitido o denegado el acceso, también se configura el mensaje de error y la pagina o sitio para ser dirigido en caso de violar alguna de las políticas de navegación establecidas.

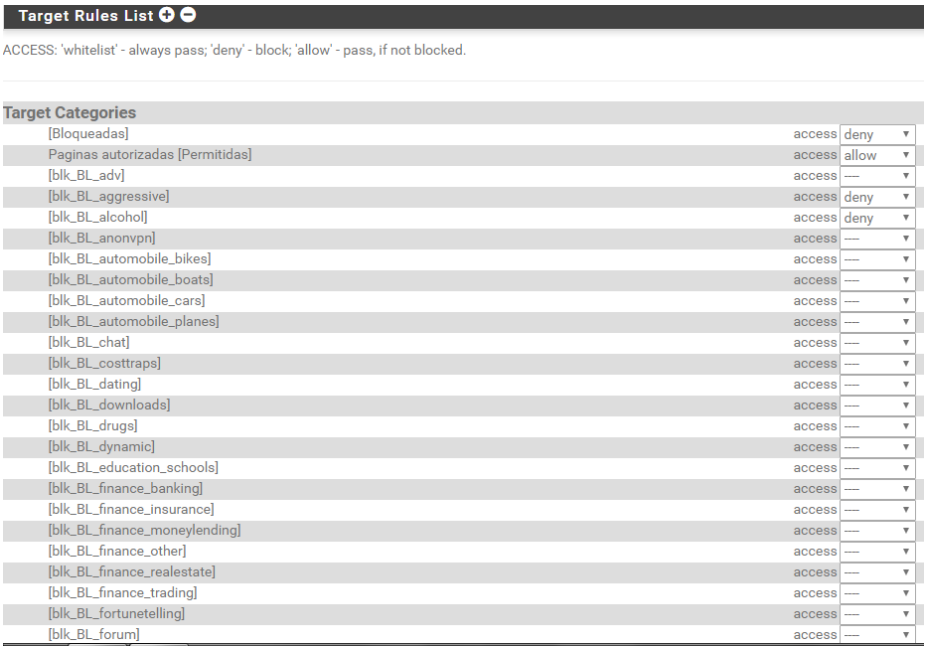


Figura 6 Categorías de la lista negra

Fuente: Software de seguridad Implementado en la institución.

6.2 SEGURIDAD Y ADMINISTRACIÓN WIFI

La institución educativa cuenta con una solución de conectividad wifi la cual está destinada a funcionarios administrativos, docentes y personal visitante que requiera de conectividad, por ningún motivo dicha red wifi está disponible para el uso de los estudiantes.

Para evitar ataques y accesos peligros a la red Wifi se establece una autenticación con un de un portal cautivo y un filtrado de direcciones MAC

