RECOMENDAR MEDIDAS DE SEGURIDAD INFORMÁTICA A LOS SISTEMAS DE INFORMACIÓN ADMINISTRATIVOS Y ACADÉMICOS DEL COLEGIO MIXTO SAN FELIPE NERI DE IPIALES, EN RELACIÓN A LAS AMENAZAS Y VULNERABILIDADES IDENTIFICADAS EN CADA UNO DE LOS SISTEMAS

PABLO ANÍBAL VELÁSQUEZ ROSALES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IPIALES-NARIÑO
2017

RECOMENDAR MEDIDAS DE SEGURIDAD INFORMÁTICA A LOS SISTEMAS DE INFORMACIÓN ADMINISTRATIVOS Y ACADÉMICOS DEL COLEGIO MIXTO SAN FELIPE NERI DE IPIALES, EN RELACIÓN A LAS AMENAZAS Y VULNERABILIDADES IDENTIFICADAS EN CADA UNO DE LOS SISTEMAS.

PABLO ANÍBAL VELÁSQUEZ ROSALES

Trabajo de grado para optar el título de Especialista en seguridad informática

Asesor

Esp. Daniel Felipe Palomo Luna

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IPIALES-NARIÑO
2017

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Ipiales, diciembre 2017

DEDICATORIA

A mi hijo Gabriel por la alegría que le ha dado a mi vida con su existencia, a mi hija Tania y a su recuerdo imborrable convertido en mi ángel de la guarda por disposición de Dios, a mi esposa por su fortaleza, comprensión y el apoyo incondicional en las buenas y las malas, a mis padres, porque a pesar de su vejez, aún siguen preocupándose por el bienestar de sus hijos, a toda mi familia por ser la motivación para seguir adelante.

AGRADECIMIENTOS

A Dios por el acompañamiento y la fortaleza para no claudicar.

A mi esposa y mi hijo por el auxilio en los momentos difíciles.

A mis padres y hermanos por su apoyo incondicional.

A la comunidad educativa del colegio Mixto San Felipe Neri de Ipiales por la oportunidad de trabajar y permitirme diseñar este proyecto, en especial al prepósito del oratorio de san Felipe Neri, Presbítero Esteban Job Solarte.

A mi asesor de proyecto especialista Daniel Palomo, por su colaboración y atención siempre oportuna.

A todos los tutores, consejeros, compañero estudiantes y demás funcionarios de la UNAD que de una u otra manera me apoyaron durante todo este proceso de estudio.

CONTENIDO

pág.

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

AUTENTICACIÓN: es el procedimiento de comprobación de la identidad de un usuario que quiere acceder a una red WIFI o a los sistemas de información.

CONFIDENCIALIDAD: es la garantía existente de que la información no está disponible para personas, entidades o procesos no autorizados.

CMSFN: sigla que identifica al Colegio Mixto San Felipe Neri de Ipiales.

DISPONIBILIDAD: es la garantía que tienen los usuarios autorizados en una organización, para disponer del acceso a la información y a los activos asociados cuando así lo requieran.

EQUIPO DE CÓMPUTO: dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas, realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando diversos tipos de información.

FIREWALL: software o hardware configurados para permitir, denegar, limitar, cifrar, descifrar, el tráfico de información entre los diferentes dispositivos conectados a una red de datos.

HACKING ÉTICO: o "*pen tests*" Son actividades ejecutadas por una o más personas, quienes, usando sus conocimientos de informática y seguridad, realizan pruebas en redes de datos, con el objeto de encontrar vulnerabilidades, para luego reportarlas y así tomar medidas de seguridad informática.

INTEGRIDAD: en el ámbito de la seguridad de la información, la integridad hace referencia a mantener los datos intactos, libre de modificaciones o alteraciones efectuadas por terceros, sin previa autorización.

MAGERIT: es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica.

MEDIO REMOVIBLE: es cualquier dispositivo o componente extraíble de hardware, que puede ser usado para el almacenamiento de información; tales como: sim card, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

NO REPUDIO: es la garantía de participación de las partes en una comunicación, para la cual existe un emisor y un receptor, donde se garantiza que la persona que envía el mensaje no puede negar que es el emisor del mismo, ya que el receptor tendrá pruebas del envío y el receptor no puede negar que recibió el mensaje, porque el emisor tendrá pruebas de la recepción del mismo.

PREPÓSITO: sacerdote de la congregación del oratorio de san Felipe Neri, quien tiene toda la autonomía de dirigir las riendas del Oratorio de San Felipe Neri, la Parroquia de nuestra señora de los dolores y representa legalmente al colegio Mixto San Felipe Neri de Ipiales.

PEN TESTS: en español se conocen como "pruebas de penetración", define el intento de múltiples formas de burlar la seguridad de las redes de datos, para robar información sensitiva de una organización, para luego reportarlo a dicha organización y así mejorar su seguridad.

PRIVACIDAD: hace referencia a la protección de datos o privacidad de la información, en donde la organización o el propietario de la información es quien determina que datos en un sistema informático, pueden ser compartidos con terceros.

PRIVILEGIO: nivel de confianza perteneciente a un objeto de sistema.

POLÍTICA DE SEGURIDAD: conjunto de reglas que ponen en práctica los requisitos de seguridad del sistema.

RECURSOS TECNOLÓGICOS: son aquellos componentes de hardware y software tales como: estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones, servicios de red de datos, *tablets*, celulares, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior del colegio mixto san Felipe Neri

RESPONSABLE DEL ACTIVO DE INFORMACIÓN: es la persona asignada para identificar, clasificar y proteger los activos de información a su cargo, además de velar por la confidencialidad, la integridad y disponibilidad de los mismos.

SAPRED: sistema administrador de procesos educativos

SGSI: sistema de gestión de seguridad de la información.

SOFTWARE MALICIOSO: es una variedad de software o programa, que tienen como objeto infiltrarse en los equipos de cómputo, con el ánimo de perjudicar los recursos tecnológicos, sistemas operativos, redes de datos, sistemas de información, etc.

UPS: *uninterruptible power supply*, Dispositivo que permite almacenar energía eléctrica en una o varias baterías internas, que por un tiempo limitado y durante un corte de energía, solventa de fluido eléctrico al o los dispositivos que se encuentren conectados.

VULNERABILIDADES: son aquellas debilidades expuestas al aprovechamiento de terceros y demás factores externos no controlables, que se constituyen en fuentes de riesgo para los activos de información del colegio mixto san Felipe Neri de Ipiales.

WIFI: o Wi-Fi, es la abreviación de la marca comercial *Wireless Fidelity*, y que en español significa fidelidad inalámbrica sin cables, La infraestructura de una conexión WiFi incluye emisores remotos.

RESUMEN

La pérdida de información digital en cualquier ámbito laboral o empresarial es un riesgo latente que puede acontecer en cualquier momento, como consecuencia del exceso de confianza y la falta de inversión en seguridad informática por parte de las personas y las empresas, la contratación de profesionales idóneos en la recuperación de la información digital perdida, genera un costo enorme para los afectados, porque incluso hoy en día y con la tecnología existente es muy poco probable recuperar el 100% de dicha información.

Lastimosamente la mayoría de entidades públicas y privadas no invierten en seguridad informática, desconocen la implementación de políticas apropiadas de seguridad informática al interior de los sistemas de información que manejan, y comúnmente se toman acciones correctivas cuando el daño se ha producido, perdiendo así tiempo, dinero, e incluso clientes.

El desarrollo de este proyecto establece las recomendaciones apropiadas de seguridad informática a los sistemas de información administrativos y académicos del Colegio Mixto San Felipe Neri de Ipiales, con el fin de reducir en la medida de las posibilidades los riegos, amenazas y vulnerabilidades que se hayan identificado, permitiendo así salvaguardar los recursos informáticos del Colegio y colaborando paralelamente con la institución en la consecución de sus objetivos académicos y administrativos.

Palabras clave: DELINCUENCIA INFORMÁTICA, AMENAZA, RIESGO, VULNERABILIDAD, DELINCUENTE INFORMÁTICO, INFORMACIÓN DIGITAL, VIRUS INFORMÁTICO, DENEGACIÓN DE SERVICIOS, CONFIDENCIALIDAD,

INTEGRIDAD, DISPONIBILIDAD, SISTEMAS DE INFORMACIÓN, DECLARACIÓN DE APLICABILIDAD.

INTRODUCCIÓN

Evidentemente el avance tecnológico facilita la realización de muchas actividades laborales y personales, hacer referencia a los métodos tediosos y complejos que antes se debían realizar por la falta de procesos informáticos y que en la actualidad se efectúan rápida y acertadamente, dan fe de la importancia del aprovechamiento de estos adelantos, pero de la misma manera en que se aprovecha para el bien, se aprovecha también para el mal, de ahí que la delincuencia informática crezca paulatinamente y se haga cada vez más común en los entornos educativos, empresariales, personales, profesionales y otros tantos que sin saberlo se convierten en objeto de vulnerabilidad y de fácil ataque de los delincuentes informáticos, que se mantienen al acecho buscando robar o dañar información.

En la actualidad la gran mayoría de las empresas hacen uso de la información digital y lo han convertido en uno de sus activos más importantes, justamente esta información está expuesta a una gran variedad de riesgos y vulnerabilidades que podrían facilitar los fraudes informáticos, como: robo de información, pérdida de información, modificación de información, virus informáticos, ataques de denegación de servicios, etc.

El colegio Mixto San Felipe Neri de la ciudad de Ipiales, es una institución educativa de carácter privado y no ha sido indiferente a esta problemática, a pesar que se tiene gran cantidad de información académica y financiera, con el tiempo se ha ido acumulando, lastimosamente no se tiene implementado hasta el momento ningún tipo de estrategias óptimas que permitan salvaguardar la información que se genera,

y por tal motivo en estos momentos es inexistente la protección apropiada de la confidencialidad, integridad y disponibilidad oportuna de la información del colegio.

El presente trabajo tiene como propósito recomendar políticas de seguridad informática que permitan ejecutar acciones en favor de los sistemas de información del colegio mixto san Felipe Neri de la ciudad de Ipiales, haciendo un análisis de los riesgos a los que se ve expuesta la información que aquí se gestiona.

Haciendo uso de la metodología MAGERIT, se buscará Identificar las amenazas y vulnerabilidades de los sistemas de información, realizando un análisis de los resultados obtenidos, respecto de las amenazas y vulnerabilidades que se hallan identificado

Se investigará acuciosamente, con el fin de diseñar y recomendar medidas apropiadas de seguridad informática a los sistemas de información administrativos y académicos del colegio.

Por otra parte, y con el propósito de evitar escenarios de ilegalidad, se solicitó la aprobación de la congregación del oratorio de san Felipe Neri de Ipiales, para llevar a cabo el presente proyecto; al mismo tiempo se declara que todas las pruebas que se realicen, se ampararán tomando como base el *Hacking* ético.

1 DESCRIPCIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

El Colegio Mixto San Felipe Neri de la ciudad de Ipiales, tiene implementada una red de datos LAN y WLAN con acceso a INTERNET, que gestiona el manejo de la información tanto académica como financiera, dicha información no cuenta con un sistema de seguridad óptimo y continuamente se han venido presentando inconvenientes en la transferencia, copia, modificación y envío de información.

Cada vez que se suscita un inconveniente de este tipo, otros procesos deben esperar hasta que se pueda dar solución al problema presentado, puesto que la comunicación entre los diversos dispositivos conectados a la red del colegio y el manejo actual de la información no permite garantizar debidamente los principios de confidencialidad, integridad y autenticidad de la información, se están presentando los siguientes inconvenientes:

- Las instalaciones físicas del colegio son compartidas con la Corporación Unificada nacional “CUN” de Ipiales, de esta situación se desprende la posibilidad del acceso de terceros sin autorización a la red de datos del colegio.
- Existen problemas en el acceso a la información de las diferentes dependencias desde los entornos de red de forma apropiada.
- La información compartida entre los diferentes dispositivos puede estar en riesgo de ser obtenida por terceros sin autorización.
- No existen políticas de seguridad.

- No existe un cronograma de procesos de *Backups* que permitan salvaguardar la información.

- La actualización de software no se realiza de forma periódica, porque no existen responsables de ejecutar estos procedimientos.

- Las contraseñas de acceso a las conexiones *WIFI* se comparten sin ningún tipo de control con docentes, estudiantes y padres de familia.

Hasta el momento las directivas del colegio no han procurado la implementación de medidas de seguridad informática y hasta la fecha no se cuenta con una persona o personas responsables de los sistemas de información que estén al tanto, de gestionar políticas de seguridad al interior de los diversos procesos informáticos, los sistemas de información del colegio mixto san Felipe Neri de Ipiales coexisten con considerables riesgos, amenazas y vulnerabilidades; algunas de ellas identificadas y otras no identificadas, lastimosamente no se han tomado medidas oportunas que permitan de alguna manera impedir la fuga, modificación o daño en la información que se administra al interior del colegio, presuntamente porque aún no ha sucedido una pérdida de información considerable.

1.2 FORMULACIÓN DEL PROBLEMA

¿Se hace necesario recomendar medidas de seguridad informática a los sistemas de información administrativos y académicos del colegio mixto San Felipe Neri de Ipiales, en relación a las amenazas y vulnerabilidades identificadas?

2 JUSTIFICACIÓN

Tomando como base el hecho, que el avance tecnológico sigue ascendiendo permanentemente, no podemos desconocer que esto involucra claramente los sistemas de información, software, comunicaciones y otros tantos.

Ante estas condiciones de favorabilidad en el auge de la tecnología, se han acelerado los procesos informáticos cotidianos de las empresas, organizaciones y demás instituciones, en donde también se incluye a las instituciones educativas.

Hoy en día se ha podido apreciar, como diferentes colegios ofrecen conjuntamente con su portafolio de servicios, la oportunidad de cargar, actualizar y consultar información en línea, brindando no solo un servicio a los padres de familia, estudiantes y docentes, sino que también al mismo tiempo, se exponen a los diferentes ataques informáticos prolíferos en la INTERNET.

En este compendio de escenarios, la tecnología no solamente ha permitido la aceleración de los procesos de los sistemas de información, paralelamente se produce un incremento de los delitos informáticos, y es indudable que siempre que alguien se conecta a una red de datos pública o privada, estará expuesto al robo de información y al acceso de la misma por personas no autorizadas, consecuentemente este tipo de sucesos, hace necesarias la toma de medidas oportunas que permitan proteger la información del colegio, del acceso no autorizado.

El Interés por mitigar la problemática generada, ante la falta de estrategias de protección de la información del Colegio San Felipe Neri, motiva el desarrollo del presente proyecto, buscando recomendar medidas apropiadas de seguridad

informática que garanticen el correcto acceso y funcionamiento de los sistemas de información.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar medidas de seguridad informática a los sistemas de información administrativos y académicos, haciendo uso de la metodología MAGERIT para el colegio mixto san Felipe Neri de Ipiales.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar las amenazas y vulnerabilidades de los sistemas de información del colegio mixto san Felipe Neri de Ipiales.

- Realizar un análisis de la información obtenida de las amenazas y vulnerabilidades de los Sistemas de Información.

- Diseñar manual con políticas de seguridad informática al interior del colegio mixto san Felipe Neri, en relación al manejo y tratamiento de los sistemas de información académicos y administrativos.

4 ALCANCE Y DELIMITACIÓN DEL PROYECTO

Tomando en cuenta que el Colegio Mixto San Felipe Neri está certificado en calidad bajo la norma ISO 9001:2008, se hace notoria una gran falencia al interior de la seguridad de sus sistemas de información y consiste en no tener certificado un proceso que garantice la seguridad de la información, por lo que nunca se le ha efectuado ningún tipo de auditoría interna, ni externa a este proceso.

La posibilidad de gestionar la certificación en ISO/IEC 27001:2013, no es una prioridad para el colegio, pero si se considera por el momento delimitar el alcance del proyecto de la siguiente forma:

- La identificación de los activos que integran los sistemas de información administrativos y académicos del Colegio Mixto San Felipe Neri de Ipiales.

- La identificación de las vulnerabilidades, amenazas y riesgos a los que están expuestos los activos identificados.

- La aplicación de la metodología MAGERIT para realizar la evaluación y el análisis de riesgos.

- La elaboración del documento con la declaración de aplicabilidad bajo la normatividad ISO/IEC 27001:2013, con el objeto de mantener el registro y control de las medidas de seguridad que sean aplicadas.

Este proyecto se recomendará para que sea a aplicado a los sistemas de información tanto administrativos como académicos del Colegio Mixto San Felipe

Neri de la ciudad de Ipiales, en el departamento de Nariño. Se pretende desarrollar el proyecto durante los meses de agosto a noviembre del presente año.

4.1 IMPACTO DEL PROYECTO

El desarrollo del presente proyecto pretende diseñar un apropiado Sistema de gestión de Seguridad informática, basado en la ISO/IEC 27001:2013, con el propósito de que a futuro se posibilite la implementación de la seguridad de la información del colegio Mixto San Felipe Neri de Ipiales y así se pueda garantizar la protección y aseguramiento de su información, conscientes que es fundamental poder desarrollar procesos informáticos seguros, que apoyen el trabajo de las diferentes gestiones, tanto directiva, académica, administrativa financiera y comunitaria del colegio según lo contemplado en la guía 34 del ministerio de educación nacional de Colombia.

Igualmente se encamina en hacer posible dar cumplimiento a la Misión y alcanzar las expectativas propuestas en la Visión del colegio para el año 2018.

Por otra parte, se espera que el SGSI genere un impacto positivo en el ahorro de inversión financiera en posibles reparaciones o compras de nuevos elementos de cómputo para el colegio, ya que en la medida de que los docentes y demás personal tengan una conciencia clara de cuál es la información que se debe proteger, y gestione adecuadamente sus riesgos, se podrá evitar inversiones innecesarias en seguridad y tecnología.

5 MARCO REFERENCIAL

La ciudad de Ipiales se proyecta hacia un continuo crecimiento comercial por ser ciudad fronteriza, actualmente percibimos como muchos colombianos, especialmente del departamento de Antioquia y del eje cafetero han migrado a esta ciudad, ellos establecen nuevos negocios y han convertido en su residencia permanente la *ciudad de las nubes verdes*[1].

Al mismo tiempo la devaluación del peso frente al dólar, ha motivado el incremento de la compra de productos en la ciudad de Ipiales por parte de los ciudadanos ecuatorianos, paralelamente en los últimos años se ha visto reflejada mayor inversión económica, en bienes muebles e inmuebles, nuevas urbanizaciones aparecen y demás escenarios surgen gradualmente. Ante este hecho el sector educativo no ha sido, ni puede ser indiferente, los nuevos vecinos de Ipiales buscan alternativas de estudio para sus hijos, es en este espacio donde también los colegios privados entran en competición en aras de matricular más estudiantes y acrecentar sus ingresos económicos.

En consecuencia este proyecto está orientado en pro de implementar medidas de seguridad informática al interior de los sistemas de información del Colegio Mixto San Felipe Neri de la ciudad de Ipiales, porque así como es importante asegurar la sostenibilidad económica de un negocio, también es importante garantizar la salvaguarda de la información que se genera en el colegio, buscando así, poder garantizarle a los clientes (Estudiantes y padres de familia), un adecuado manejo de la información académica y financiera.

[1] Ipiales es conocida como La ciudad de las nubes verdes, obtenido de: http://www.colombiaturismoweb.com/DEPARTAMENTOS/NARINO/MUNICIPIOS/IPIALES/IPIALES.htm

5.1 MARCO TEÓRICO

Al implementar un sistema de gestión de seguridad informática debemos tomar en cuenta diversas políticas y procedimientos de seguridad de la información, que objetivamente deben ser articulados con la identidad del servicio que presta la organización, y estos procedimientos surgen como una herramienta que pretende concientizar a cada uno de los miembros de la estructura organizacional, y que en el caso particular del presente proyecto involucra a todos los empleados del Colegio Mixto San Felipe Neri de la ciudad de Ipiales.

5.1.1 ISO/IEC 27000: Es un conjunto de estándares desarrollados por ISO (Organización internacional de Estandarización) e IEC (Comisión electrotécnica internacional), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Algunas de las normas que conforman la serie ISO/IEC 27000 van encaminadas precisamente a documentar mejores prácticas en estos aspectos, y orienta en la adaptación de disposiciones concretas como la norma ISO/IEC 27001, que indica qué requisitos deben conformar un SGSI[2], pero no estipula cómo cumplirlos. Gracias a estas recomendaciones se posibilita obviar la redundancia en la definición de requisitos, obteniendo un valioso ahorro en tiempo y en la implantación del SGSI.

Se toma entonces como base el fundamento del estándar ISO/IEC 27001,

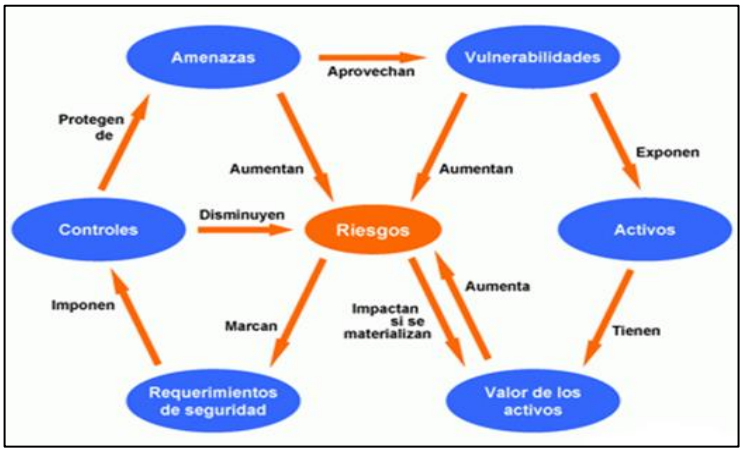
[2] Sistema de Gestión de Seguridad de la Información, Fuente: http://www.iso27000.es/sgsi.html

5.1.2 ISO/IEC 27001: Fue publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013. Es la norma principal de la serie 27000 y además contiene los requisitos del sistema de gestión de seguridad de la información.

En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización debe argumentar sólidamente la no aplicabilidad de los controles no implementados.

5.1.3 Aplicación de un SGSI: Un Sistema de Gestión de Seguridad de la Información (SGSI) establece políticas y procedimientos articulados con los objetivos propuestos por una organización que intenta que sus sistemas informáticos se expongan lo menos posible al nivel de riesgo que la organización haya decidido asumir.

Figura 1 Riesgos SGSI



Fuente: http://www.iso27000.es/sgsi.html

5.1.4 MAGERIT[3] Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Fue desarrollada por el Consejo Superior de Administración Electrónica en el año 2012, la versión actual es la No. 3, y es de libre implementación.

El método que propone ha tenido gran aceptación por la reflexión de la metodología que se aplica y la abundante información que existe, igualmente evidencia gran cantidad de ejemplos de implantación exitosos.

El objetivo primordial de la metodología MAGERIT es conocer los riesgos para minimizarlos y en lo posible eliminarlos, aplicando la implantación de controles de seguridad.

5.1.5 Ciclo PHVA EL Ciclo PHVA (planear, hacer, verificar y actuar) es un concepto gerencial que potencializa la relación entre el ser humano y los procesos.

Se constituye como el concepto central de la Administración por Calidad Total (ACT) y el eje sobre el que giran todas sus metodologías y prácticas.

Aunque inicialmente se aplicó en el desarrollo de nuevos productos, en la actualidad es aplicable en cualquier entorno, para el control de los procesos tanto en la empresa, como en la vida personal.

Aplicar el ciclo PHVA a partir de la adecuada interpretación de su planteamiento original, de su forma de operación, sus manifestaciones y el potencial que

[3] https://sites.google.com/a/misena.edu.co/metodologias-de-evaluacion-de-riego-informatico/

representa para la administración de la organización y para las personas, permite mejorar la efectividad los resultados.

5.1.6 ¿Qué es la seguridad de la información? Reconociendo que la información digital para cualquier persona natural o jurídica es un recurso que al igual que los activos comerciales, tienen un valor incalculable cuando no se puede recuperar, por simple deducción deben también ser protegidos.

Toda empresa que haga uso de información debería salvaguardarla de una amplia gama de amenazas, a fin de garantizar la continuidad de la misma, minimizando el daño que se pudiera causar por fallas en la seguridad de la información.

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

Es necesario propender por el diseño y/o implementación de medidas reactivas a proactivas en la gestión de la seguridad. Las medidas reactivas son soluciones parciales, medidas de protección implementadas sin apenas intervención del usuario, que básicamente consisten en “la instalación del producto” sin un seguimiento y control continuado.

Los riesgos a los que se ven expuestas las empresas hacen necesario la creación de directrices que orienten hacia un uso responsable de los recursos. Las políticas de seguridad son documentos que constituyen la base del entorno de seguridad de

una empresa y deben definir las responsabilidades, los requisitos de seguridad, las funciones, y las normas a seguir por los empleados de la empresa.

5.2 MARCO LEGAL

5.2.1 Decreto 1526 de 2002. Por el cual se indica la obligatoriedad de La información básica que debe contener el sistema de información del sector educativo.

5.2.2 Ley 1341 de 2009. De las nuevas tecnologías de la información y la comunicación. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

5.2.3 Ley 1273 de 2009. Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

En esta ley se tipificó como delitos, una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

5.2.4 Ley Estatutaria 1581 de 2012. Protección de datos personales, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional, como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

5.2.5 Decreto 1377 de 2013 Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012.

5.2.6 Ley Estatutaria 1266 del 31 de diciembre de 2008 Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. se refiere al que todo individuo puede conocer, actualizar y rectificar toda información que se relacione con él, la cual se encuentra almacenada en centrales de información.

5.2.7 Ley 527 de agosto de 1999 Comercio electrónico. Por medio del cual se define y reglamenta el acceso y usos de los mensajes de datos del comercio electrónico y de las firmas digitales y se establece las entidades de la certificación y se dictan otras disposiciones.

5.3 MARCO CONTEXTUAL

Este proyecto se lleva a cabo en el Colegio Mixto San Felipe Neri, ubicado en la carrera 4ta No 13-29 del municipio de Ipiales, departamento de Nariño, la institución educativa está bajo la supervisión y direccionamiento de los sacerdotes de la Congregación del oratorio de San Felipe Neri, el Presbítero Esteban Job Solarte quien se desempeña como prepósito[4] del Oratorio y representante legal del colegio. Al mismo tiempo se fomentan actividades de tipo educativo, de formación en conocimientos y valores, conjuntamente con los procesos de administración y operatividad de la institución.

Para realizar las actividades administrativas y académicas el personal directivo, docentes y administrativo cuenta con 6 equipos de cómputo propiedad de la institución, 20 computadores en el laboratorio de informática y 5 computadores portátiles de propiedad de docentes. El tiempo destinado para la aplicación del proyecto será de cuatro meses.

5.4 MARCO CONCEPTUAL

5.4.1 Especificaciones de la ISO/IEC 27001[5] Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI).
Requiere:

[4] Primero, principal o jefe de una colectividad. Quien la dirige o preside. http://universojus.com/definicion/preposito
[5] http://www.iso27000.es/download/doc_sgsi_all.pdf

- Organización de la seguridad de la información.
- Política de seguridad.
- Gestión de activos.
- Control de acceso.
- Seguridad de los recursos humanos.
- Cumplimiento.
- Seguridad física y del entorno.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Gestión de las comunicaciones y operaciones.
- Gestión de la continuidad del negocio.
- Gestión de incidentes de seguridad de la información.

Esta norma busca proponer un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI), convirtiéndose en una decisión estratégica para las organizaciones que desean proteger sus activos de los sistemas de información.

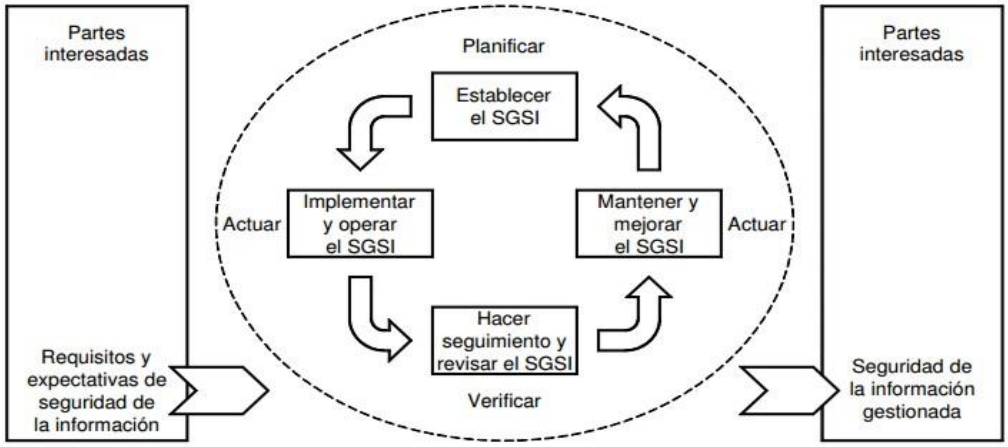
La implementación de un SGSI intenta ajustarse en su totalidad a las necesidades y expectativas que exigen las organizaciones hoy en día, por ejemplo, una situación simple requiere una solución de SGSI simple. A la par se puede usar para evaluar la conformidad de las partes interesadas, tanto internas como externas.

Si una organización quiere funcionar competentemente debe identificar y gestionar muchas actividades, considerando cada una de las actividades que hagan uso de los recursos y cuya gestión permita la transformación de entradas en salidas.

A menudo el resultado de un proceso constituye directamente la entrada del proceso siguiente. La aplicación de un sistema de procesos dentro de una organización,

junto con la identificación e interacciones entre estos procesos, y su gestión, se puede denominar como un “enfoque basado en procesos”, que necesita de la adopción del modelo PHVA, también reflejado en los principios establecidos en las Directrices OCDE (2002)[6] que controlan la seguridad de sistemas y redes de información. Gracias a ello se obtiene un modelo robusto para implementar los principios en aquellas directrices que controlan la evaluación de riesgos, diseño e implementación de la seguridad, gestión y reevaluación de la seguridad.

Figura 2 Modelo PHVA aplicado a los procesos de SGSI



Fuente: Norma Técnica NTC-ISO/IEC colombiana 27001

5.4.2 Amenaza. Es la probabilidad de ocurrencia de un imprevisto que puede ser de origen natural o intencionado; las amenazas representan factores de riesgos externos que pueden explotar una vulnerabilidad existente en la Entidad.

[6] Directrices OCDE para la seguridad de sistemas y redes de información. Hacia una cultura de la seguridad. París: OCDE, Julio de 2002. www.oecd.org.

5.4.3 Confidencialidad. Propiedad de la seguridad de la información, que garantiza que la información solamente pueda ser accedida por las personas autorizadas.

5.4.4 Disponibilidad. Propiedad de la seguridad de la información que garantiza que la información esté disponible y pueda ser accedida por las personas autorizadas en el momento que ellas lo requieran.

5.4.5 Impacto. Son las consecuencias o pérdidas que pueden ocurrir la materialización de una amenaza o la explotación de una vulnerabilidad; el impacto puede afectar los aspectos financieros, tecnológicos, físicos, de imagen o aspectos legales de la entidad.

5.4.6 Integridad. Propiedad que garantiza que la información no ha sido alterada, modificada por personas no autorizadas para hacerlo.

5.4.7 Riesgo. Es la magnitud de pérdidas proyectadas tras la ocurrencia de explotación de una amenaza o vulnerabilidad.

5.4.8 Seguridad Informática. Consiste en los procedimientos, políticas, técnicas y herramientas de hardware y software implementadas con el fin de proteger los sistemas informáticos y la información.

5.4.9 Valoración de riesgos. Proceso que permite la identificación, análisis y administración de los riesgos que internos y externos que posee una organización.

5.4.10 Vulnerabilidad. Es un factor de riesgo interno que representa las debilidades o el grado de exposición de los activos informáticos de la entidad, las vulnerabilidades permiten la explotación de una amenaza.

6 METODOLOGÍA

6.1 ÁREA DE CONOCIMIENTO ESPECÍFICO DEL PROYECTO

Seguridad informática en redes LAN y WLAN.

6.2 CLASE DE INVESTIGACIÓN.

Aplicada, puesto que con el desarrollo del presente proyecto se pretende estructurar recomendaciones apropiadas para los sistemas de gestión de seguridad de la información y procurar su futura implementación en el Colegio Mixto San Felipe Neri de la ciudad de Ipiales.

6.2.1 Técnicas para la recolección de información. La información necesaria para justificar los procesos de investigación efectuados en el desarrollo de este proyecto se describe a continuación:

Cuadro 1. Técnicas para la recolección de información

Técnica	Descripción	Tipo
Encuesta	Con fines de investigación, las encuestas se elaborarán para obtener información específica e importante para la indagación que se realiza.	Abiertas y cerradas

Técnica	Descripción	Tipo
	Se interactuará personalmente de forma espontánea con el fin de efectuar un intercambio de comunicación, buscando obtener los mejores resultados, en la identificación de los hallazgos importantes.	
Entrevista	Se realizará cara a cara, conversando con cada una de las personas que intervienen en el manejo de la información, con el fin de dilucidar y aclarar la información que se está obteniendo. Se formularán preguntas a cada empleado de forma personal, por teléfono o por correo. Se buscará obtener información detallada de los procedimientos habituales realizados respecto del trabajo en los sistemas de cómputo.	Directa, sincrónica y asincrónica.
Prueba	Se auditarán los procedimientos aplicados con el fin de verificar la ejecución de métodos apropiados y el desempeño de cada uno de los participantes para determinar la aptitud, habilidad, conocimiento y grado de responsabilidad.	Directa.
Observación.	Se recogerá información adicional por medio de la Observación Directa, prestando atención a los comportamientos de las personas, mientras realizan sus actividades cotidianas en los sistemas de información, se utilizará como indicador el referente de lo que los participantes ejecutan, haciendo de su propia conducta, la evidencia del grado de asimilación y	Directa

Técnica	Descripción	Tipo
	responsabilidad con la implementación de medidas de seguridad.	

Fuente: http://datateca.unad.edu.co/contenidos/100104/1001004-MODULO-TI-2014-1.pdf

6.3 FASES DE APLICACIÓN

6.3.1 Fase1. Documentación y consulta de información referente a las recomendaciones de medidas de seguridad informática. Para lograr el objetivo que se está proyectando, es necesario tomar como base los conocimientos adquiridos a lo largo del programa de especialización en seguridad informática, indagando todo lo posible y necesario para realizar un ajustado diseño de medidas de seguridad informática, con el propósito de acertar en las recomendaciones y el apropiamiento de los conceptos propios para este fin.

6.3.2 Fase 2. Identificación de activos informáticos. Es necesario direccionar este proyecto a los puntos críticos de la institución educativa en cuanto a las medidas de seguridad informática se refiere, ya que estos puntos representan un riesgo alto de vulnerabilidad, es importante también destacar que no solo se tomará en cuenta el laboratorio de informática, sino también el acceso a los equipos de cómputo de las demás dependencias, claves de acceso de los usuarios, entre otros.

6.3.3 Fase 3. Identificar recursos de software que utiliza el colegio para el manejo de información. Es necesario identificar los recursos de software que se

utilizan en las diferentes dependencias del colegio, verificando si están o no licenciados, con el fin de poder definir estrategias de salvaguarda de la información que se está generando.

6.3.4 Fase 4. Recomendaciones para la implementación de medidas de seguridad informática para el colegio. En esta fase del proyecto se pretende presentar las medidas probables de aplicabilidad, que permitan satisfacer las necesidades y requerimientos identificados en las fases anteriores.

6.3.5 Fase 5. Entrega de resultados e informes. Elaboración de un documento o resultado final que describa el paso a paso del desarrollo del proyecto enfocado a la solución de los problemas identificados.

6.4 ENCUESTAS

6.4.1 Encuesta aplicada a las personas encargadas del manejo de información del colegio. Se procede a encuestar a los responsables directos del manejo de la información

6.4.1.1 Objetivo: Identificar las debilidades que se presentan actualmente al interior de la Seguridad de la Información académica del colegio.

Población y única muestra estadística: 6 personas

Justificación: Se encuestan únicamente a 6 personas, porque cada una de ellas es responsable del manejo y salvaguarda de la información en su respectiva dependencia.

Fecha: septiembre 16 de 2015

Cuadro 2. Resultado de la encuesta aplicada al personal del colegio

Pregunta	SI %	NO %
¿Considera adecuada la seguridad de la información en la oficina a su cargo?	**16.67 %**	**83.33 %**
¿Conoce usted las normas de Seguridad Informática que debe considerar al manejar la información académica del colegio?	**33.33 %**	**66.67 %**
¿Sabe a quién dirigirse cuando se presenta un incidente informático, para buscar una solución oportuna?	**50 %**	**50 %**
¿Ha recibido capacitación y concientización sobre Seguridad Informática dentro del colegio?	**16.67 %**	**83.33 %**
¿Cree que el nivel de Seguridad Informática dentro del colegio es apropiado?	**0 %**	**100 %**
¿Considera que la seguridad informática de la que dispone en su dependencia es suficiente para salvaguardar la información a su cargo?	**33.33 %**	**66.67 %**
¿Conoce usted de la existencia de políticas de Seguridad de la Información, establecidas por el colegio?	**0 %**	**100 %**
¿Realiza copias de seguridad de la información que maneja en sus labores diarias de acuerdo a lo establecido en la organización?	**50 %**	**50 %**
¿Maneja contraseñas Alfanuméricas para el acceso a la red?	**83.33 %**	**16.67 %**

Pregunta	SI %	NO %
¿Maneja contraseñas Alfanuméricas para el acceso al sistema operativo?	**16.67 %**	**83.33 %**
¿Maneja contraseñas Alfanuméricas para el acceso al software contable, de notas o de tesorería?	**33.33 %**	**66.67 %**
¿Cuándo se presenta un inconveniente de software o hardware en el equipo informático a su cargo, este se soluciona oportunamente?	**50 %**	**50 %**
¿Usted cree que es segura la conexión a la red de datos del colegio?	**33.33 %**	**66.67 %**
¿Aplica usted las normas establecidas por el colegio, para evitar la fuga de información?	**33.33 %**	**66.67 %**
¿Cree usted que la organización debería invertir para la implementación de un Sistema de Gestión en Seguridad de la Información?	**100 %**	**0 %**

Fuente: el autor

7 METODOLOGÍA MAGERIT (METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE IT)

MAGERIT es una metodología que se esfuerza por enfatizarse en dividir los activos de la organización en variados grupos, para identificar más riesgos y poder tomar contramedidas para evitar así cualquier inconveniente.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

7.1 IDENTIFICACIÓN DE ACTIVOS INFORMÁTICOS

Los activos son todos los elementos que una organización posee para el tratamiento de la información (hardware, software, recurso humano, etc.). MAGERIT diferencia los activos agrupándolos en varios tipos de acuerdo a la función que ejercen en el tratamiento de la información.

Se relacionó los activos de información de acuerdo con los parámetros dados por las características del colegio Mixto San Felipe Neri.

7.1.1 Valoración de los activos. Cada activo es diferente de otro, por eso para realizar cada valoración conviene tomar en consideración los siguientes aspectos:

- Dimensión en la que cada uno de los activos posee un grado de importancia.
- Estimación de la valoración en cada dimensión

7.1.2 Criterios de la valoración de activos. Permite estimar la importancia de cada activo en una escala del 0 al 10

Cuadro 3. Criterios de Valoración de activos

Nivel	Criterio
10	Nivel 10
9	Nivel 9
8	Nivel 8 (+)
7	Alto
6	Alto
5	Medio (+)
4	Medio
3	Medio (-)
2	Bajo (+)
1	Bajo
0	Depreciable

Fuente: Herramienta PILAR 5.2.9

7.1.3 Dimensiones

- [D] disponibilidad
- [I] integridad de los datos

- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos

Cuadro 4. Tipos de activos informáticos

Tipos de Activo	Descripción	[D]	[I]	[C]	[A]	[T]
Activos de Información	Computadores (Computadores de las diferentes dependencias)	9	9	9	7	7
	Documentación (Sistema de información académica y financiera)	8	8	8		
	Medios de Impresión					8
Software o aplicación	Sistemas operativos,	8	8		7	
	Software para la administración académica y de notas SAPRED.	10	10	10	9	8
		7	7			7
	Software antivirus	8	10	10		8
	Editores de Texto y hojas de cálculo.					

Tipos de Activo	Descripción	[D]	[I]	[C]	[A]	[T]
Hardware	Equipos de oficina (Puestos de Trabajo de los directivos, docentes, secretarias)	9	9	9		
Red	Dispositivos físicos, cableados y de conexión inalámbrica.	9				
	Dispositivos de conectividad de redes	9				
Comunicaciones	Telefonía		7			
	Red WIFI					8
	Red LAN					9
	INTERNET		9	9		
Servicios	Tratamiento de los sistemas información académica.	8	8	8	9	9
Personal	Empleados del Colegio Mixto San Felipe Neri.	10		10	10	
Instalaciones Físicas	Edificio	8				
	Oficinas	8				

Fuente: El autor

Cuadro 5. PC Rectoría

PC RECTORÍA	Descripción
Procesador	Intel Pentium dual CORE 2 GHZ.
Memoria RAM	4 GB

PC RECTORÍA	Descripción
Disco Duro	1 TB

Fuente: El autor

Cuadro 6. PC Secretaría del colegio

PC SECRETARÍA	Descripción
Procesador	Intel CORE I3 3,1 GHZ
Memoria RAM	4 GB
Disco Duro	1 TB

Fuente: El autor

Cuadro 7. PC coordinación

PC COORDINACIÓN	Descripción
Procesador	Intel Celeron 2.16 GHZ.
Memoria RAM	4 GB
Disco Duro	1 TB

Fuente: El autor

Cuadro 8. PC biblioteca

PC BIBLIOTECA	Descripción
Procesador	AMD Athlon 2000+ 1.67 GHZ
Memoria RAM	1,21 GB
Disco Duro	160 GB

Fuente: El autor

Cuadro 9. PC Psicología

PC PSICOLOGÍA	Descripción
Procesador	Intel Pentium dual CORE 2 GHZ.
Memoria RAM	1 GB
Disco Duro	360 GB

Fuente: El autor

Cuadro 10. PC Tesorería

PC TESORERÍA	Descripción
Procesador	PENTIUM 4 3.0 GHZ.
Memoria RAM	1 GB
Disco Duro	360 MB

Fuente: El autor

Cuadro 11. PC Contabilidad

PC CONTABILIDAD	Descripción
Procesador	INTEL CORE i3 2100 3.1 GHZ
Memoria RAM	4 GB
Disco Duro	1 TB

Fuente: El autor

Cuadro 12. PC laboratorio de inglés

PC INGLÉS	Descripción
Procesador	Intel Celeron 2.16 GHZ.
Memoria RAM	4 GB
Disco Duro	1 TB

Fuente: El autor

7.2 OBJETIVOS DE MAGERIT

7.2.1 Directos

- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

7.2.2 Indirectos. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

7.3 IDENTIFICACIÓN DE LOS RIESGOS.

Para la identificación de riesgos que pueden afectar los activos de la información, podemos considerar que los eventos que consiguen incidir directamente sobre la integridad, disponibilidad y confidencialidad de la información son:

7.3.1 Desastres naturales. Eventos catastróficos que pueden comprometer la infraestructura física del medio donde se almacena la información.