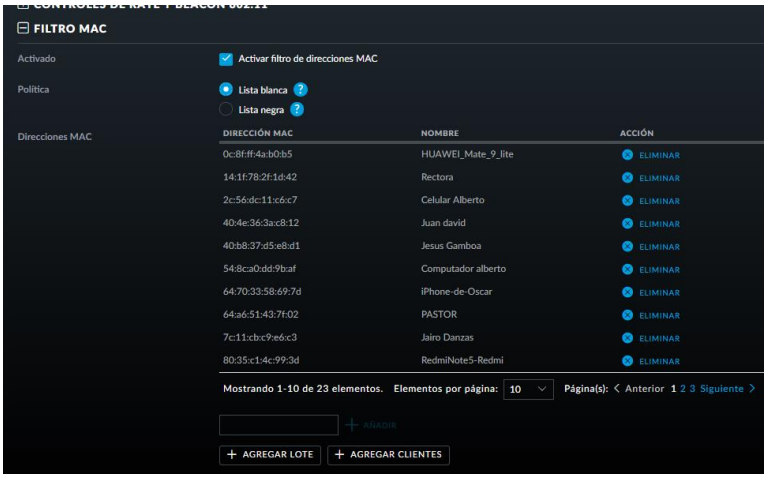
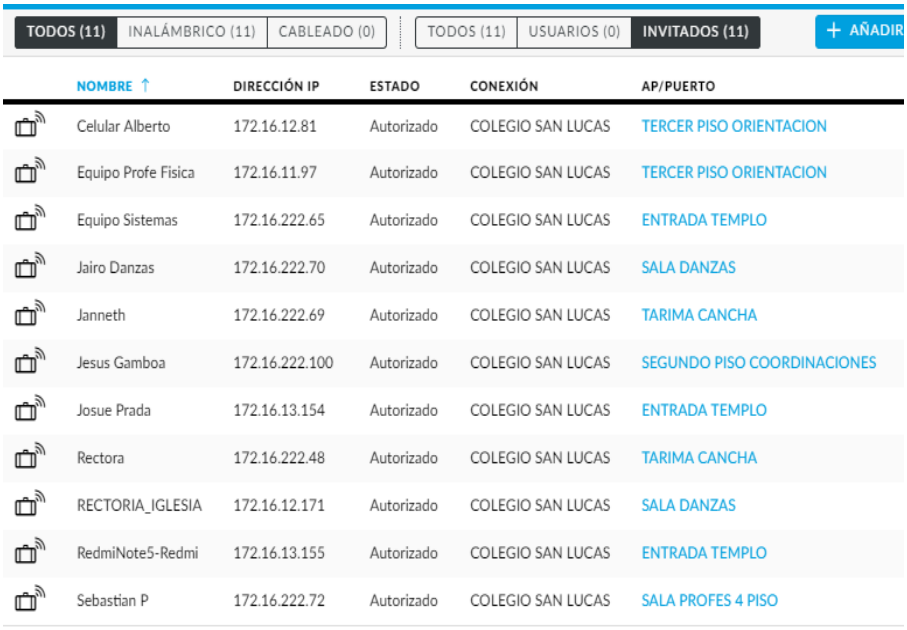


Figura 7 Configuración de Filtrado MAC

Fuente: Controladora Unifi Cloud Key

Por seguridad la red cuenta con diferentes grupos de usuarios (Ver figura 13), los cuales tiene un límite de subida y bajada en el ancho de banda del internet, esto con el fin de evitar saturación del servicio con aplicaciones de Streaming, video y descarga de contenidos como juego, música y películas.



NOMBRE	DIRECCIÓN IP	ESTADO	CONEXIÓN	AP/PUERTO
Celular Alberto	172.16.12.81	Autorizado	COLEGIO SAN LUCAS	TERCER PISO ORIENTACION
Equipo Profe Fisica	172.16.11.97	Autorizado	COLEGIO SAN LUCAS	TERCER PISO ORIENTACION
Equipo Sistemas	172.16.222.65	Autorizado	COLEGIO SAN LUCAS	ENTRADA TEMPLO
Jairo Danzas	172.16.222.70	Autorizado	COLEGIO SAN LUCAS	SALA DANZAS
Janneth	172.16.222.69	Autorizado	COLEGIO SAN LUCAS	TARIMA CANCHA
Jesus Gamboa	172.16.222.100	Autorizado	COLEGIO SAN LUCAS	SEGUNDO PISO COORDINACIONES
Josue Prada	172.16.13.154	Autorizado	COLEGIO SAN LUCAS	ENTRADA TEMPLO
Rectora	172.16.222.48	Autorizado	COLEGIO SAN LUCAS	TARIMA CANCHA
RECTORIA_IGLESIA	172.16.12.171	Autorizado	COLEGIO SAN LUCAS	SALA DANZAS
RedmiNote5-Redmi	172.16.13.155	Autorizado	COLEGIO SAN LUCAS	ENTRADA TEMPLO
Sebastian P	172.16.222.72	Autorizado	COLEGIO SAN LUCAS	SALA PROFES 4 PISO

Figura 8 Dispositivos Conectados

Fuente: Controladora Unifi Cloud Key

Toda la gestión anterior se realiza por medio de una tarjeta controladora, la cual permite aprovisionar las configuraciones anteriores a cualquier nuevo dispositivo de la misma familia que se detecte como nuevo en la red y requiera de alguna parametrización.