7.3.2 Alteraciones del entorno. Los cambios bruscos de temperatura o las condiciones de humedad o sequia puede afectar los equipos electrónicos y por ende la información almacenada en ellos.

7.3.3 Accesos físicos. Son aquellos eventos cuando personal no autorizado accede físicamente a los medios de almacenamiento para ser hurtados, dañados o comprometidos.

7.3.4 Fallas en Hardware. Sucede cuando uno del equipo dispuesto para la protección de la información falla por diferentes razones (falla en disco por agotamiento, memoria, BIOS, etc.)

7.3.5 Virus. Pérdida o daños en la información a causa de programas maliciosos o malware que no son detectados por los antivirus

7.3.6 Corrupción lógica. Actualizaciones de sistemas operativos que generan daños en el hardware o software de los equipos dispuestos para el almacenamiento de la información.

7.3.7 Vulnerabilidades en los sistemas de seguridad. Las fallas o falencias que presenta los sistemas de seguridad que pueden ser aprovechados por externos.

7.3.8 Fugas de información. Revelación de información sensible por parte de funcionarios en cualquier medio de comunicación (Papel, correos, verbal u otros.)

7.4 IDENTIFICACIÓN DE AMENAZAS

Las amenazas se clasifican en cuatro grupos, discriminados así:

- [N] Desastres Naturales
- [I] De origen industrial
- [E] Errores y fallos no intencionados
- [A] Ataques intencionados

El objetivo de subdividir en grupos permite caracterizar el medio al que se enfrenta el sistema, que puede suceder, que consecuencias pueden resultar y que probabilidad existe que ocurra. Podemos resumirlo en la expresión “conoce a tu enemigo”[7]. Esta actividad consta de 2 sub-tareas:

[7] MAGERIT-versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método, https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ç, p 40

- Identificación de las amenazas
- Valoración de las amenazas

Se pueden determinar cómo amenazas, todos los eventos o situaciones que ocasionen un daño en el hardware o pérdida de la información.

Estas amenazas pueden ser de Origen naturales, externas e internas, las podemos categorizar a nivel de la intencionalidad en: Accidentes, errores humanos o incluso acciones malintencionadas.

El problema más grave que presenta la institución, es que no existe un departamento de **sistemas** que se encargue de realizar todos los procesos concernientes a la seguridad, estabilidad e integridad de los equipos, la red, la información, etc.; Sino que todo recae sobre el área académica.

Igualmente, el colegio Mixto San Felipe Neri de Ipiales, está expuesto a otros tipos de amenazas, dentro de las cuales encontramos:

7.4.1 Amenazas Naturales. Ocasionando la pérdida total o parcial de la Infraestructura:

- Terremotos.
- Inundaciones.
- Incendios.
- Explosión.

7.4.2 Amenazas Externas. Pueden causar graves pérdidas de información, tiempo, e incluso dinero.

- Virus informáticos, gusanos, caballos de Troya.
- Intrusos en la red (Accesos de Usuarios no permitidos).
- Pérdida o Robo de la información.
- Conflictos Sociales.
- Fallas eléctricas.
- Robo de equipos usado para el manejo de la información.

7.4.3 Amenazas Internas. Son mucho más costosas, debido a que el atacante tiene mayor acceso a la información.

- Descuido por parte de los empleados y alumnos.
- Uso indebido del Acceso a Internet por parte de los empleados y alumnos.
- Errores en la utilización de herramientas y recursos del sistema.
- Conflictos entre empleados de la empresa que pongan en riesgo la confidencialidad de la información.

7.4.4 Accidentes.

- Daño del Hardware (equipos, servidor, cableado).
- Incendio o inundación provocados ya sea por el personal o por algún daño en el Hardware o agente externo.

7.4.5 Errores.

- Fallas dentro de alguno de los sistemas de información.

- Falla de Servidores.
- Desgaste o daño permanente del Hardware.
- Software desactualizado.
- Ejecución defectuosa de procedimientos.

7.4.6 Acciones Malintencionadas.

- Actividades fraudulentas por parte de los empleados de la empresa con el fin de obtener algún beneficio económico o social.
- Fuga de información a través del personal que ingresa de manera temporal en sustitución de empleados en vacaciones.

7.4.7 Identificación de amenazas al interior del colegio. En el siguiente cuadro se relacionan los activos del colegio y la exposición de amenazas.

Cuadro 13. Identificación de amenazas en activos

ACTIVOS	AMENAZAS
Ofimática	[E.1] Errores de los usuarios [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualizaciones de programas (software) [E.8] Difusión de software dañino
Antivirus	[E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualizaciones de programas (software)
Sistema Operativo	[I.5] Avería de origen físico o lógico

ACTIVOS	AMENAZAS
	[E.1] Errores de los usuarios [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualizaciones de programas (software) [A.7] Uso no previsto
Sistema de Información	[E.1] Errores de los usuarios [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualizaciones de programas (software) [A.7] Uso no previsto [A.24] Denegación de servicios [A.11] Acceso no autorizado
Base de datos	[E.1] Errores de los usuarios [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualizaciones de programas (software) [E.8] Difusión de software dañino
Servidor de base de datos	[E.2] Errores del administrador [E.23] Errores de mantenimiento, actualización de equipos hardware [A.11] Acceso no autorizado [N.1] Daños por Fuego [I.2] Daños por agua [I.3] Contaminación medioambiental [I.5] Avería de origen físico o lógico

ACTIVOS	AMENAZAS
	[I.7]Condiciones inadecuadas de temperaturas o humedad
Impresoras	[I.5] Avería de origen físico o lógico [I.7]Condiciones inadecuadas de temperaturas o humedad [E.23] Errores de mantenimiento, actualización de equipos hardware [A.11]Acceso no autorizado
Equipos de escritorio	[I.2] Daños por agua [I.5] Avería de origen físico o lógico [I.7]Condiciones inadecuadas de temperaturas o humedad [E.23] Errores de mantenimiento, actualización de equipos hardware [E.24] Caída del sistema por agotamiento de recursos [A.11]Acceso no autorizado [A.6] Abuso de privilegios de acceso
SWITCH 32 puertos TRENET	[I.2] Daños por agua [I.5] Avería de origen físico o lógico [I.7]Condiciones inadecuadas de temperaturas o humedad [E.24] Caída del sistema por agotamiento de recursos
MÓDEM - ROUTER	[I.2] Daños por agua [I.5] Avería de origen físico o lógico [I.3] Contaminación medioambiental [E.4] Errores de configuración [E.24] Caída del sistema por agotamiento de recursos
Cámaras de seguridad	[A.11]Acceso no autorizado

ACTIVOS	AMENAZAS
	[I.2] Daños por agua [I.3] Contaminación medioambiental [I.5] Avería de origen físico o lógico
Telefonía	[I.8] Fallo de servicios de comunicaciones [E.9] Errores de [re-]encaminamiento [E.15] Alteración de la información [E.19] Fugas de información [A.7] Uso no previsto [A.10] Alteración de secuencia [A.12] Análisis de tráfico [A.14] Interceptación de información (escucha)
Red LAN	[E.9] Errores de re-encaminamiento [E.10] Errores de secuencia [A.5] Suplantación de la identidad del usuario [A.10] Alteración de secuencia [A.11] Acceso no autorizado
Red WIFI	[E.9] Errores de re-encaminamiento [E.10] Errores de secuencia [A.5] Suplantación de la identidad del usuario [A.10] Alteración de secuencia [A.11] Acceso no autorizado
Internet	[I.8] Fallo de servicios de comunicaciones [E.15] Alteración de la información
Disco duro Externo	[A.11] Acceso no autorizado [E.15] Alteración de la información [A.15] Modificación de la información [I.5] Avería de origen físico o lógico
Generador eléctrico	[I.3] Contaminación medioambiental

ACTIVOS	AMENAZAS
	[I.7]Condiciones inadecuadas de temperaturas o humedad
UPS	[I.7]Condiciones inadecuadas de temperaturas o humedad
Cableado	[I.3] Contaminación medioambiental [I.7]Condiciones inadecuadas de temperaturas o humedad
Sistema de Vigilancia	[I.3] Contaminación medioambiental [I.7]Condiciones inadecuadas de temperaturas o humedad
Mobiliario	[N.1] Daños por Fuego [I.2] Daños por agua
Edificio	[N.1] Daños por Fuego [I.2] Daños por agua [N.*.1] Tormentas [N.*.4] Terremotos

Fuente: El autor

Cuadro 14. Identificación amenazas empleados

EMPLEADOS	AMENAZAS
Rector	[E.28.1] Enfermedad [A.30] Ingeniería Social [A.29] Extorsión
Coordinador	[E.28.1] Enfermedad [A.30] Ingeniería Social [A.29] Extorsión
Psicóloga	[E.28.1] Enfermedad

EMPLEADOS	AMENAZAS
	[A.30] Ingeniería Social [A.29] Extorsión
Contadora	[E.28.1] Enfermedad [A.30] Ingeniería Social [A.29] Extorsión
Auxiliar Contable	[E.28.1] Enfermedad [A.30] Ingeniería Social [A.29] Extorsión
Secretaria	[E.28.1] Enfermedad [A.30] Ingeniería Social [A.29] Extorsión
Bibliotecaria	[E.28.1] Enfermedad [A.30] Ingeniería Social [A.29] Extorsión
Docentes	[E.28.1] Enfermedad [A.30] Ingeniería Social [A.29] Extorsión
Servicios generales	[E.28.1] Enfermedad [A.30] Ingeniería Social [A.29] Extorsión

Fuente: El Autor

7.5 IDENTIFICACIÓN DE VULNERABILIDADES.

Al interior del colegio es preocupante confirmar que algunos estudiantes tienen acceso a INTERNET no autorizado desde sus equipos móviles, aunque muchos de

ellos incluso no son descubiertos, se presume que el acceso a la red se utiliza por parte de los estudiantes para acceder a las redes sociales y descargar aplicaciones, pero este hecho de conocer la clave de acceso WIFI, deja en evidencia la vulnerabilidad de la *WLAN*, más aún si tomamos en cuenta que se pone en riesgo la información de aquellos equipos que tienen carpetas compartidas en la red.

El análisis de los hallazgos encontrados en la institución, se clasifican de la siguiente manera:

7.5.1 Problemas Encontrados. El principal problema es la falta de responsabilidad de algunos usuarios autorizados con conexión a la red, que comparten la clave WIFI con estudiantes e incluso con funcionarios de la universidad CUN.

Esto ha suscitado en algunas ocasiones la saturación de conexiones que tiene la red inalámbrica, por causa de la cantidad de equipos conectados en forma simultánea, disminuyendo el rendimiento en el flujo de información. Ante esta situación se proyecta recuperar la información *MAC* de los diferentes dispositivos móviles autorizados, para compararla con las *MAC* de los dispositivos conectados a la WIFI y realizar un filtrado de acceso configurando dichos permisos desde el mismo *ROUTER*.

7.5.2 Vulnerabilidades encontradas. Se relacionan las siguientes:

- No existe ningún protocolo de seguridad de la información.
- No existe un servidor que administre los servicios.
- El control de acceso de los usuarios es débil.

- Los equipos se conectan entre sí por medio de un módem y de este se conectan al *ROUTER*.
- El acceso a los sitios de internet no está limitado.
- No se ha configurado un *Proxy*.
- No existe un programa que permita rastrear el acceso de los usuarios a la red.
- No existe un protocolo de generación de *Backups*.
- El acceso a INTERNET de forma inalámbrica no cuenta con un filtro *MAC*.
- Aprovechamiento de las debilidades de los identificadores de sesión y sistemas de autenticación.
- Modificación de datos, y en particular la modificación de datos personales de los usuarios
- El control de acceso no ofrece garantías de seguridad, si bien las claves le son entregadas a los profesores, estos desafortunadamente las comparten con los alumnos para que se conecten a la red desde sus equipos móviles.

7.5.3 Pruebas de software. Se realiza un test de caja blanca[8] con el fin de conocer la estructura interna del sitio web disponible para el acceso a SAPRED, y de esta manera poder analizar el desempeño y el funcionamiento del programa.

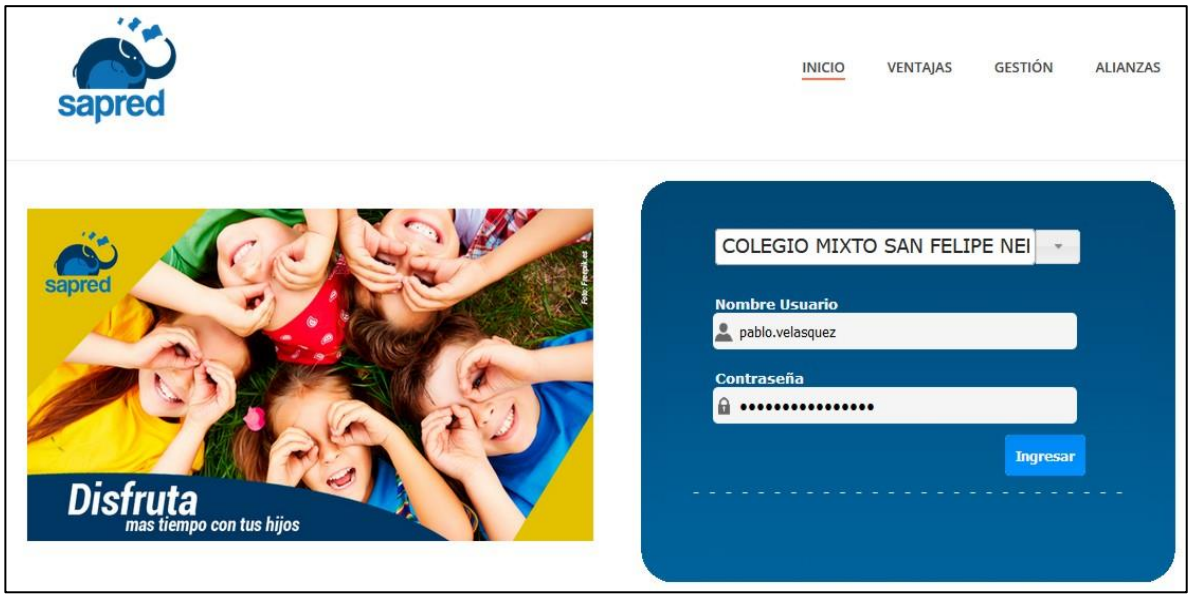
Seguidamente se procederá a realizar una prueba exploratoria del acceso al sitio web, con el objetivo de encontrar posibles problemas en su respectivo funcionamiento.

En la figura 3 se muestra el sitio web y un formulario de ingreso de información, en donde cada uno de los docentes puede seleccionar el colegio mixto san Felipe Neri

[8] Las pruebas de caja blanca (también conocidas como pruebas de caja de cristal o pruebas estructurales) se centran en los detalles procedimentales del software, obtenido de: https://www.ecured.cu/Pruebas_de_caja_blanca

de entre muchas otras instituciones educativas afiliadas a SAPRED[9], posteriormente se ingresa el nombre de usuario, que para todos los usuarios de las diferentes instituciones educativas está compuesto del primer nombre y del primer apellido, separados por un punto y sin espacios.

Figura 3. Ingreso al programa SAPRED desde su URL



Fuente: www.sapred.com

[9] Sistema Administrador de Procesos Educativos

Figura 4. Acceso al software SAPRED

Fuente: www.sapred.com

La figura anterior indica las opciones disponibles después de haber accedido a la plataforma SAPRED.

La figura 5 nos muestra la consulta de información académica de una estudiante del colegio.

Figura 5. Consulta de información académica de estudiantes

Fuente: www.sapred.com

En la plataforma SAPRED contratada por el colegio Mixto San Felipe Neri de Ipiales, se ofrece a los docentes los siguientes servicios Informáticos:

7.5.3.1 Acceso a la plataforma. Cada docente, tendrá un usuario con contraseña que será de uso personal e intransferible.

7.5.3.2 Uso del Servicio de Internet. El docente puede hacer uso de INTERNET para el envío, descarga o visualización de información, propia de su quehacer docente.

7.5.3.3 Manejo de información explícita. Cada docente únicamente podrá gestionar la información correspondiente a su área de desempeño y asignará calificaciones únicamente a los estudiantes a su cargo.

7.5.3.4 Veracidad de la información. La información tramitada en la plataforma, es de entera responsabilidad del docente y no puede ser gestionada por terceros.

7.5.4 Vulnerabilidades de SAPRED por falla de usuario. Se comprueba que algunos docentes no han cambiado la clave de acceso en el sistema SAPRED, clave que se adjudica automáticamente al crear el usuario. Ver ANEXO J.

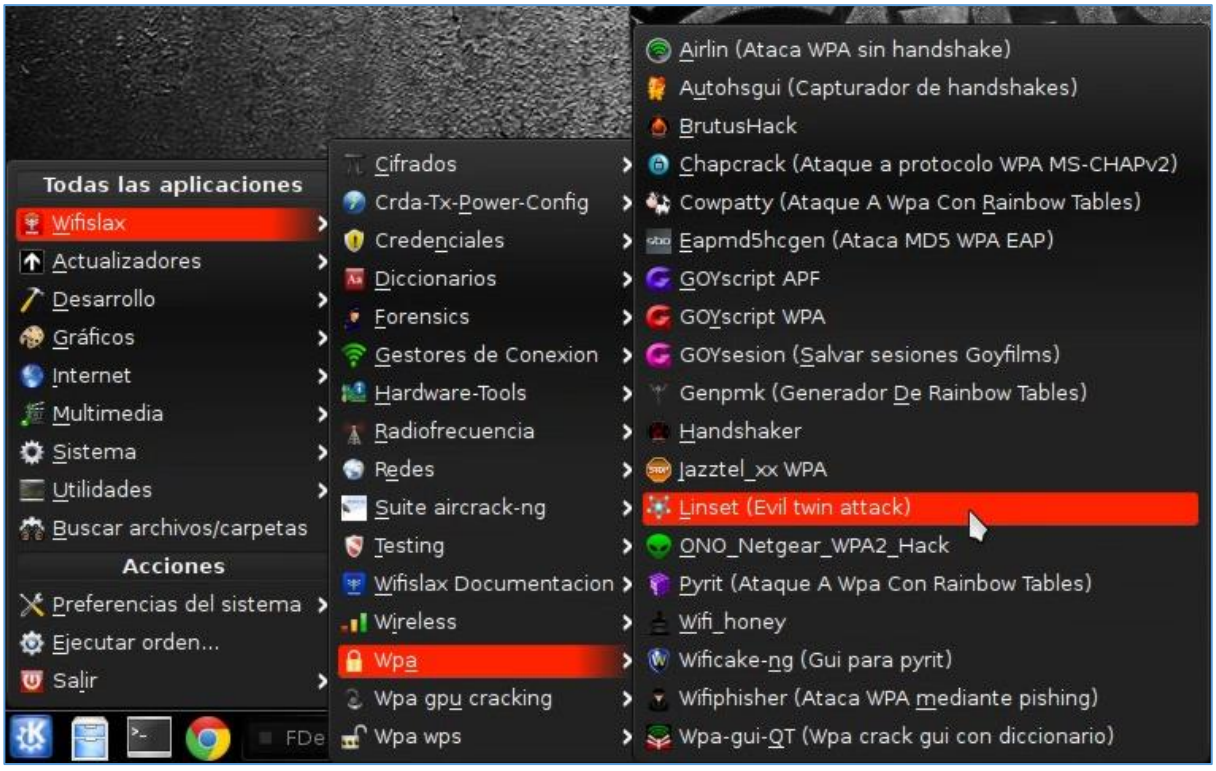
Este proceso es 100% responsabilidad del docente, pero en algunos casos no se está ejecutando, acrecentando el riesgo de que cualquier persona pueda ingresar al sistema y modificar la información empleando la ingeniería social.

7.5.4.1 Recomendaciones uso apropiado SAPRED. Emitir circular a todos los usuarios (docentes, administrativos y directivos) desde rectoría, con el ánimo de actualizar la contraseña de acceso a SAPRED, y verificar el cambio solicitado en la plataforma online.

Incluir la presente solicitud, de obligatorio cumplimiento por parte de todos los usuarios de SAPRED, en el manual de políticas de seguridad informática del colegio mixto san Felipe Neri.

7.5.5 *Hacking* ético a la *WLAN* del colegio mixto San Felipe Neri. Para identificar las vulnerabilidades en la red WLAN del colegio, se utiliza el software libre *WIFISLAX* distribución 4.11.1; seguidamente se accede a la aplicación *Linset*[10] (*Evil twin attack*). Con el fin de empezar el ataque a la WIFI CMIXTO_2017.

Figura 6. Acceso a *Linset* desde *WIFISLAX* 4.11.1



Fuente: el autor

[10] Aplicación para Linux que nos permite auditar o crackear una red Wi-Fi con el fin de comprobar la seguridad del Router y descifrar la clave de acceso fácilmente, sin necesidad de diccionarios de claves, creando una copia falsa de la red Wi-Fi que se esté atacando.

Después de cargar la aplicación, se procede a seleccionar la interface (tarjeta de red inalámbrica del PC atacante), para realizar el ataque con *WIFISLAX*.

Figura 7. Selección de interface

Fuente: el autor

Aparece la siguiente pantalla en donde se escoge la opción 1, con el fin de escanear todos los canales disponibles.

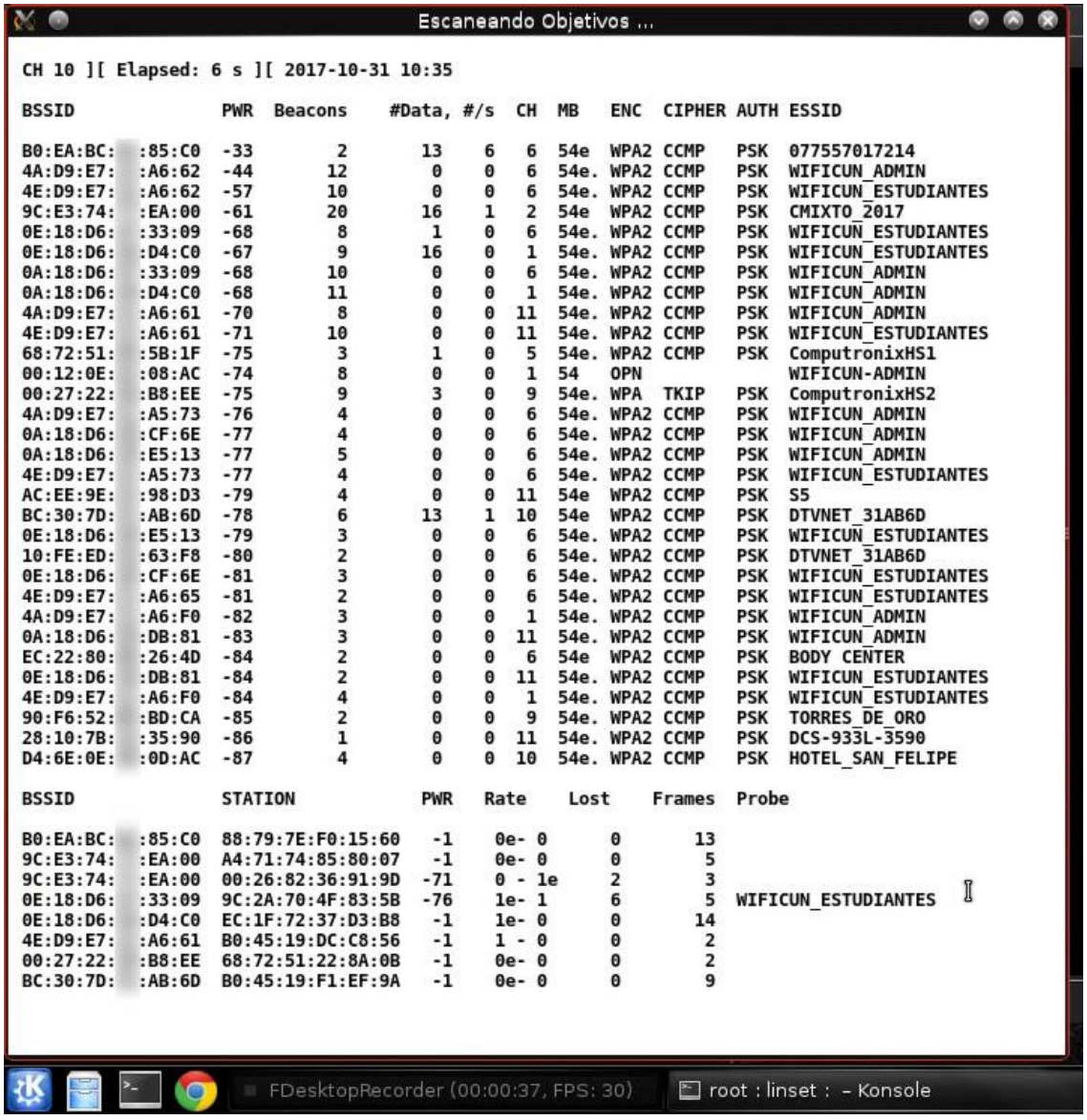
Figura 8. Selección de todos los canales

Fuente: el autor

El siguiente paso fue escanear los objetivos o redes inalámbricas disponibles en el entorno cercano al PC dispuesto para el ataque, por situaciones de seguridad se realizó desenfoque a la imagen en la sección de los *BSSID*[11].

[11] "identificación del set del servicio básico", toma sus valores en números binarios para indicar la información del dispositivo. http://www.quesignifica.org/bssid/

Figura 9. Escaneo de objetivos WIFI

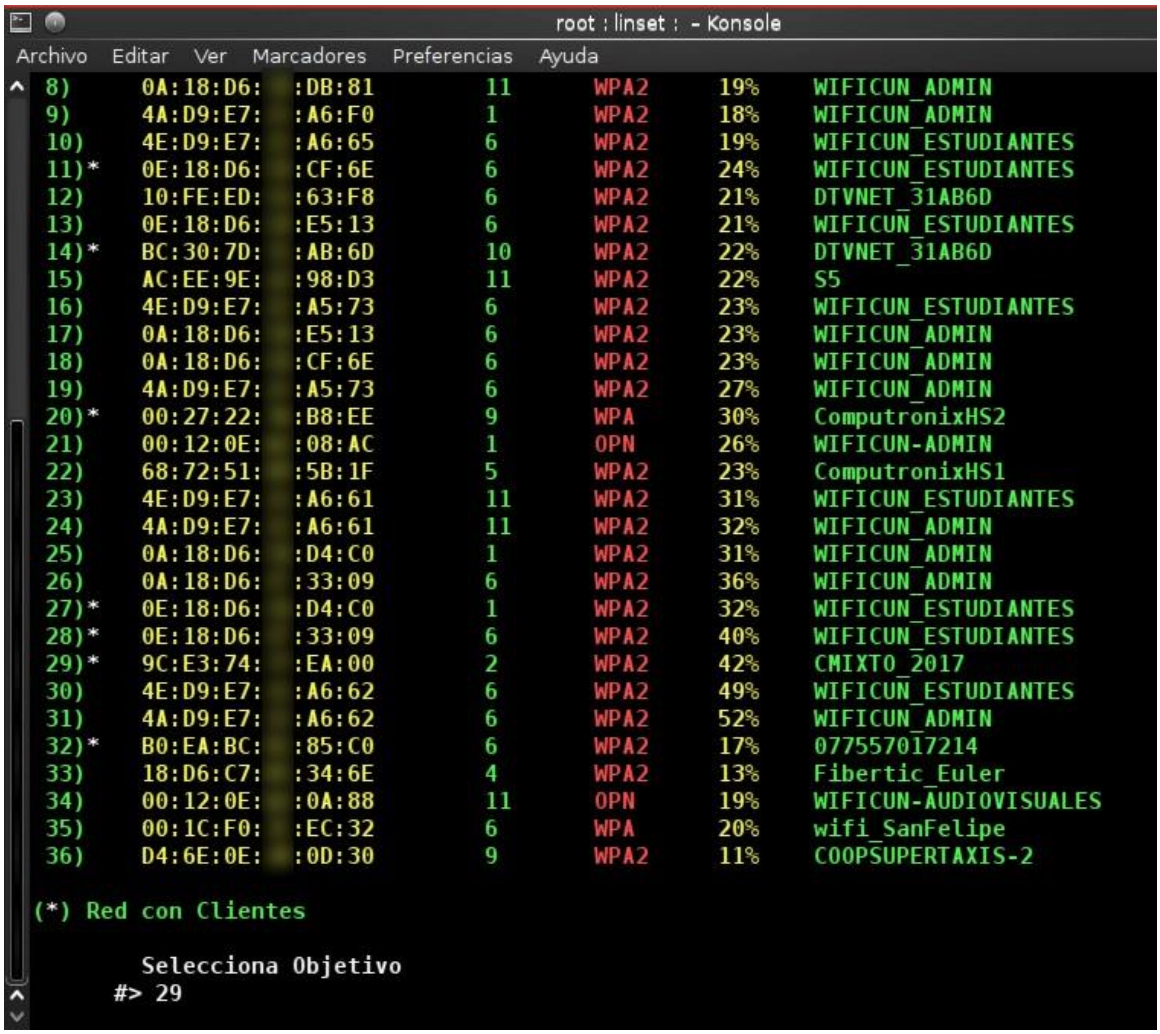


Fuente: el autor

Se procede a seleccionar la red CMIXTO_2017 que se desea atacar, para tal efecto debemos verificar que existen estaciones conectadas, se busca entonces el *BSSID* de la WIFI que vamos a atacar, relacionando las *MAC* de la columna *STATION* que identifican los dispositivos conectados, posteriormente cerramos la ventana.

Seguidamente aparece otra ventana con las redes escaneadas, aquí se logra identificar cuáles de ellas tienen usuarios conectados, gracias al asterisco que aparece al lado del número de red, se digita el número de la red escogida que en este caso se identificó con el número 29.

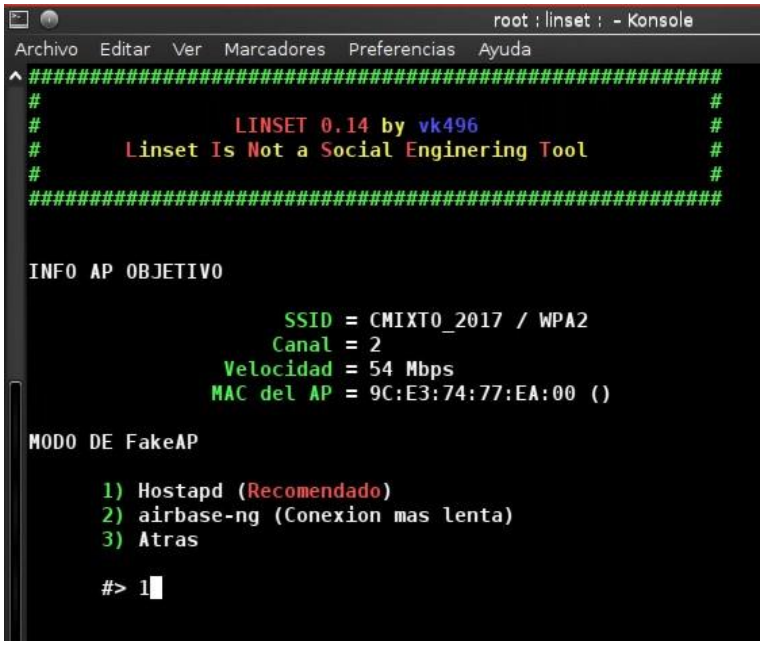
Figura 10. Redes escaneadas



Fuente el autor

Posteriormente aparece la siguiente ventana con la información del objetivo a atacar, aquí se escoge la opción 1 que indica *Hostapd*[12] (Recomendado).

Figura 11. Seleccionando *Hostapd*



Fuente: el autor

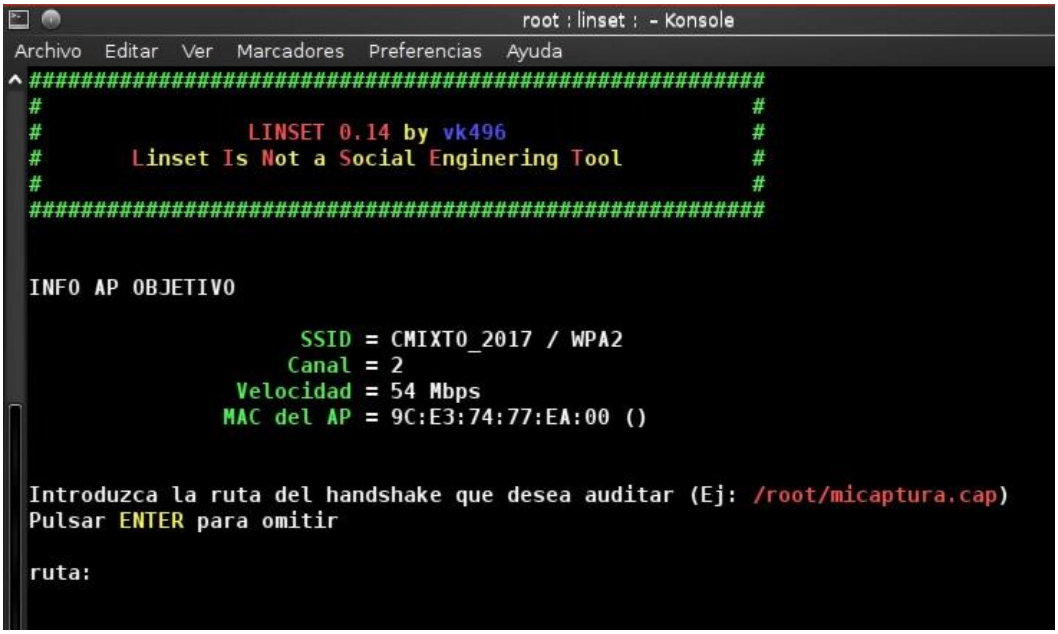
En la ventana que aparece únicamente se presiona la tecla *enter*, puesto que hasta este paso no tenemos la ruta del *handshake*[13] que deseamos auditar.

La figura siguiente muestra la información del dispositivo que se está atacando, especificando la *MAC* y el canal de comunicación.

[12] Permite crear puntos de acceso y servidores de autenticación WIFI totalmente configurables, haciendo uso de la tarjeta de red inalámbrica del atacante. http://foro.seguridadwireless.net/wireless-linux-wifi/hostapd-crea-aps-con-una-tarjeta-wireless/

[13] Hace referencia a un paquete de datos que solo se consigue des autenticando a un cliente legítimo de una red inalámbrica. https://www.s21sec.com/es/blog/2013/03/capturando-facilmente-un-handshake-wpa/

Figura 12. Información del objetivo de *hackeo*



Fuente: el autor

Figura 13. Iniciando la captura del *handshake*

Fuente: el autor

A continuación, aparece una ventana que nos permitirá capturar el *handshake* del cliente con el analizador de paquetes *aircrack*-ng[14], para ello se escoge la opción 1 y presionamos *Enter*.

Posteriormente aparece el siguiente menú, se selecciona la opción 1, que a partir de su ejecución permite realizar una des autenticación masiva de todos los usuarios conectados a la *WLAN* del colegio, situación que permaneció activa durante todo el tiempo que duró el ataque.

Figura 14. Des autenticando usuarios

Fuente: el autor

[14] crackeador de redes WEP y WPA/WPA2-PSK, http://www.seguridadwireless.net/hwagm/manual-aircrack-ng-castellano.html

A continuación, se captura el *handshake* y esto se logra conseguir gracias a la víctima, que al ser des autenticada pierde su conexión a INTERNET, seguidamente el dispositivo del usuario des autenticado intenta reconectarse y es aquí donde se obtiene la información necesaria y objetivo del ataque, en la figura siguiente se ha resaltado en color amarillo el *handshake*.

Figura 15. Captura de paquete de datos con handshake

Fuente: el autor

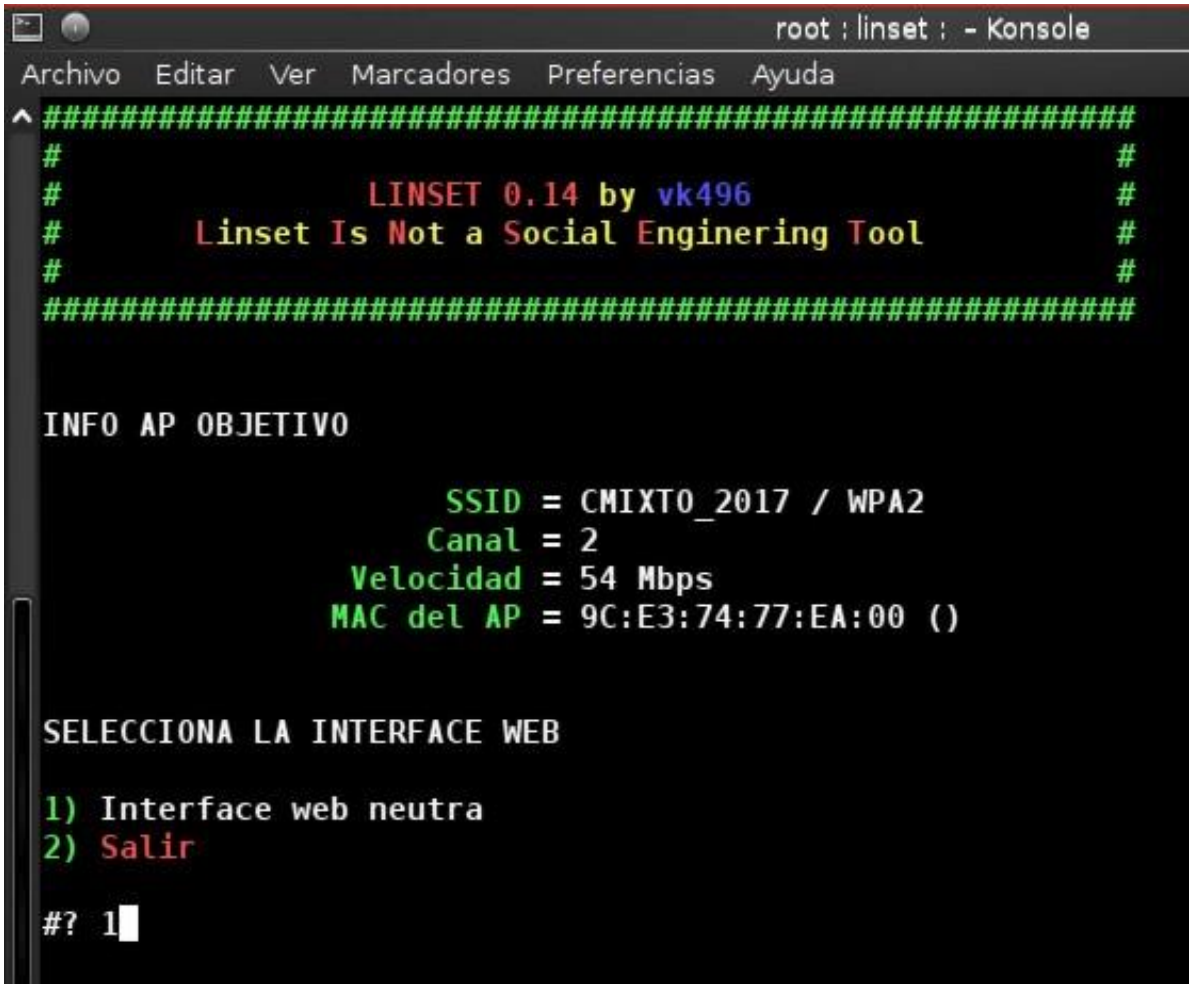
Habiendo conseguido el *handshake*, en la siguiente ventana se escoge la opción 1, que se identifica por la palabra “SI”, en el caso de no haber conseguido ningún resultado, se debe repetir el ataque seleccionando la opción 2.

Figura 16. Aceptando la captura del *Handshake*

Fuente: el autor

A continuación, en la ventana que aparece seleccionamos la interfaz web que le será mostrada a la víctima del hackeo en su PC o dispositivo móvil, dado que no existen más opciones se escoge la opción 1.

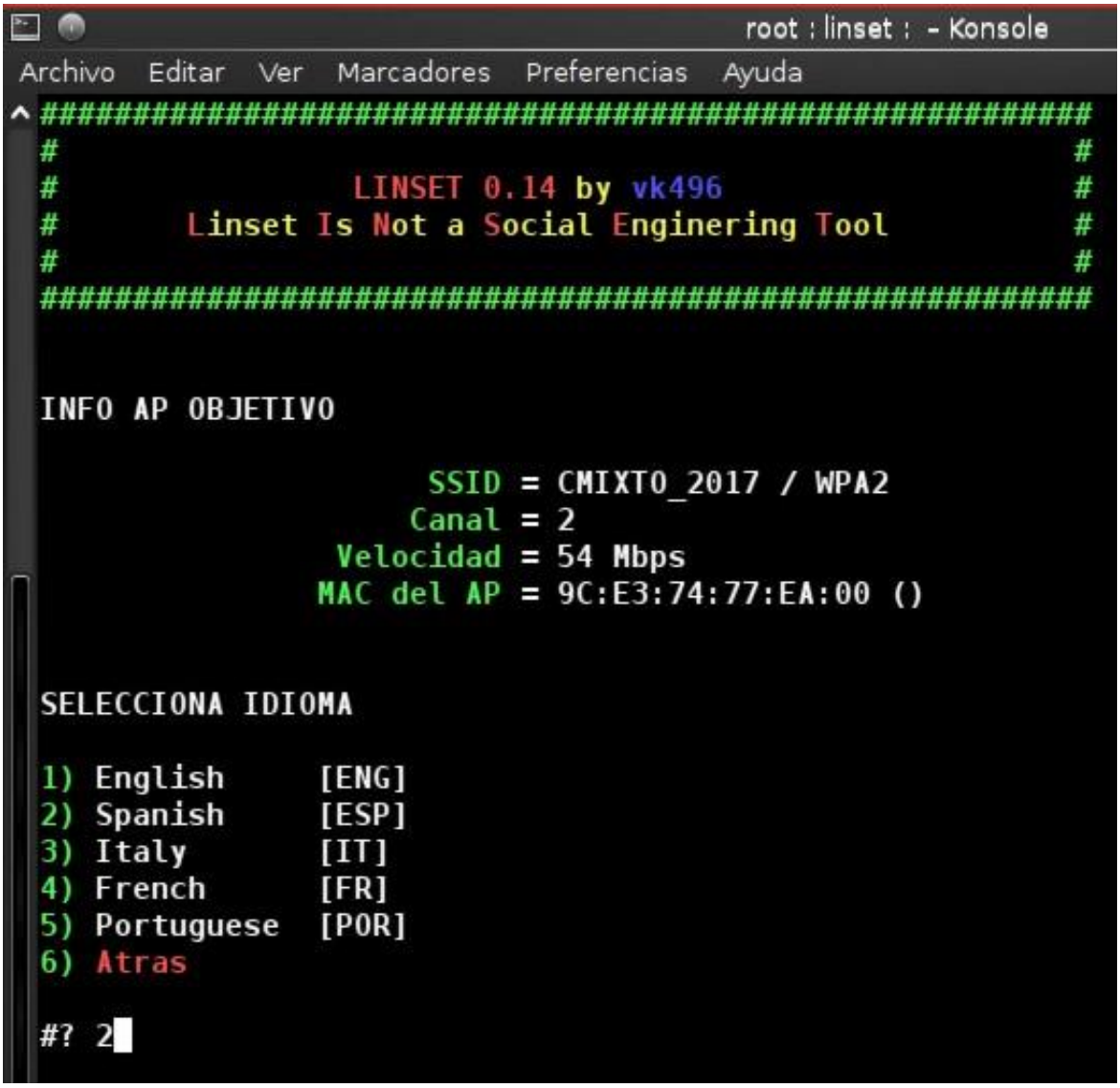
Figura 17. Selección de la interface *WEB*



Fuente: el autor

La siguiente ventana, permite escoger el idioma con el cual se le solicita la información a la víctima, por obvias razones se escoge la opción 2, en español.