Cabe resalta que estos dispositivos Wifi también forman parte de la red que está siendo objeto de políticas por el software de seguridad de Pfsense.

La utilización del portal cautivo es obligatoria para cualquier usuario que acceda a la red, esto ayuda a controlar que los usuarios aceptan los términos y condiciones de uso de la red, genera una imagen institucional ya que dicho portal maneja los distintivos propios del colegio san Lucas.

7 CONCLUSIONES

- El diagnóstico de la situación actual de la institución permitió identificar que no se cuenta con un sistema de seguridad de la información definido y alineado con los objetivos del Colegio. La falta de conocimiento del personal administrativo y docente en temas de seguridad y puntos vulnerables en equipos, infraestructura, accesos y manejo de información pusieron de manifiesto el alto grado de inseguridad con la que se encontraba la Institución.

- Basándose en la norma ISO 27001 se priorizaron los activos vitales para el correcto funcionamiento de la institución, así como la identificación de amenazas y vulnerabilidades que ponían en riesgo la confidencialidad, disponibilidad e integridad de la información del colegio, fue necesario definir un criterio de aceptación al riesgo para aplicar los controles necesarios definidos en la norma y que contribuyeran a mitigar la probabilidad de que dichos riesgos identificados se materialicen.

- Para permitir el control de los riesgos identificados se planteó un sistema de seguridad de la información para la Institución Celco San Lucas definiendo su alcance, el objetivo, la metodología y consideraciones generales para su correcto desarrollo e implementación.

- Las políticas de seguridad son la base del Sistema de seguridad de la información, en estas se encuentran definidos los compromisos de los entes que conforman la institución educativa y que deben ser de cumplimiento obligatorio si se desea minimizar el impacto que podría tener la institución en su funcionamiento, mantenimiento y progreso, estas políticas están basadas en cinco grupos de seguridad (Información, comunicaciones, equipos, redes y accesos) diseñados para mitigar los riesgos identificados.

- Con la ayuda del software de seguridad (Pfsense) instalado en el centro de comunicaciones principal y que funciona como Firewall, se mejoró la seguridad de navegación hacia y desde internet, se mitigaron los ataques informáticos externos y permitió controlar el acceso a material peligroso para los equipos de sistemas. La implementación de una controladora de red Wifi (CloudKey Ubiquiti) también reforzó las políticas de acceso, garantizando que solo los equipos de la institución tengan acceso a la red y a internet.

- La información es el recurso más valioso de la institución, su perdida, modificación o alteración pueden acarrear inconvenientes para la debida prestación del servicio educativo, el éxito del Sistema de Seguridad dependerá del correcto alineamiento de la institución a las políticas de seguridad planteadas, así como el seguimiento, control y retroalimentación de un sistema que se diseñó para su mejora continua.

8 BIBLIOGRAFIA

1. Berrío López, Juan & Montoya Pérez, Yury & Adolfo Pérez Zapata, Gustavo & Jiménez Builes, Jovani. (2016). Modelo para la evaluación de desempeño de los controladores de un SGSI basado en el estándar ISO/IEC 27001.

2. colorado, f. (2018). 3 articulo El Ciclo PHVA de Deming y al Proceso Administrativo de Fayol. [online] Academia.edu. Disponible en: http://www.academia.edu/5110051/3_Articulo_El_Ciclo_PHVA_de_Deming_y_al_Proceso_Administrativo_de_Fayol [Accedido 2 junio. 2018].

3. Software ISO. (2018). ¿En qué consiste el ciclo PHVA de mejora continua? [online] Disponible en: https://www.isotools.org/2015/02/20/en-que-consiste-el-ciclo-phva-de-mejora-continua/ [Accedido 5 junio. 2018].

4. Javerianacali.edu.co. (2018). [online] Disponible en: https://www.javerianacali.edu.co/sites/ujc/files/node/field-documents/field_document_file/directriz_seguridad_informatica_2016.pdf [Accedido 7 Agos. 2018].