Figura 18. Selección de idioma para captura de clave



Fuente: el autor

A continuación, aparecen 4 ventanas, la primera ventana que contiene texto en color verde es la encargada de enviar la interface *WEB* falsa, que solicitará a la víctima la clave de acceso WIFI. La segunda ventana con texto en color blanco estará contando los intentos erróneos que haya realizado la víctima hasta conseguir la

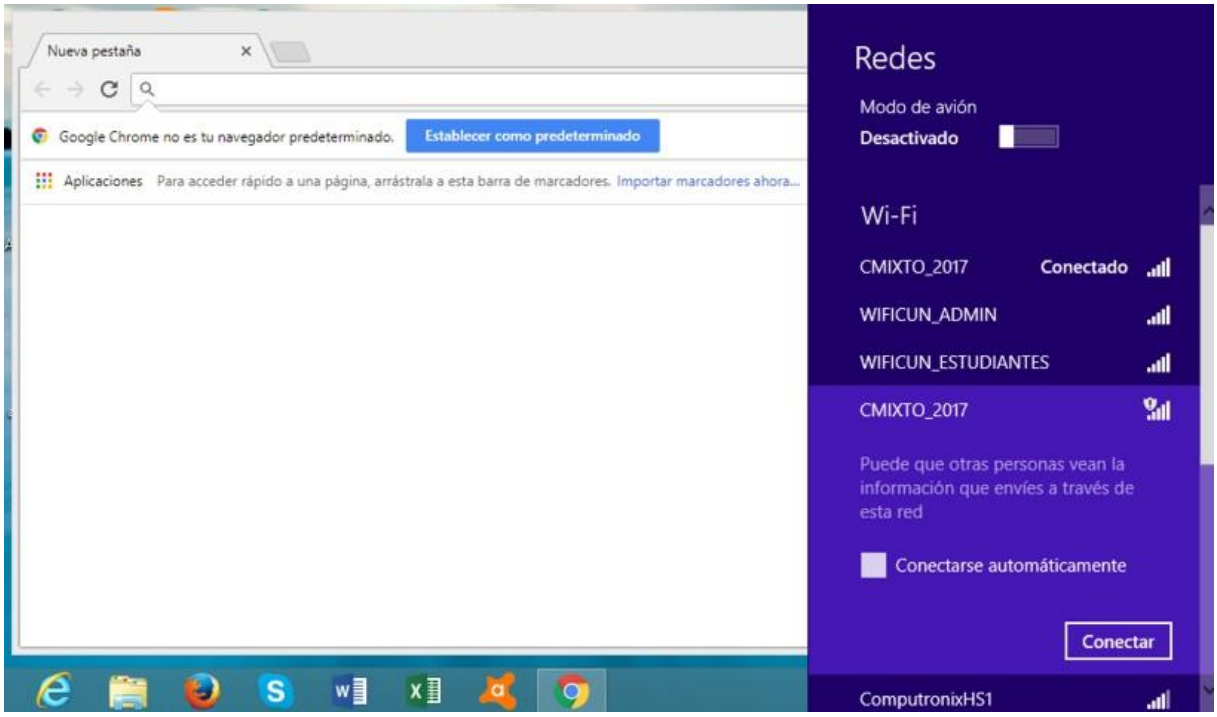
clave de acceso correcta, igualmente nos mostrará el tiempo que llevamos atacando la *WLAN*. La tercera ventana con texto en color azul, nos muestra los sitios *WEB* que la víctima está intentando acceder. La cuarta ventana con texto en color rojo indica el continuo ataque que se está ejecutando al Router de la *WLAN* y que está siendo atacada, efectuando la denegación de servicios, la herramienta *LINSET* se está encargando de evitar que los usuarios se puedan conectar a la red WIFI original. Mientras se esté llevando a cabo el ataque los usuarios no podrán acceder al servicio de INTERNET

Figura 19. Esperando que la víctima ingrese el password de la WIFI

Fuente: el autor

La figura 20 muestra la Información de la red WIFI clonada falsa; la persona que pierde su conexión a la INTERNET, intentará recuperar la conexión hacienda clic en el botón conectar.

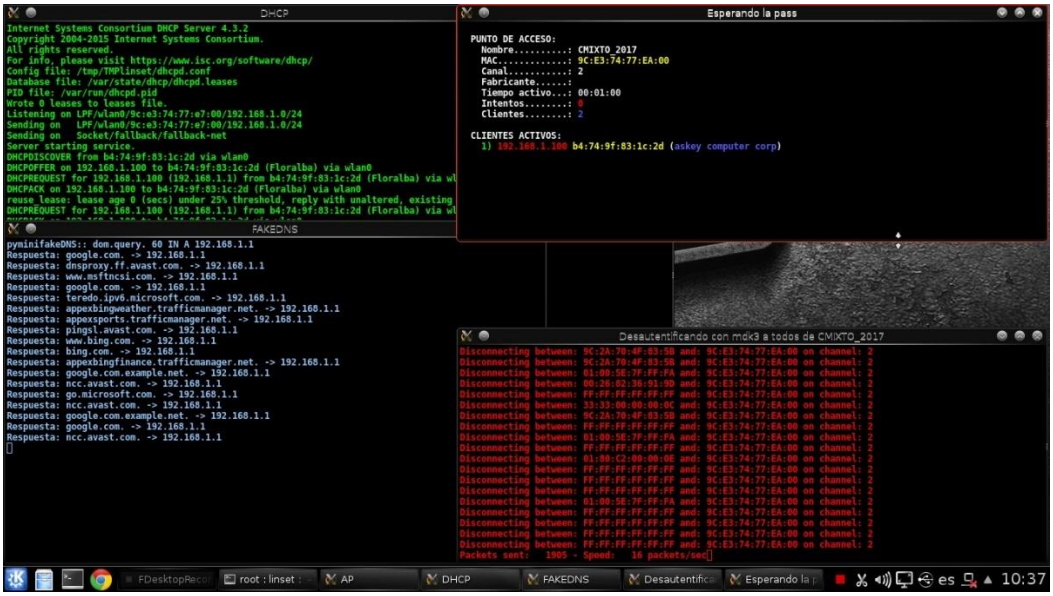
Figura 20. Pantalla del PC de la víctima conectando a la red falsa CMIXTO_2017



Fuente: el autor

La figura 21 muestra en la sección “esperando la *pass*” cuantos clientes se encuentran activos y que al mismo tiempo estarán experimentando la NO conexión a INTERNET.

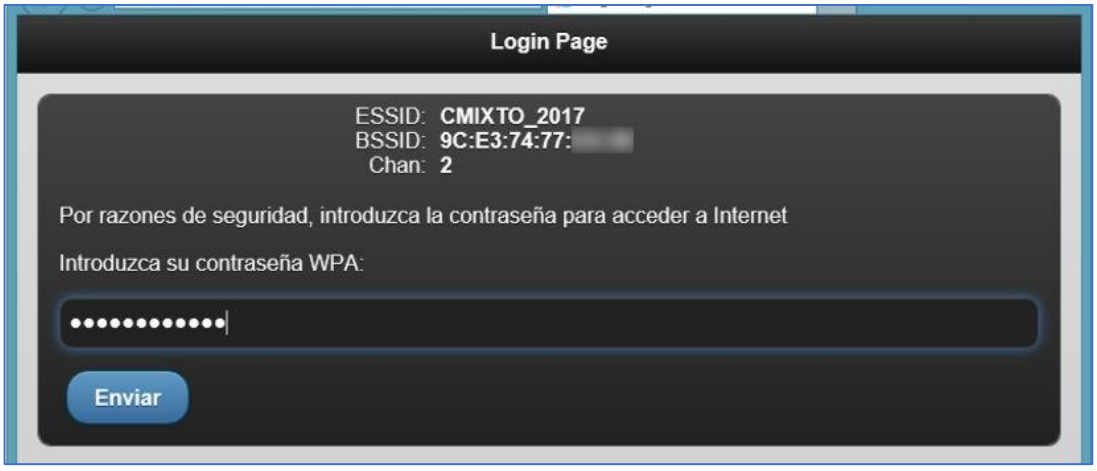
Figura 21. Verificando clientes activos en la WIFI atacada.



Fuente: el autor

La figura 22 permite verificar que la víctima ha caido en la trampa y procede a escribir la clave de acceso.

Figura 22. La víctima introduce la clave de acceso a la WIFI



Fuente: el autor

Figura 23. Captura exitosa del password visualizado en *WIFISLAX*

Fuente: el autor

La figura anterior muestra que se ha obtenido la clave buscada y que el ataque realizado arrojó los resultados esperados.

Cabe aclarar que durante todo el tiempo que duró el ataque para capturar la clave de acceso a la WIFI, CMIXTO_2017 los usuarios conectados inalámbricamente no tuvieron acceso a INTERNET.

8 DECLARACIÓN DE APLICABILIDAD

*S*e trata de un documento que enlista los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001.El **Anexo A** suele ser utilizado como una referencia para la implementación de medidas de protección de la información, así como para comprobar que no se están dejando de lado medidas de seguridad necesarias que no habían sido consideradas dentro de una organización.

Los propósitos que se desean alcanzar a través de la implementación de controles (es decir, objetivos de control), se encuentran incluidos de manera implícita en los controles seleccionados.

8.1 RAZONES DE LA APLICABILIDAD

- RL: Requerimiento Legal
- OC: Obligaciones contractuales
- RN/BP: Requerimiento de negocio/Mejores prácticas
- RAR: Resultado análisis de riesgos

Cuadro 15. Declaración de aplicabilidad

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
	5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN			
5.1 ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	5.1.1 DOCUMENTO DE POLÍTICA PARA LA SEGURIDAD DE LA INFORMACIÓN	SI	RAR	En el Colegio Mixto San Felipe Neri se pudo identificar los riesgos de información que allí existen, por eso es necesario establecer una política de seguridad de la información para divulgar y concientizar a todos los empleados y docentes de la entidad, e interesados sobre el riesgo a los que se encuentran expuestos, de igual forma darles a conocer los controles implementados, que van a permitir minimizar los riesgos. La política establecida debe tener claro los responsables del desarrollo e implementación
	5.1.2 REVISIÓN DE LAS POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	SI	RAR	La política de seguridad de la información del colegio deberá ser frecuentemente revisada para asegurar su idoneidad con respecto a los riesgos de información. Está política debe ser comunicada a todas las partes interesadas.
	6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
6.1 ORGANIZACIÓN INTERNA	6.1.1 ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN	SI	RN/BP	Mediante la política de seguridad de la información el colegio debe establecer un compromiso, organización y asignación de responsabilidades para su cumplimiento. También se tiene que asegurar que la información se encuentre protegida, por medio de: revisión del sistema de gestión de seguridad de la información, firmas de acuerdos de confidencialidad, mantener un contacto permanente con las autoridades y grupos de interés especiales, y realizar una revisión
	6.1.2 SEPARACIÓN DE DEBERES	SI	RN/BP	
	6.1.3 CONTACTO CON LAS AUTORIDADES	SI	RN/BP	

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
	6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL	SI	RN/BP	independiente de la seguridad de la información. Por eso es importante establecer controles para la organización interna de seguridad de la información
	6.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.	SI	RN/BP	
6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO	6.2.1 POLÍTICA PARA DISPOSITIVOS MÓVILES	SI	OC	El Colegio Mixto San Felipe Neri restringe la conexión a las redes inalámbricas de internet, por medio de claves o usuarios de red, a los dispositivos móviles y equipos de terceros
	B7 SEGURIDAD DE LOS RECURSOS HUMANOS			
7.1 ANTES DE ASUMIR EL EMPLEO	7.1.1 SELECCIÓN	SI	OC	En el colegio, cada año existe cambio de personal docente, los nuevos docentes deben tener acceso a la información del colegio, por tal motivo es importante implementar controles basados en reglamentos, la ética y las leyes vigentes, que permitan asegurar un proceso de verificación de antecedentes, asignación de roles y responsabilidades, términos de contratación y condiciones laborales antes de dar acceso a la información.
	7.1.2 TÉRMINOS Y CONDICIONES DEL EMPLEO	SI	RL	
7.2 DURANTE LA EJECUCIÓN DEL EMPLEO	7.2.1 RESPONSABILIDADES DE LA DIRECCIÓN	SI	OC	Las personas y docentes del colegio que fueron contratados, en función de sus actividades siempre tendrán acceso a la información, por tal motivo es necesario establecer controles que permitan concientizar a los empleados de los

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
	7.2.2 TOMA DE CONCIENCIA, EDUCACIÓN, Y FORMACIÓN EN S.I.	SI	RN/BP	riesgos, responsabilidades y deberes respecto a la seguridad de la información. También es necesario capacitar y concientizar al personal permanente en temas de seguridad de la información según sus funciones laborales. De igual forma es necesario establecer un proceso disciplinario que permita al colegio saber, que hacer en caso de que alguien logre violar la seguridad de la información. Para minimizar estos percances es necesario que la dirección exija al personal el cumplimiento de las reglas, políticas y procedimientos establecidos.
	7.2.3 PROCESO DISCIPLINARIO	SI	RL	
7.3 TERMINACIÓN Y CAMBIO DE EMPLEO	7.3.1 TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO	SI	OC	En el colegio se pueden presentar renuncias, terminaciones o cambios de la contratación del personal, por tal motivo se requiere tener un control que permita asegurar la devolución de los activos a cargo, de igual forma el cambio o retiro de los derechos de acceso cuando sea requerido según el caso.
	8 GESTION DE ACTIVOS			
8.1 RESPONSABILIDAD POR LOS ACTIVOS	8.1.1 INVENTARIO DE ACTIVOS	SI	RN/BP	En el proceso de implementación de medidas de seguridad, el colegio debe realizar un inventario de todos los activos de información, que permiten llevar a cabo el desarrollo de la actividad educativa. También es importante identificar los propietarios o usuarios de estos, se requiere que se pueda garantizar el uso adecuado de estos activos implementando reglas y su respectiva documentación.
	8.1.2 PROPIEDAD DE LOS ACTIVOS	SI	RN/BP	
	8.1.3 USO ACEPTABLE DE LOS ACTIVOS	SI	RN/BP	

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
	8.1.4 DEVOLUCIÓN DE LOS ACTIVOS	SI	RN/BP	Los activos del colegio, deberán ser devueltos por los empleados al finalizar cualquier relación laboral con el colegio. Este debe asegurar la devolución una vez se presenten renuncias, terminación o cambios de contratación que hacen parte del colegio.
8.2 CLASIFICACIÓN DE LA INFORMACIÓN	8.2.1 CLASIFICACIÓN DE LA INFORMACIÓN	SI	RN/BP	Dentro de las actividades del colegio, se tiene información de diferentes tipos de importancia y protección, hay información clasificada como secreta la cual debe tener un gran rango de protección, y existen otras que no requieren un nivel tan alto de protección debido a que todos los empleados pueden tener acceso, por tal motivo es necesario tener controles y procedimientos que permitan dar a la información el nivel adecuado de protección, etiquetado y manejo con base a la clasificación de información que se utilice, teniendo en cuenta para esto el valor, lo requisitos legales, la sensibilidad y la importancia para la entidad.
	8.2.2 ETIQUETADO DE LA INFORMACIÓN	SI	RAR	
	8.2.3 MANEJO DE ACTIVOS	SI	RN/BP	
8.3 MANEJO DE MEDIOS	8.3.1. GESTIÓN DE MEDIOS REMOVIBLES	SI	RN/BP	Para la entidad es necesario establecer controles que permitan evitar divulgación, modificación, retiro o destrucción de información no autorizada, esto se puede presentar en el intercambio de información como puede ser, correo electrónico, servicios de mensajería, USB, CD, etc.
	8.3.2 DISPOSICIÓN DE LOS MEDIOS	SI	RN/BP	
	8.3.3 TRANSFERENCIA DE MEDIOS FÍSICOS.	SI	RN/BP	
	9 CONTROL DE ACCESO			

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
9.1 REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESOS	9.1.1 POLÍTICA DE CONTROL DE ACCESO	SI	RN/BP	Es importante para el colegio establecer controles de seguridad que permitan certificar que los encargados de los activos de información, controlen efectivamente el acceso a la misma.
	9.1.2 ACCESO A REDES Y A SERVICIOS EN RED	SI	OC	Actualmente el Colegio cuenta con una red LAN y WLAN, las cuales soportan las actividades de los directivos, docentes, administrativos y estudiantes, por lo tanto, es necesario tener un control de seguridad que permita corroborar que los usuarios solo tengan acceso a los servicios que están autorizados.
9.2 GESTIÓN DE ACCESO DE USUARIOS	9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	SI	RN/BP	Los empleados del colegio manejan diferentes tipos de información, de acuerdo a la dependencia o proyecto desarrollado, por tal motivo es importante que el acceso de los usuarios a la información sea de acuerdo al área, proyecto o dependencia a la que pertenezcan. Por eso se requiere tener unos controles de seguridad que aseguren el acceso de usuarios autorizados, así como evitar el acceso de usuarios no autorizados a información fuera de área o proyecto.
	9.2.2 SUMINSITRO DE ACCESO DE USUARIOS	SI	RN/BP	
	9.2.3 GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO	SI	RN/BP	
	9.2.4 GESTIÓN DE LA INF. DE AUTENTICACIÓN SECRETA DE USUARIOS	SI	RN/BP	
	9.2.5 REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIOS	SI	RN/BP	

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
	9.2.6 RETIRO O AJUSTE DE LOS DERECHOS DE ACCESO.	SI	RN/BP	
9.3 RESPONSABILIDADES DE LOS USUARIOS	9.3.1 USO DE INFORMACIÓN DE AUTENTICACIÓN SECRETA	SI	OC	Todo el personal del colegio, tiene un control de acceso de autenticación a la red. Se requiere tener un control de seguridad que permita establecer la modalidad del acceso y generalidades de cambio de contraseñas para los usuarios.
9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	9.4.1 RESTRICCIÓN DE ACCESO A LA INFORMACIÓN	SI	OC	Todo el personal del colegio, tiene un control de acceso de autenticación a la red. Esto afecta tanto al acceso al sistema operativo de estaciones de trabajo como de servidores, así como los entornos de desarrollo y las aplicaciones desarrolladas para los clientes cuando se encuentran en fase de pruebas. Se requiere tener un control de seguridad que permita establecer la modalidad del acceso y generalidades de cambio de contraseñas para los usuarios.
	9.4.2 PROCEDIMIENTO DE INGRESO SEGURO.	SI	OC	
	9.4.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS.	SI	OC	
	9.4.4 USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS.	SI	RN/BP	
	9.4.5 CONTROL DE ACCESO A CODIGOS FUENTE DE PROGRAMAS.	SI	OC	
	10 CRIPTOGRAFIA			
10.1 CONTROLES CRIPTOGRAFICOS	10.1.1 POLÍTICA SOBRE USO DE CONTROLES CRIPTOGRÁFICOS	SI	RN/BP	Debido a la diferente información que se maneja en el colegio, es necesario establecer controles criptográficos, para así poder garantizar la confidencialidad e integridad de la información.
	10.1.2 GESTIÓN DE LLAVES	SI	RN/BP	

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
	11 SEGURIDAD Física Y DEL ENTORNO			
11.1 ÁREAS SEGURAS	11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA	SI	OC	El Colegio dispone un rack de comunicaciones para el laboratorio de informática, sistemas de extinción de incendios, dispositivos de suministro eléctrico UPS individuales ininterrumpido con capacidad para 15 minutos, El acceso a las instalaciones del colegio se encuentra controlados por una recepción presente desde las 6:00 a.m. hasta las 9:30 p.m. Es importante establecer controles de seguridad para evitar el acceso físico no autorizado, y el posible daño a la infraestructura y demás activos de información del colegio.
	11.1.2 CONTROLES DE ACCESO FÍSICOS	SI	OC	
	11.1.3 SEGURIDAD DE OFICINAS, RECINTOS E INSTALACIONES	SI	OC	
	11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES	SI	OC	
	11.1.5 TRABAJO EN ÁREAS SEGURAS	SI	OC	
	11.1.6 ÁREAS DE DESPACHO Y CARGA	NO	-	En el colegio no se cuenta con áreas de despacho o carga, por tal motivo no se requiere establecer esta política de seguridad.
11.2 EQUIPOS	11.2.1 UBICACIÓN Y PROTECCION DE LOS EQUIPOS	SI	RN/BP	En el día a día del colegio, se usan los equipos como: PCs del laboratorio de informática, computadores de Coordinación, secretaría, psicología,

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
	11.2.2 SERVICIOS DE SUMINSITRO	SI	RN/BP	tesorería, rectoría, entre otros. En estos equipos se procesa la información de todas las dependencias del colegio, por tal motivo se requiere implementar un control que permita evitar la pérdida, robo, daño de los equipos tanto dentro y fuera del colegio.
	11.2.3 SEGURIDAD EN EL CABLEADO		RN/BP	
	11.2.4 MANTENIMIENTO DE EQUIPOS	SI	RN/BP	
	11.2.5 RETIRO DE ACTIVOS	SI	RN/BP	
	11.2.6 SEGURIDAD DE EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES	SI	RN/BP	
	11.2.7 DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS	SI	RN/BP	
	11.2.8 EQUIPOS DE USUARIO DESATENDIDO	SI	RN/BP	Los empleados del colegio a cargo de los activos, deben asegurar que los equipos no supervisados cuentan con la protección adecuada. Para que así se mantenga la confidencialidad, integridad y disponibilidad de la información

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
	11.2.9 POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA.	SI	RN/BP	Se debe adoptar una política de puesto de trabajo limpio que permita tener despejado el puesto de trabajo de documentación y objetos. Es necesario que en esos controles se exijan informes de revisiones periódicas a los equipos, incluyendo actividades para la revisión de rendimiento, capacidad, eventos de seguridad y limpieza de los diversos componentes (aplicaciones, almacenamiento, CPU, memoria, red, etc.).
	12 SEGURIDAD DE LAS OPERACIONES			
12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	12.1.1 PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS	SI	RN/BP	En el colegio se debe tener controles de seguridad que garanticen que los cambios se controlen, revisan y se someten a pruebas, permitiendo determinar que no comprometan la seguridad del sistema, ni el entorno operativo, evitando que la información se filtre, esto debido a que el personal del colegio utiliza herramientas de ofimática y tecnológicas, con las que interactúa constantemente a través de los equipos asignados a cada persona.
	12.1.2 GESTIÓN DE CAMBIOS	SI	RN/BP	
	12.1.3 GESTIÓN DE CAPACIDAD	SI	RN/BP	
	12.1.4 SEPARACION DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y OPERACIÓN.	No	OC	El colegio no tiene implementado ningún tipo de prueba de aplicaciones por lo tanto no se hace necesario implementar esta política de seguridad.

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
12.2 PROTECCION CONTRA CODIGOS MALICIOSOS	12.2.1 CONTROLES CONTRA CÓDIGOS MALICIOSOS	SI	RAR	Los equipos de los usuarios del colegio, usan servicios como INTERNET, medios extraíbles, entre otros. Los cuales puede llegar afectar el funcionamiento del hardware, software, por lo tanto, es necesario determinar controles de seguridad que permitan detección y prevención de códigos maliciosos, también es necesario alternativas de concientización de los usuarios.
12.3 COPIAS DE RESPALDO	12.3.1 RESPALDO DE LA INFORMACIÓN	SI	RN/BP	Para el colegio, es muy importante la información que se encuentran en los equipos de cómputo de los docentes y los jefes de dependencias. En este sentido es importante establecer controles de seguridad que aseguren la ejecución de procedimientos de Backups y recuperación, que permitan restaurar en el menor tiempo la información ante la materialización de un riesgo, y así permitir que la empresa continué con sus actividades habituales sin ningún inconveniente.
12.4 REGISTRO Y SEGUIMIENTO	12.4.1 REGISTRO DE EVENTOS	SI	RN/BP	Para el colegio es importante establecer controles de seguridad que permitan la detección oportuna de actividades de procesamiento de información no autorizadas y herramientas para investigaciones futuras de incidentes de seguridad de la información. Esto debido a que los docentes tienen acceso a los diferentes activos de la información en la ejecución de las actividades propias de su cargo.
	12.4.2 PROTECCIÓN DE LA INFORMACIÓN DE REGISTRO	SI	RAR	
	12.4.3 REGISTROS DEL ADMINSITRADOR Y DEL OPERADOR	SI	RN/BP	
	12.4.4 SINCRONIZACIÓN DE RELOJES	SI	RN/BP	

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
12.5 CONTROL DE SOFTWARE OPERACIONAL	12.5.1 INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS	SI	OC	Los sistemas operativos que usa el colegio van desde Windows XP, Windows 7, Windows 8.0, Windows 8.1 y Windows 10, algunos de ellos disponen de licencia en regla y configurados para descargar las actualizaciones. Es importante establecer controles de seguridad para garantizar la protección, control y correcta operación de los sistemas operativos. De igual forma para los equipos asignados a los usuarios formales del colegio se restringe la posibilidad de instalación de software
12.6 GESTION DE LA VULNERABILIDAD TÉCNICA	12.6.1 GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS	SI	RN/BP	Los activos del colegio, están expuestos a vulnerabilidades de tipo técnico, por tal motivo es necesario implementar controles de seguridad para minimizar los riesgos derivados de las vulnerabilidades técnicas.
	12.6.2 RESTRICCIÓN SOBRE LA INSTALACION DE SOFWARE	SI	RAR	El colegio usa diversas versiones de Windows como sistema operativo para sus PCs, es importante establecer controles de seguridad para garantizar la protección, control y correcta operación de los sistemas operativos.
12.7 CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	12.7 CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	SI	RAR	El sistema SAPRED, propiedad de S.I.T.I. Ltda, asume la responsabilidad de auditar y garantizar el perfecto funcionamiento de los procesos de gestión académica procesados en la plataforma online contratada por el colegio.

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
				Las demás auditorías de los sistemas de información del colegio, deben ser acordadas, planeadas y controladas con el objetivo de no interferir en el desarrollo normal de los procesos y así obtener los hallazgos y las no conformidades más relevantes que permitan proponer oportunidades de mejoramiento.
	13 SEGURIDAD DE LAS COMUNICACIONES			
13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES	13.1.1 CONTROLES DE REDES	SI	OC	El Colegio cuenta con redes LAN, WLAN, en ellas se ejercen procesos de distribución, modificación y eliminación de archivos por lo anterior es importante establecer controles de seguridad para asegurar la información en la red, protegerla de amenazas y garantizar su infraestructura de soporte.
	13.1.2 SEGURIDAD DE LOS SERVICIOS DE RED	SI	OC	
	13.1.3 SEPARACIÓN EN LAS REDES	SI	OC	El colegio cuenta con dos (2) Redes LAN y una (1) WLAN, por lo tanto, es necesario implementar un control de seguridad que permita separar las redes en función de los grupos de servicios, usuarios y sistemas de información.
13.2 TRANSFERENCIA DE INFORMACIÓN	13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE TRASNFERENCIA DE INFORMACIÓN	SI	RN/BP	En el colegio se presentan actividades de intercambio de información con terceras personas como pueden ser estudiantes, padres de familia, etc. Como parte del desarrollo de las actividades de cada una de las dependencias, por lo cual es importante

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
	13.2.2 ACUERDOS SOBRE TRASNFERENCIA DE INFORMACIÓN	SI	RN/BP	establecer controles de seguridad para asegurar que se cumplen las políticas y procedimientos del colegio para el intercambio de información para así garantizar que no se le dé un uso inadecuado a la información que sale de la institución educativa.
	13.2.3 MENSAJERIA ELECTRÓNICA	SI	RN/BP	
	13.2.4 ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN	SI	RL	Mediante una política de seguridad, el colegio debe establecer el compromiso, organización y asignación de responsabilidades para su cumplimiento, de igual forma debe velar por mantener protegido los activos de información mediante la revisión periódica, la firma de los acuerdos de confidencialidad, manteniendo contacto con las autoridades y con grupos de interés especiales, y la revisión independiente de seguridad de la información, por lo anterior es importante establecer controles para la organización interna de seguridad de la información.
	14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS			
14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	14.1.1 ÁNALISIS Y ESPECIFICACIÓN DE REQUISITOS DE SI	SI	RN/BP	El colegio utiliza herramientas ofimáticas y tecnológicas para agrupar y consolidar la información académica y financiera, por lo tanto, se hace necesario establecer controles de seguridad para garantizar que se tienen en cuenta los requisitos básicos del funcionamiento del software, antes de implementar cambios en las aplicaciones de software del colegio.
	14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONE	SI	RN/BP	

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
	S EN REDES PÚBLICAS			
	14.1.3 PROTECCIÓN DE TRANSACCIO N POR REDES TELEMATICAS	NO	RN/BP	El colegio desarrolla* actividades de servicios a través de diferentes aplicaciones, por lo cual es necesario aplicar los controles de seguridad tales como llaves o encriptación para los sistemas de información de las dependencias, para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción.
14.2 CONTROL DE ACCESO AL SISTEMA OPERATIVO	14.2.1 POLÍTICA DE DESARROLLO SEGURO	SI	RL	En el colegio es necesario establecer controles de seguridad para la salvaguarda de los sistemas de información accedidos por terceros, que permitan garantizar que cumplen con las características técnicas y de seguridad que se requiere.
	14.2.2 PROCEDIMIE NTO DE CONTROL DE CAMBIOS EN SISTEMAS	SI	RN/BP	Se debe adoptar controles que en el ciclo de vida de desarrollo permitan hacer uso de procedimientos formales de control de cambios.
	14.2.3 REVISIÓN TÉCNICAS DE LAS APLICACIONE S DESPUES DE CAMBIOS EN LA PLATAFORMA	NO	-	No es necesario este control, debido a que no afecta el proceso de desarrollo en el negocio del colegio

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
	14.2.4 RESTRICCIONES EN LOS CAMBIOS A LOS PAQUETES DE SOFTWARE	NO	-	
	14.2.5 DESARROLLO CONTRATADO EXTERNAMENTE	SI	RN/BP	En el colegio se debe establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información.
	14.2.8 PRUEBAS DE SEGURIDAD DE SISTEMAS	SI	RN/BP	Debido a que el colegio administra información académica y financiera de sistemas de información específicos. Debido a esto debe establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema. También aplica tener monitoreo y supervisión a las actividades de desarrollo por terceros. Es indispensable tener control sobre las pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.
	14.2.9 PRUEBAS DE ACEPTACIÓN DE SISTEMAS	SI	RN/BP	Se debe validar los nuevos sistemas de información en un computador de prueba, antes de ser implementados de forma real. Además, está establecido en la política de desarrollo por terceros los criterios y pruebas de aceptación para los nuevos sistemas de información que adquiera el colegio.
	15 RELACIONES CON LOS PROVEEDORES			

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
15.1 RELACIONES CON LOS PROVEEDORES	15.1.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES	SI	-	Es necesario este control, debido a que se contratan firmas externas para la evaluación académica de estudiantes mediante la aplicación de simulacros, se compran implementos para los laboratorios de química, informática e inglés.
	15.1.2 TRATAMIENTO DE LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES	SI	-	
	15.1.3 CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN	SI	RN/BP	El colegio en algún momento dado, tendrá la necesidad de realizar una actualización o adquisición de nuevos suministros tecnológicos, por tal motivo es importante tener un control que permita tener acuerdos con los proveedores, los cuales deberían incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.
15.2 GESTIÓN DE LA PRESENTACIÓN DE SERVICIOS DE PROVEEDORES	15.2.1 SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE LOS PROVEEDORES	SI	RN/BP	El colegio requiere realizar diferentes tipos de compras, debido a esto es necesario establecer controles de seguridad para garantizar que tienen en cuenta las necesidades prioritarias antes de gestionar compras de bienes o servicios que puedan afectar en la

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
	15.2.2 GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES	SI	RN/BP	seguridad de la información de la institución.
	16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION			
16.1 GESTION DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	SI	RN/BP	Mediante la política de seguridad de la información del colegio, se debe establecer un compromiso con la organización y asignación de responsabilidades para su cumplimiento. Se debe asegurar que la información se encuentre protegida, por medio de: revisión del sistema de gestión de seguridad de la información, firmas de acuerdos de confidencialidad, mantener un contacto permanente con las autoridades y grupos de interés especiales, y realizar una revisión independiente de la seguridad de la información.
	16.1.2 REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN	SI	RN/BP	En el colegio se clasificó un grupo de activos de información a los que se les ha realizado su respectivo análisis, evaluación y tratamiento del riesgo, los cuales pueden ser objeto de incidentes de seguridad de la información, por tanto es importante establecer controles que aseguren que los eventos y debilidades de seguridad de la información son comunicados oportunamente a través de los canales de gestión apropiados al área de seguridad de la información para su respectiva gestión tan pronto como sea posible.
	16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	SI	RN/BP	

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
	16.1.4 EVALUACIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y DECISIONES SOBRE ELLOS	SI	RN/BP	
	16.1.5 RESPUESTA A INCIDENTES DE SEGUIRIDAD DE LA INFORMACIÓN	SI	RN/BP	En el colegio se clasificó los activos de información, los cuales pueden ser objeto de incidentes de seguridad de la información y deben ser analizados por el personal designado por la administración para identificar acciones de mejora, en tal sentido es necesario establecer controles de seguridad para garantizar un manejo eficaz y consistente de los incidentes de seguridad de la información.
	16.1.6 APRENDIZAJE OBTENIDO DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	SI	RN/BP	
	16.1.7 RECOLECCIÓN DE EVIDENCIA	SI	RN/BP	
	17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DE NEGOCIO			
17.1 CONTINUIDAD EN SEGURIDAD DE LA INFORMACIÓN	17.1.1 PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA	SI	RN/BP	El colegio ante los padres de familia y estudiantes que hacen las veces de clientes está comprometido a garantizar el cumplimiento de los objetos de los contratos del servicio educativo, por eso ante cualquier complicación en las actividades del desarrollo del servicio

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
	INFORMACIÓN			por fallas tecnológicas importantes o desastres, la entidad debe tener una gestión de continuidad del servicio que permita minimizar el impacto generado por dicha interrupción, por lo anterior es necesario establecer controles para asegurar una adecuada gestión de continuidad del servicio educativo.
	17.1.2 IMPLEMENTACIÓN DE LA CONTINUIDAD DE LA SI	SI	RN/BP	
	17.1.3 VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SI	SI	RN/BP	
17.2 REDUNDANCIAS	17.2.1 DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN	SI	RN/BP	El colegio cuenta con 2 discos duros externos, para almacenar la información de respaldo, principalmente de los procesos académicos y financieros de la institución.
	18 CUMPLIMIENTO			
18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES.	SI	RL	El comité de seguridad informática apoyado en el SGSI garantizará la limitación de los privilegios de instalación de software a los usuarios de las diferentes dependencias, verificando la utilización de software licenciado y la instalación de distribuciones del software libre cuando así se requiera, en el marco del cumplimiento de la legislación colombiana, respecto de los requisitos contractuales en la utilización del software.
	18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL	SI	RL	
	18.1.3 PROTECCIÓN DE REGISTROS	SI	RL	

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
	18.1.4 PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE DATOS PERSONALES	SI	RL	
	18.1.5 REGLAMENTACIÓN DE CONTROLES CRIPTOGRÁFICOS	SI	RL	El colegio en los sistemas de información que desarrolla en las diferentes dependencias, debe establecer controles criptográficos con el objetivo principal de garantizar la confidencialidad e integridad de la información.
18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN	18.2.1 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN	SI	RN/BP	Mediante la política de seguridad de la información el colegio debe establecer un compromiso, organización y asignación de responsabilidades para su cumplimiento. También se debe asegurar que la información se encuentre protegida, por medio de: revisión del sistema de gestión de seguridad de la información, firmas de acuerdos de confidencialidad, mantener un contacto permanente con las autoridades y grupos de interés especiales, y realizar una revisión independiente de la seguridad de la información. Es importante establecer controles para la organización interna de seguridad de la información
	18.2.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	SI	RL	Los empleados del colegio, están en permanentemente contacto con los activos de información para los cuales se han diseñado políticas y controles en materia de seguridad de la información, en tal sentido es importante establecer controles de seguridad que garanticen que todo el personal del colegio conozca y aplique las

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	RAZÓN	JUSTIFICACIÓN
				políticas de seguridad de la información y los respectivos controles.

Fuente: el autor

9 SEGURIDAD BÁSICA APLICADA AL ROUTER

9.1 RECOPILACIÓN DE DIRECCIONES MAC

Ante la necesidad de proteger el acceso a la WIFI del colegio, se recopila la información pertinente de los dispositivos móviles que se conectan al Router, con el fin de aplicar la denegación de servicios a aquellos no relacionados en el formato de información MAC de dispositivos móviles del Colegio Mixto San Felipe Neri de Ipiales.

Cuadro 16. Información MAC Dispositivos Móviles

<table>
<tr><th colspan="7">INFORMACIÓN MAC DISPOSITIVOS MÓVILES</th></tr>
<tr><td colspan="2">Nombre Del Proceso</td><td colspan="5">Registro de direcciones MAC</td></tr>
<tr><td colspan="2">Líder responsable del Proceso</td><td colspan="5">Ing. Pablo Velásquez</td></tr>
<tr><td colspan="2">Dependencia Responsable</td><td colspan="5">Comité de seguridad informática</td></tr>
<tr><td colspan="2">Fecha inicio requerimiento de información:</td><td>Septiembre 18 de 2017</td><td colspan="2">Fecha finalización.</td><td colspan="2"></td></tr>
<tr><td rowspan="2">Nombre del empleado</td><td rowspan="2">Dependencia</td><td rowspan="2">Descripción del dispositivo</td><td rowspan="2">. Dirección MAC</td><td colspan="3">Acceso WIFI</td></tr>
<tr><td>Denegado</td><td>Aplazado</td><td>Aprobado</td></tr>
</table>

Presbítero Edgar Juez	Parroquia	PC	90:97:F3:XX:80:08			X
Pablo Velásquez	Rectoría	PC	4C:0F:6E:XX:E1:AA			X
Pablo Velásquez	Rectoría	Celular	CC:A2:23:XX:5A:2E			X
Sandra Yandún	Ciencias	PC	78:C3:E9:XX:10:78			X
Sandra Yandún	Ciencias	Celular	00:53:49:XX:D1:2A			X
William Chaves	Ciencias	pc	44:D4:E0:XX:2B:89			X
Víctor Obando	Coordinación	PC personal	C4:54:44:XX:AE:1C			X
Víctor Obando	Coordinación	Celular	9C:2A:70:XX:83:5B			X
Víctor Obando	Coordinación	Celular	A4:71:74:XX:80:07			X
Nancy Coral	Psicología	PC	14:1F:78:XX:FA:BA			X
Oswaldo Varela	Laboratorio Inglés	PC	18:CF:5E:XX:E4:41			X
Oswaldo Varela	Laboratorio Inglés	Celular	84:DB:AC:XX:9F:A9			X
Doris Mejía	Secretaría	Celular	00:87:01:XX:61:42			X
Doris Mejía	Secretaría	PC	00:26:82:XX:91:9D			X
Cristina Meza	Contabilidad	Celular	04:4F:4C:XX:27:F7			X
Elaborado por:		Pablo Velásquez	Firma Responsable.			
Cargo:						
Lugar y Fecha:						

Fuente: el autor

9.2 MEDIDAS DE SEGURIDAD BÁSICAS PARA PROTEGER EL ROUTER DEL CMSFN

Para evitar la conexión de personas no autorizadas al *Router* de la institución, se procede a realizar un bloqueo por direcciones *MAC*.

Accedemos desde cualquier navegador digitando la dirección IP 192.168.100.1 y posteriormente digitamos la información correspondiente al *ACCOUNT* o usuario y la clave o *password* requerida.

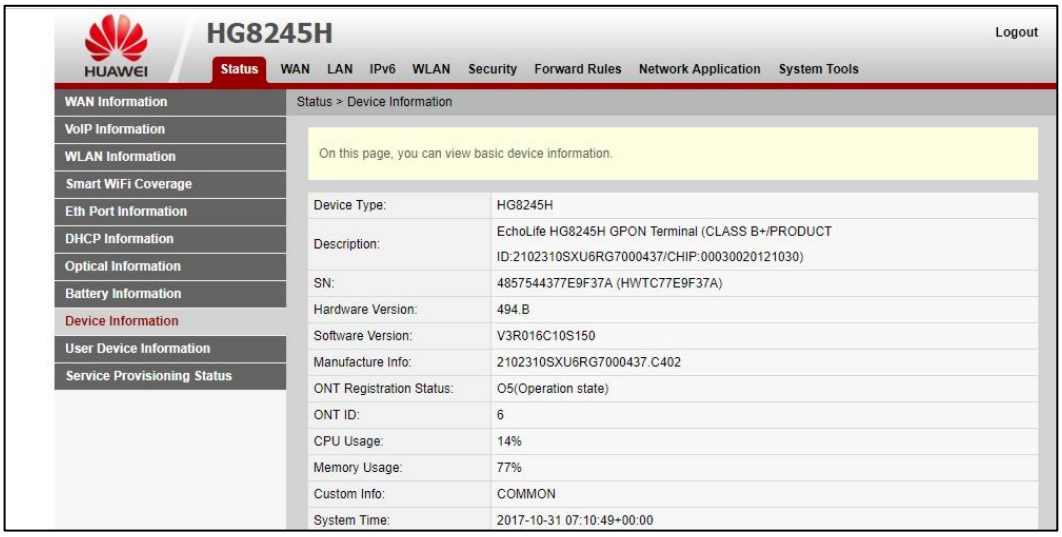
Figura 24. Accediendo al *Router*

Fuente: el autor

Seguidamente en la figura 25 podremos observar que se ha accedido a la configuración del Router y que desde aquí podremos realizar las respectivas

modificaciones para proteger las conexiones inalámbricas de personas no autorizadas.