5. Iso27000.es. (2018). ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información. [online] Disponible en: http://iso27000.es/iso27002.html [Accedido 1 junio. 2018].

6. Jara Pérez, D. (2018). Valoración y Plan de Tratamiento de Riesgos de Seguridad de la Información para los Procesos Incluidos en el Alcance del SGSI del Cliente TGE de la Empresa ASSURANCE CONTROLTECH. [online] Repository.udistrital.edu.co. Disponible en: http://repository.udistrital.edu.co/handle/11349/6492 [Accedido 3 Agos. 2018].

7. WeLiveSecurity. (2018). La importancia de un SGSI. [online] Disponible en: https://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/ [Accedido 1 Agos. 2018].

8. Moyano Orjuela, L. and Suárez Cárdenas, Y. (2018). Plan de Implementación del SGSI Basado en la Norma ISO 27001:2013 para la Empresa Interfaces y Soluciones S.A.S. [online] Repository.udistrital.edu.co. Disponible en: http://repository.udistrital.edu.co/handle/11349/6737 [Accedido 2 Agos. 2018].

9. Intranet.bogotaturismo.gov.co. (2018). NORMA TÉCNICA NTC -ISO/IEC COLOMBIANA 27001. [online] Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf [Accedido 7 Agos. 2018].

10. González, M. (2018). El Ciclo PHVA y su Papel Dentro de Procesos Exitosos de Mejoramiento y Aprendizaje. [online] Ideasplusgve.com. Disponible en:

http://www.ideasplusgve.com/articulo/57-el-ciclo-phva-y-su-papel-dentro-de-procesos-exitosos-de-mejoramiento-y-aprendizaje.html [Accedido 19 junio. 2018].

11. Novoa, H. and Barrera, C. (2018). Metodologías para el análisis de riesgos en los sgsi. [online] Hemeroteca.unad.edu.co. Disponible en: http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874 [Accedido 25 Julio. 2018].
12. S., P. and Maria, A. (2018). Fundamentos de iso 27001 y su aplicación en las empresas. [online] Revistas.utp.edu.co. Disponible en: http://revistas.utp.edu.co/index.php/revistaciencia/article/view/1177 [Accedido 26 Julio. 2018].

13. Emb.cl. (2018). Revista Gerencia - La seguridad de la información en un mundo sin fronteras. [online] Disponible en: http://www.emb.cl/gerencia/articulo.mvc?xid=558&sec=11 [Accedido 30 julio. 2018].

14. Toro, R. (2018). ISO 27001:2015: Un cambio en la Integración de los Sistemas de Gestión. [online] PMG SSI - ISO 27001. Disponible en: https://www.pmg-ssi.com/2014/11/iso-270012015-un-cambio-en-la-integracion-de-los-sistemas-de-gestion/ [Accedido 20 julio. 2018].

15. Toro, R. (2018). ISO 27001: El impacto en los Sistemas de Gestión de Seguridad de la Información. [online] PMG SSI - ISO 27001. Disponible en: https://www.pmg-ssi.com/2015/04/iso-27001-el-impacto-en-los-sistemas-de-gestion-de-seguridad-de-la-informacion/ [Accedido 20 Julio. 2018].

16. Vecino, Hugo. (2017). Normas ISO y marcos de referencia para gobernanza de las TIC, revisión. Memoria: Comtel 2017-ISSN 2520-3363. 1. 27.

17. Valbuena Villanueva, C. and Diaz Labrador, Y. (2018). Propuesta de Modelo de un Sistema de Gestión de la Seguridad de la Información Aplicada a Hospitales Privados (Ips). [online] Repository.udistrital.edu.co. Disponible en: http://repository.udistrital.edu.co/handle/11349/13417 [Accedido 7 Agos. 2018].

18. Valencia Duque, Francisco & Orozco-Alzate, Mauricio. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. RISTI - Revista Ibérica de Sistemas e Tecnologías de Información. 73-88.

19. 27001Academy. (2018). ¿Qué es norma ISO 27001? [online] Disponible en: https://advisera.com/27001academy/es/que-es-iso-27001/ [Accedido 15 junio. 2018].