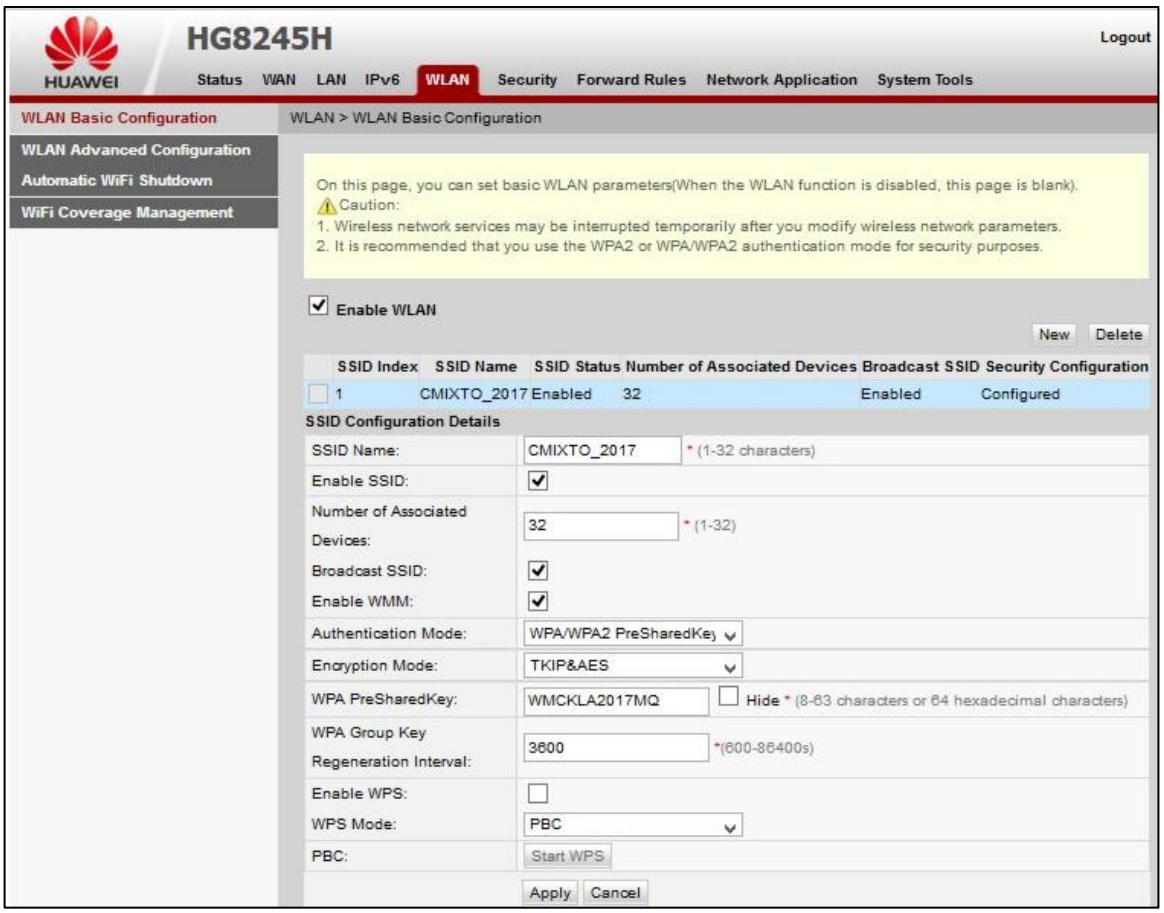
Figura 25. Información del *Router*



Fuente: el autor

En la figura 26 podemos verificar la clave de acceso actual de conexión WIFI, misma que puede ser cambiada por el administrador de la red y de esta manera obligar a los intrusos que ya conocían la clave anterior a intentar averiguar la nueva contraseña.

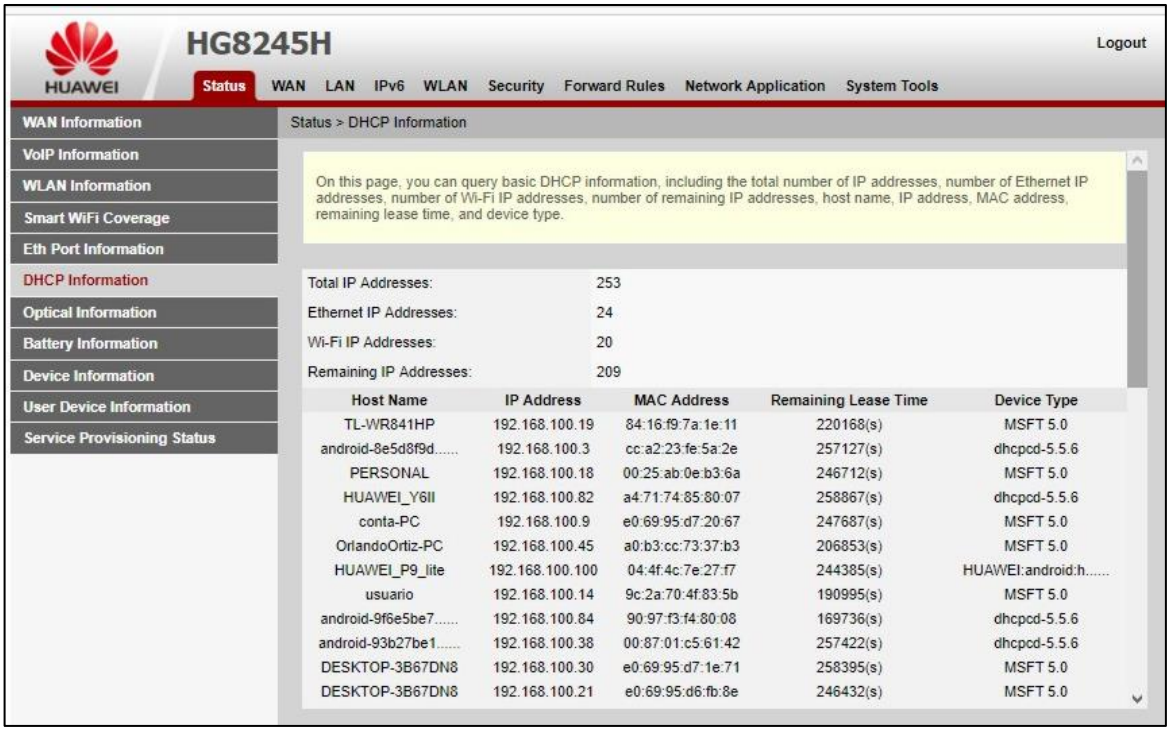
Figura 26. Verificando WIFI y clave de acceso



Fuente: el autor

Cada vez que los dispositivos de red inician su comunicación en la red, el *Router* deja un historial con las direcciones *MAC* y actualiza la información de dichas direcciones, estos datos se pueden observar en la figura 27.

Figura 27. Conexiones *MAC* - *DHCP* información

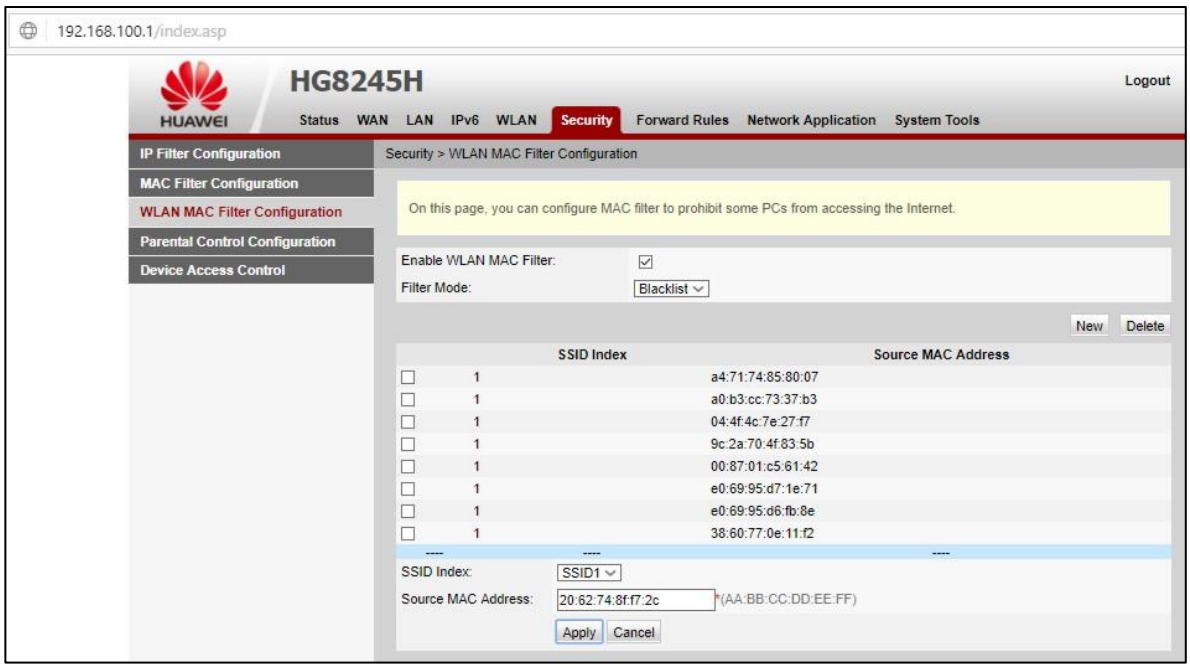


Fuente: el autor

Se realiza una comparación de direcciones *MAC* con la información recopilada en el formato “Información Dispositivos Móviles Empleados CMSFN**”,** Ver Cuadro 16 de este documento, ANEXO I.

Seguidamente y tomando como base las direcciones *MAC* autorizadas, se elabora una lista negra “*Blacklist*” en la opción “*WLAN MAC filter configuration*”, del menú “*Security*” de la configuración del *Router* y se agregan una a una las direcciones *MAC* en este apartado, activando la casilla de verificación “*Enable WLAN MAC Filter*”, de esta manera los dispositivos aquí registrados no tendrán acceso a INTERNET, aunque conozcan la clave de acceso a la WIFI. Ver figura 28.

Figura 28. Bloqueo de direcciones *MAC*



Fuente: el autor

10 RECURSOS

10.1 RECURSOS HUMANOS.

A continuación, se describen los recursos humanos necesarios para la ejecución del presente proyecto.

Cuadro 17. Definición de recursos humanos

RECURSO	Cantidad	Tiempo Horas
1 persona responsable - proponente del proyecto	1	N/A
Trabajo de investigación amenazas y vulnerabilidades de los sistemas de información.	N/A	100
Diseño de políticas de seguridad.	N/A	50
Diseño de guías y diapositivas de apoyo para capacitación de personal.	N/A	30
Capacitación de personal en el desarrollo de habilidades de protección y seguridad informática. Docentes, secretaria, coordinador, auxiliares de tesorería y contaduría, psicología.	N/A	20
Implementación de políticas de seguridad.	N/A	100
	TOTAL	**300**

Fuente: el autor

10.2 RECURSOS FINANCIEROS.

Cuadro 18. Definición de recursos Financieros

RECURSO	VALOR EN PESOS
Acceso a INTERNET	50000
Papelería	50000
Impresión guías, Proyecto	150000
Transporte sitio capacitación personal Colegio	50000
DVDs	30000
Impresión manual guía con políticas de seguridad informática para el colegio mixto san Felipe Neri.	100000
TOTAL	**430.000**

Fuente: el autor

10.3 RECURSOS TECNOLÓGICOS.

Se aprovecha la existencia de los recursos tecnológicos disponibles en el colegio mixto San Felipe Neri de Ipiales, por lo tanto, no se genera un costo en dinero.

Cuadro 19. Definición de recursos Tecnológicos

RECURSOS	Cantidad	Costo
Computadores para capacitación en sala de informática.	21	N/A

RECURSOS	Cantidad	Costo
Video Beam	1	N/A
Mesas múltiples	7	N/A
Routers	2	N/A
Tableros	2	N/A
Swicht	3	N/A
Sillas	30	N/A
Mesa docente	1	N/A
Fotocopiadora	1	N/A
Memorias USB	10	N/A
PC Portátil proponente proyecto	1	N/A
Amplificador sonido	1	N/A
Micrófonos	1	N/A
Marcadores borrables	3	N/A
Tablero	1	N/A
TOTAL	85	N/A

Fuente: el autor

11 RECOMENDACIÓN DE MEDIDAS DE SEGURIDAD INFORMÁTICA A LOS SISTEMAS DE INFORMACIÓN DEL COLEGIO MIXTO SAN FELIPE NERI

11.1 POLÍTICA DE SEGURIDAD.

En el colegio Mixto San Felipe Neri de Ipiales, la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual se establece un compromiso claro de protección de dicho activo como parte fundamental de la continuidad del servicio educativo que se presta, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de las necesidades actuales, el colegio Mixto San Felipe Neri implementa el presente modelo de gestión de seguridad de la información, como la herramienta que permitirá identificar y minimizar los riesgos a los cuales se expone la información, ayudando a la reducción de costos operativos y financieros, estableciendo una cultura de seguridad informática eficaz.

Los directivos, docentes, personal administrativo y de servicios generales y todos aquellos que tengan responsabilidades sobre los sistemas de información, y recursos de procesamiento de la información, deben adoptar los lineamientos que aquí se establecen, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

10.1.1 Responsables del desarrollo, implantación y gestión de la política. A continuación, se relacionan las personas responsables de dar a conocer las políticas de seguridad.

11.1.1.1 Director de Política de Seguridad. Ingeniero Pablo Velásquez: Responsable de realizar, supervisar, inspeccionar, y modificar las normas y reglas establecidas en la política de seguridad.

11.1.1.2 Administrador de la Seguridad de la Información. Ingenieros Pablo Velásquez y Ómar Zúñiga, Encargados de la asignación de roles de acceso a la información, proveer permisos y soportes informáticos, controlar la entrada y salida de información, identificar y dar solución de incidencias, etc.

11.2 POLÍTICA DE RESPONSABILIDAD POR LOS ACTIVOS.

El Colegio Mixto San Felipe Neri al ser propietario de la información física, así como de la información generada, procesada, almacenada y transmitida en sus procesos académicos y administrativos, otorgará la responsabilidad pertinente a las diferentes dependencias sobre sus activos de información, asegurando la consecución de las conductas que regulen el uso adecuado de la misma.

La información concebida en los sistemas de información de las diversas dependencias y de los equipos, tales como, estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes entre otros, son propiedad del colegio, y al

mismo tiempo se convierten en activos intangibles de la institución y se proporcionan a los empleados del colegio y terceros autorizados, para cumplir con los propósitos de la actividad educativa, administrativa y financiera que se presta.

11.3 POLÍTICA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

El comité de seguridad de la información en concordancia con el director de la política de seguridad y el administrador la Seguridad de la Información, definirán los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad, y se generará una guía de clasificación de la Información para que los propietarios de la misma la cataloguen y determinen los controles requeridos para su protección.

Toda la información del colegio debe ser identificada, clasificada y documentada de acuerdo con las guías de clasificación de la Información establecidas por el Comité de Seguridad de la Información.

Una vez clasificada la información, se proporcionará los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado por parte de los docentes, administrativos y personal provisto por terceras partes, que se encuentre autorizado y requiera de ella para la ejecución de sus actividades.

11.4 POLÍTICA DE USO DE PERIFÉRICOS Y MEDIOS DE ALMACENAMIENTO

El uso de periféricos tales como impresoras, video beam, y medios de almacenamiento como memorias USB, discos duros extraíbles, memorias SIM, etc., en el intercambio de la información, será reglamentado por el comité de seguridad de la información en concordancia con el director de la política de seguridad y el administrador la Seguridad de la Información, considerando las labores realizadas por los funcionarios y su necesidad de uso.

11.5 POLÍTICAS DE CONTROL DE ACCESO A REDES Y RECURSOS DE RED

El comité de seguridad de la información, conjuntamente con el director de la política de seguridad y el administrador la seguridad de la Información, como responsables de las redes de datos y los recursos de red del colegio, deben propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico, asegurando que las redes inalámbricas cuenten con métodos de autenticación que evite accesos no autorizados.

11.6 POLÍTICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS

Se establecerá privilegios con el fin de controlar el acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información del colegio. De la misma manera se velará porque los docentes, administrativos y el personal provisto por terceras partes, tengan acceso

únicamente a la información necesaria para el desarrollo de sus labores y la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

11.7 POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

El comité de seguridad de la información velará porque la información del colegio, sea clasificada como reservada o restringida, igualmente será cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

11.7.1 Controles Criptográficos. Dirigido a los responsables de cada dependencia; el comité de seguridad de la información brindará la capacitación necesaria para almacenar y/o transmitir la información digital clasificada como reservada o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.

11.8 POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

El colegio proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos necesarios de procesamiento y almacenamiento, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente, ocasionados por la infección de software malicioso. Además, facilitará los mecanismos para generar cultura de seguridad para docentes, administrativos y demás personal, frente a los ataques de software malicioso.

11.9 POLÍTICA DE GESTIÓN DE VULNERABILIDADES

El comité de seguridad de la información, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de los sistemas de información por medio de la realización periódica de pruebas de vulnerabilidades, realizando la corrección pertinente sobre los hallazgos encontrados por dichas pruebas, igualmente se adelantará los procesos correspondientes para la realización de pruebas de vulnerabilidades y hacking ético.

12 MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA DEL COLEGIO MIXTO SAN FELIPE NERI

12.1 NORMATIVIDAD

Cuadro 20. Normatividad legal vigente colombiana, de los Sistemas de Gestión de Seguridad de la Información

LEGISLACIÓN	TEMA	REFERENCIA
Ley 527/99	Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos	El mensaje de datos es “La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos, Internet, el correo electrónico, el telegrama, el télex o el telefax”.
Ley 594/00	Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones	La presente ley “tiene por objeto establecer las reglas y principios generales que regulan la función archivística del Estado”. Y “comprende a la administración pública en sus diferentes niveles, las entidades privadas que cumplen funciones públicas y los demás organismos regulados por la presente ley”.
Ley 1266/08	Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial,	Se regula el manejo de la información para “todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada”.

LEGISLACIÓN	TEMA	REFERENCIA
	de servicios y la proveniente de terceros países.	
Ley 1273/09	Por medio de la cual se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.	"De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos".
Ley 1581/12	Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales	Hace referencia, en particular, al artículo 15 de la Constitución Nacional, según el cual "todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución…". La ley tiene por objeto "desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así

LEGISLACIÓN	TEMA	REFERENCIA
		como el derecho a la información consagrado en el artículo 20 de la misma".
LEY 1712 DE 2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública	Hace referencia, principalmente, al artículo 74 de la Constitución Nacional en el cual se establece que "Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley". El objeto de la ley es "regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información"

Fuente: Manual de políticas de seguridad y privacidad de la información gobernación de Cundinamarca.

12.2 OBJETIVO

Que todos los empleados del Colegio Mixto San Felipe Neri de la ciudad de Ipiales conozcan los conceptos básicos de seguridad de la información que se implementan en la institución educativa, en procura de su respectiva apropiación y el cumplimiento de las disposiciones aquí consignadas, en pro del manejo responsable y la protección de la misma.

12.3 ALCANCE

El presente Manual es una herramienta de estricto cumplimiento para todos los directivos docentes (Rector, Coordinadores), profesores, orientadores escolares,

personal administrativo financiero y servicios generales del Colegio Mixto San Felipe Neri y toda persona ajena a la institución educativa que proporcione por cualquier tipo de contratación, un servicio en el cual se involucre el manejo de información digital o impresa.
Quienes obligatoriamente se comprometen a cumplir con las determinaciones aquí contempladas.

12.4 SEGURIDAD DE LA INFORMACIÓN

Consiste en asumir responsablemente y por todos los medios posibles la salvaguarda y la protección de la información que se procese en el colegio, garantizan en todo momento, la confidencialidad, integridad y disponibilidad de la misma, certificando que dicha información es 100% original y que procede de una fuente fidedigna.

12.5 GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Reconoce la elaboración de políticas de seguridad que se articulan con las necesidades propias del Colegio Mixto San Felipe Neri. Aquí se analiza las posibilidades de riesgo a los que se ve expuesta la información, con base en las normas establecidas, los procedimientos que se ejecutan al interior de la institución, y las capacitaciones realizadas a los usuarios que manejan los activos de la información.

Su adecuamiento requiere del tiempo apropiado para poder planificar, diseñar, implementar y así conseguir acertadamente que se cumpla con los parámetros de seguridad de la información, propuestos en favor de la institución educativa.

12.6 PRINCIPIOS FUNDAMENTALES DE SEGURIDAD DE LA INFORMACIÓN

Solamente quienes se encuentren autorizados a disponer de la información, podrán hacer uso de la misma, el manejo apropiado que se le dé, deberá permitir en todo momento, que esta esté siempre disponible, sea integra, veraz y se maneje con la mayor confidencialidad entre los usuarios que dispongan de ella.

12.7 PRINCIPIO DE DISPONIBILIDAD

Toda información que involucre los procesos propios del adecuado funcionamiento del Colegio Mixto San Felipe Neri, deberá estar siempre disponible, por ninguna circunstancia se puede almacenar en un sitio diferente al autorizado, la o las personas que tengan a cargo la dependencia donde se procesa la información, son los únicos responsables del principio de disponibilidad.

12.8 PRINCIPIO DE INTEGRIDAD

No puede permitirse por ningún motivo, que la información de cualquiera de las dependencias del colegio esté corrupta, y que su veracidad se ponga en tela de

juicio. Solamente quien esté autorizado podrá realizar las modificaciones pertinentes.

12.9 PRINCIPIO DE CONFIDENCIALIDAD

Este principio somete a todos los empleados del Colegio Mixto San Felipe Neri a ser transparentes con el manejo de la información, salvaguardando el conocimiento de su contenido como un secreto.

Además, todos los usuarios deberán velar por la confidencialidad de la información a su cargo, evitando que sea revelada a terceros, so pena de ser sancionados de acuerdo a las especificaciones del reglamento interno de trabajo.

Figura 29. Principios de Seguridad de la información Colegio Mixto San Felipe Neri.

Fuente: Manual del Sistema de Gestión de Seguridad de la Información para el Colegio Mixto San Felipe Neri.

12.10 DEFINICIONES DE SEGURIDAD

12.10.1 Vulnerabilidad. Debilidad que se produce cuando un atacante tiene la oportunidad de acceder a los activos de la información, porque en un momento dado cuenta con los medios propicios.

12.10.2 Amenaza. Cuando un atacante ha logrado identificar una debilidad en los sistemas de información y la aprovecha para poder acceder sin la previa autorización.

12.10.3 Agente de amenaza. Aprovecha cualquier vulnerabilidad para poder tener acceso a los sistemas de información.

12.10.4 Riesgo. Es el impacto causado sobre los activos informáticos, después de aprovechar una o más vulnerabilidades.

12.10.5 Salvaguarda. Es la mitigación de los riesgos potenciales que se han establecido para la información, aplicando diversos controles.

12.11 COMPROMISO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El comité de seguridad de la información es el apoyo y soporte de la protección de la información del Colegio Mixto San Felipe Neri, puesto que tiene la competencia en la orientación, capacitación y desarrollo apropiado de los procedimientos convenientes en la implementación de los sistemas de gestión de seguridad informática (SGSI).

12.12 GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN

12.12.1 Activos de Información. Toda la información que se ocasione, procese, transfiera y almacene por cualquiera de los empleados del Colegio Mixto San Felipe Neri u otro particular asociado a contratación, se convierte en propiedad absoluta de la institución, pudiendo ser verificada y revisada en cualquier momento por el empleador o quien haga las veces de su designado sin previo consentimiento del funcionario responsable del activo.

12.12.2 Inventario de Activos. Todos los empleados del colegio y responsables de los procesos de los sistemas de información, deben identificar y elaborar un inventario de dichos activos a su cargo, aplicando el procedimiento indicado en el ANEXO F, "*Inventario de activos de información, software, hardware y servicios*", además son los directos responsables de cumplir con el principio de disponibilidad.

12.12.3 Clasificación de la Información. La información del Colegio Mixto San Felipe Neri se clasifica según su confidencialidad, integridad y disponibilidad de acuerdo con la sensibilidad e importancia de ésta, aplicando el procedimiento indicado en el ANEXO E, "*Medidas de seguridad según el nivel de clasificación de la información*."

Al realizar la clasificación, se debe identificar también el propietario de cada activo y su responsabilidad, basado en:

- Realizar un análisis de riesgos de los activos de información, según las necesidades del proceso.
- Tomar decisiones y acciones apropiadas con el fin de eliminar en la medida de las posibilidades los riesgos a los que se expone el activo.
- Mantener actualizados el inventario de los activos de información.
- De ser necesario re-clasificar los activos, siguiendo el procedimiento apropiado.
- Recopilar y manipular la información a su cargo de acuerdo con el nivel de clasificación.

12.12.3.1 **Según su Confidencialidad**. La información se clasificará de la siguiente manera:

- SECRETO: información pertinente a una o varias actividades o planes educativos, curriculares, administrativos, financieros, etc., que motiven el mejoramiento continuo en los procesos de la institución y que a su vez hacen parte de la autoría del personal empleado por el colegio y/o de cada una de las dependencias, catalogado de carácter exclusivo y cuya divulgación sin autorización podría afectar los intereses de la comunidad educativa.

- RESERVADO: Es aquella información cuya divulgación sin previa autorización podría generar perjuicios para los intereses o el buen nombre del Colegio Mixto San Felipe Neri o miembros de la comunidad educativa.

- CONFIDENCIAL: La información que por su contenido digital o impreso es del interés único del o los autorizados por la institución educativa, por lo que su circulación sin previa autorización puede ocasionar perjuicios a la comunidad educativa.

- INTERNO: Es aquella información dirigida únicamente a los empleados del colegio, su divulgación y/o uso inapropiado, modificación o destrucción podría resultar en pérdidas que, de alguna manera, podrían ser recuperables para la institución, pero que al mismo tiempo implica des favorabilidad en la credibilidad o reputación de las personas o la misma institución.

- PÚBLICA: Información que puede ser distribuida o publicada sin ningún tipo de restricciones, sin que esto conlleve un impacto negativo para los miembros de la comunidad educativa.

12.12.3.2 **Según su Integridad.** La información se clasificará de la siguiente manera:

4. De imposible reparación y/o recuperación, y que al mismo tiempo ocasiona pérdidas graves para el colegio.
3. De difícil reparación y que genera pérdidas significativas.
2. Puede repararse, pero genera pérdidas leves.
1. No afecta la operación de las actividades cotidianas del colegio y puede repararse fácilmente.

12.12.3.3 **Según su disponibilidad.** La información se clasificará de la siguiente manera:

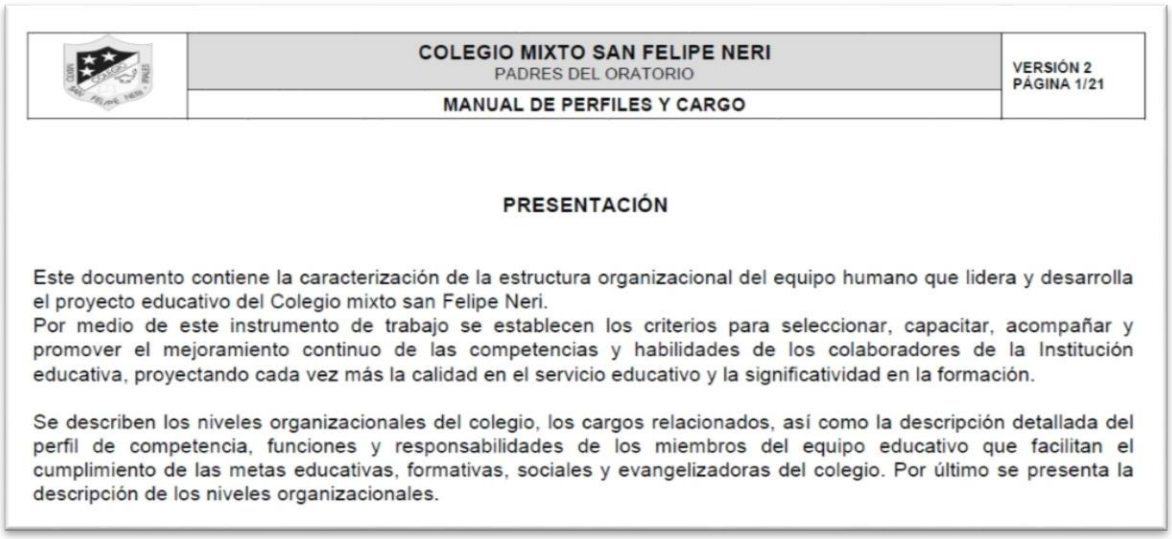
Por la necesidad de su acceso en la premura de tiempo, se tomará como base 5 niveles:

5. CRÍTICOS, la paralización necesita resolverse en minutos o en un máximo de 12 horas.
4. URGENTE, la paralización necesita resolverse en máximo 24 horas.
3. IMPORTANTE, la paralización puede resolverse en máximo 72 horas.
2. NORMAL, la paralización producida puede esperar hasta 1 semana
1. NO ESENCIALES, la paralización producida puede esperar hasta 1 mes.

12.12.4 Rotulado de la Información. Todos los documentos físicos o digitales expedidos por el colegio mixto san Felipe Neri, para los procesos directivo, académico, administrativo financiero o comunitario, están marcados de acuerdo a la versión y al esquema de documentación establecido en la NTC/ISO 9001:2008 establecida en la certificación de calidad del colegio.

12.12.5 Roles y Responsabilidades. Los roles y responsabilidades con respecto a la seguridad de la información se evidencian en el Manual de Funciones del colegio Mixto San Felipe Neri, “Manual de perfiles y cargo” aprobado por el consejo directivo de la institución y socializado con los docentes y directivos docentes al inicio de cada año lectivo, en la planeación institucional.

Figura 30. Presentación del manual de perfiles de cargo del colegio



COLEGIO MIXTO SAN FELIPE NERI
PADRES DEL ORATORIO

VERSIÓN 2
PÁGINA 1/21

MANUAL DE PERFILES Y CARGO

PRESENTACIÓN

Este documento contiene la caracterización de la estructura organizacional del equipo humano que lidera y desarrolla el proyecto educativo del Colegio mixto san Felipe Neri.
Por medio de este instrumento de trabajo se establecen los criterios para seleccionar, capacitar, acompañar y promover el mejoramiento continuo de las competencias y habilidades de los colaboradores de la Institución educativa, proyectando cada vez más la calidad en el servicio educativo y la significatividad en la formación.

Se describen los niveles organizacionales del colegio, los cargos relacionados, así como la descripción detallada del perfil de competencia, funciones y responsabilidades de los miembros del equipo educativo que facilitan el cumplimiento de las metas educativas, formativas, sociales y evangelizadoras del colegio. Por último se presenta la descripción de los niveles organizacionales.

Fuente: Manual Perfiles de cargo - Colegio Mixto San Felipe Neri

12.12.6 Términos y condiciones laborales. Es de obligatorio cumplimiento que los empleados del Colegio Mixto San Felipe Neri o cualquier otro tipo de persona vinculada con la institución, firmen un acta de aceptación del Manual de Seguridad de la Información, cuando de hacer uso de esta información se refiera.
Para el caso de personas ajenas a la contratación del colegio, se incluirá las condiciones aquí dispuestas en el contrato o acuerdo de prestación de servicios.

12.12.7 Concienciación a los usuarios. El Colegio Mixto San Felipe Neri de Ipiales establecerá en la planeación institucional al inicio de cada año lectivo, jornadas pedagógicas con responsabilidad absoluta del comité de seguridad de la información, que permitan la capacitación que sus empleados (Directivos docentes, docentes, administrativos, servicios generales) con el fin de concientizar la adecuada gestión de los activos de información de manera permanente.

De esta manera se promoverá la protección, el uso y el procesamiento adecuado de la información.

12.12.7.1 Cambio de claves de acceso plataforma SAPRED. De estricto cumplimiento todos los usuarios (docentes, administrativos y directivos docentes) que acceden a la plataforma SAPRED, deberán en un plazo no mayor a 2 días después de haber iniciado el nuevo calendario escolar, cambiar la contraseña de acceso al sitio web SAPRED. Lo anterior en pro de evitar el acceso a personas no autorizadas.

12.12.8 Acciones que afectan la seguridad de la Información. A continuación, se describen algunas acciones identificadas que afectan la seguridad de la información, y que ponen en riesgo la disponibilidad, confidencialidad e integridad de la misma, así:

- Dejar los computadores encendidos en horas no laborables.
- Permitir que personas ajenas al Colegio Mixto San Felipe Neri, ingresen sin previa autorización a las dependencias en donde se procesa información relevante para la Institución.
- No clasificar los activos informáticos.
- Desatender la protección de los documentos impresos que contienen información clasificada, al terminar la jornada laboral.
- Utilizar los sistemas de información de la Institución, con el fin de obtener, conservar o divulgar material publicitario o comercial diferente a las establecidas por el colegio.
- Instalar software sin el consentimiento del comité de seguridad de la información.

- Destruir la documentación institucional, sin seguir los parámetros establecidos en el manual de Gestión Documental.
- Descuidar información clasificada de la institución, sin las medidas apropiadas de seguridad que garanticen su protección.
- Enviar información clasificada como no pública de la institución a través de correos electrónicos personales, diferentes a los asignados por la institución.
- Conectar computadores portátiles u otros dispositivos electrónicos personales a la red de datos del Colegio Mixto San Felipe Neri sin previa autorización.
- Ingresar a la red de datos institucional por cualquier servicio de acceso remoto sin la autorización del comité de seguridad de la información.
- Usar servicios de INTERNET en los equipos de la institución, diferente al propósito de las actividades propias del desempeño laboral.
- Desarrollar actividades personales, o utilizar de los recursos tecnológicos del Colegio Mixto San Felipe Neri para beneficio personal.
- Uso de la identidad (cuenta de usuario y contraseña) de otro usuario o facilitar, prestar o permitir el uso de su cuenta personal a otro empleado.
- Dejar al alcance de personas no autorizadas los dispositivos portátiles, móviles y de almacenamiento removibles, entregados para actividades propias del Colegio Mixto San Felipe Neri.
- Retirar de las instalaciones de la institución, computadores de escritorios, portátiles e información física o digital, clasificada, sin autorización.
- Entregar, enseñar y divulgar información clasificada del Colegio Mixto San Felipe Neri a terceros no autorizados.
- Llevar a cabo actividades ilegales, como intentar el acceso no autorizado otros computadores de la red de datos del Colegio Mixto San Felipe Neri.
- Producir cualquier acción que atente contra la reputación o buen nombre del Colegio Mixto San Felipe Neri o alguno de sus empleados.
- Otorgar privilegios de acceso a los activos de información a empleados o terceros no autorizados.

- Realizar acciones con carácter mal intencionado, para evitar y/o transgredir los controles establecidos en el presente manual.
- Comer, beber y fumar cerca a los equipos de cómputo.
- Realizar cualquier otra acción que contravenga disposiciones constitucionales, legales o institucionales.

La ejecución de alguna de las acciones antes descritas, acarreará las acciones disciplinarias pertinentes a que haya lugar, y en consecuencia se actuará de acuerdo a los procedimientos establecidos para cada caso.

12.12.9 Seguridad física y ambiental. Se busca proteger por los medios posibles, los activos de información de cualquier amenaza natural y/o ambiental, tales como inundaciones, terremotos, tormentas, tornados, incendios, explosiones, vandalismo, fraude, robo. Etc.

12.12.10 Seguridad física y del entorno. El Colegio Mixto San Felipe Neri encomendará a todos sus colaboradores la efectividad de los mecanismos de seguridad física y control de acceso, que aseguren la protección de la información apoyados en el personal de servicios generales y el circuito cerrado de televisión disponible, y del mismo modo, estará atento a las amenazas físicas externas e internas y las condiciones medioambientales de sus instalaciones.

12.12.11 Seguridad de los equipos.

- Los computadores se deben ubicar de tal manera que se logre reducir la exposición a riesgos ocasionados por amenazas ambientales y oportunidades de acceso no autorizado.

- Los computadores destinados al procesamiento de la información clasificada, se ubicarán de tal manera que el responsable de la dependencia no pueda ser visto a través de ventanas o paredes de vidrio.

- Los computadores se deben ubicar de tal manera que se reduzca el riesgo de visualización por personas no autorizadas cuando este se encuentra en uso.

12.12.12 Suministro de energía. Los computadores de cada una de las dependencias deben estar provistos de una UPS, que permita solventar el fluido eléctrico cuando se suscite posibles fallas, en el suministro de energía u otras anomalías eléctricas.

Para evitar alteraciones en el suministro de energía, se verificará las especificaciones del fabricante o proveedor de cada equipo.

Para asegurar la continuidad del suministro de energía se deben atender los siguientes controles:

- Dispone de múltiples tomas corrientes o líneas de suministro.
- Se cuenta con un suministro constante de energía Ininterrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del servicio de los equipos de cómputo.
- Se verifica que los niveles de carga no superen los establecidos por las normas.
- Las instalaciones eléctricas están protegidas con sistema de polo a tierra y que estos cumplen con los estándares vigentes.
- Las instalaciones eléctricas están protegidas contra las fluctuaciones de voltaje tales como *breakers* y supresores de picos.

12.12.13 Seguridad del cableado. Para el cableado de energía eléctrica y de comunicaciones que transporta información y que sirve de apoyo a los servicios de los sistemas de información, se verifica la inexistencia de intercepción o deterioro:

- Se cumple con el reglamento técnico de instalaciones eléctricas – *RETIE*15, expedido por el Ministerio de Minas y Energía.
- Se cumple con los estándares ANSI/EIA/TIA 568A o 568B16
- Las instalaciones de cableado estructurado están protegidas contra la influencia o daño causado por agentes externos.
- Los elementos metálicos que forman parte de los cableados estructurados están conectados al sistema de polo a tierra de la edificación.
- Los centros de cableado cuentan con rack para alojar los equipos y terminaciones de los cableados, cumpliendo las normas técnicas y asegurados con chapas o cerraduras de seguridad, cuyas llaves sean administradas por personal técnico capacitado.

12.12.14 Mantenimiento de los equipos. El mantenimiento de los computadores y demás equipos de cómputo se gestiona tomando en cuenta los siguientes controles:

- Mantenimiento preventivo a los equipos de acuerdo con la regularidad de uso.
- Uso de un sistema de información y verificación por parte del jefe de cada dependencia que permite llevar el control del detalle y de la frecuencia del mantenimiento realizado a c/u de los equipos.

15 Este reglamento se preocupa por poder controlar todos los aspectos relacionados con la instalación eléctrica en términos del mantenimiento y cuidado del medio ambiente, las personas involucradas, la simbología, la evaluación de los niveles de riesgo y los requerimientos generales para la instalación.

16 Requerimientos generales sobre cómo instalar el Cableado de Telecomunicaciones en Edificios Comerciales

- Sólo el personal de mantenimiento que se encuentra autorizado puede llevar a cabo reparaciones en los equipos.
- El responsable técnico de los equipos registra todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
- El jefe de cada dependencia elabora acta de entrega y firma con copia adjunta al responsable técnico a cargo, el retiro del o los computadores de las instalaciones del Colegio Mixto San Felipe Neri para su mantenimiento.
- Eliminación de la información confidencial de forma segura de los equipos que se haga necesario retirar y/o realizando previamente las respectivas copias de respaldo de ser necesario.
- El jefe de cada dependencia acompañará el mantenimiento de los equipos a su cargo, siempre y cuando considere que estos contengan información relevante.

12.12.15 Destrucción o reutilización segura de equipos. Se realiza borrado seguro de la información o destrucción física del dispositivo de almacenamiento, antes de la reutilización o de la devolución de cualquier equipo de cómputo.

12.12.16 Normas de escritorios y pantallas limpias. Estas normas tienen como finalidad reducir los riesgos producidos por el acceso no autorizado, pérdida y daño de la información. Para lo cual se establecen las siguientes pautas:

- Almacenar bajo llave todos los documentos en papel y los dispositivos de almacenamiento removibles que se consideren importantes, en cajones y/u otro tipo de archivos seguro cuando no están siendo utilizados, especialmente fuera del horario laboral.
- Guardar bajo llave la información clasificada (preferiblemente en una caja fuerte) cuando no esté en uso.

- Bloquear la sesión de los computadores personales cuando no se está usando y restablecer su uso con la solicitud de contraseña.
- Activar el protector de pantalla en forma automática, máximo después de cinco (5) minutos de inactividad.
- Desconcertar las fotocopiadoras después del horario normal de trabajo.
- Retirar inmediatamente la información relevante una vez impresa y darle el trámite necesario oportunamente.
- Evitar que se creen accesos directos a archivos importantes en el escritorio de Windows o cualquier otro sistema operativo activo en los equipos de cómputo.

12.12.17 Protección contra código malicioso. El comité de seguridad de la información, implementa controles para prevenir y detectar código malicioso, lo cual se basa en software, concienciación de usuarios y gestión del cambio.

Los controles implementados contemplan las siguientes directrices:

- No permite el uso de software no autorizado por el comité de seguridad de la información.
- No permite compartir carpetas en los equipos de cómputo.
- Instala y actualiza software de detección y reparación de virus y anti-spyware examinado cada uno de los computadores y medios informáticos, como medida preventiva y rutinaria.
- Realiza continuamente mantenimiento de software y datos de los equipos de procesamiento.
- Verifica antes de su uso, la presencia de virus en archivos de medios electrónicos de origen dudoso, o en archivos recibidos a través de correos electrónicos no confiables.
- Concientiza al personal de como contrarrestar la acción de los virus informáticos.

12.12.18 Controles de las redes. El Comité de seguridad de la información define los controles de seguridad de la red de datos del colegio. Estos controles contemplan salvaguardas especiales para:

- Los equipos activos de las redes LAN, del colegio.
- Mantener la disponibilidad de los servicios de red e infraestructura tecnológica conectada a ella.
- Transmisión de información a través de redes públicas.
- Intercambio de información interinstitucional con el sector público y privado.
- Supervisión de accesos autorizados con nombres de usuario y manejo de *password*.

12.12.19 Seguridad de los servicios de red. Los servicios de red provenientes de un tercero, se ajustan a las siguientes condiciones:

El Colegio Mixto San Felipe Neri establece los mecanismos de control en sus relaciones con personal externo, el cual le provee bienes y servicios a la institución. Los empleados responsables de la realización y/o firma de contratos, acuerdos o convenios con personal externo deben garantizar el cumplimiento del Manual de Seguridad de la Información por parte de estos.

Para lo cual se definen las siguientes directrices:

- Todos los contratos deben tener claramente definidos los acuerdos de niveles de servicios contratados.
- Diligenciar y firmar los acuerdos de confidencialidad y de intercambios de información con personal ajeno al colegio.

- Antes de permitir el acceso o la entrega de información a un tercero, se debe realizar una evaluación del riesgo, por parte del propietario del activo de información o jefe de la dependencia.
- Chequeo del tráfico de la red con software libre ejemplo: Pandora FMS
- Monitoreo de los puertos en la red haciendo uso de herramientas amparadas por licencias de software libre (*KALI LINUX, WIFISLAX*)

12.12.20 Mensajería electrónica. La mensajería electrónica del Colegio Mixto San Felipe Neri de Ipiales, está asociada a los servicios de correo electrónico de los dominios @hotmail.com, @hotmail.es, @gmail.com @yahoo.com @gmail.com y está regulada por los términos de uso adecuado y netiqueta.

12.12.21 Responsabilidad de los usuarios. Todos los empleados del Colegio Mixto San Felipe Neri o terceros, que tienen acceso a los sistemas de información, conocen y cumplen los términos de las disposiciones descritas en el presente manual, donde se dictan pautas sobre derechos y deberes con respecto al uso adecuado de la información.

12.12.22 Identificación de equipos en la red. El Colegio Mixto San Felipe Neri controla e identifica los equipos conectados a su red, mediante el uso de controladores de dominio y *DHCP*.

El servicio *DHCP* para los equipos de cómputo realiza la reserva de las direcciones *MAC* con respecto a las direcciones IP que asigna el servicio.

12.12.23 Acceso a INTERNET. El acceso a INTERNET se regula bajo los siguientes parámetros:

- El Colegio Mixto San Felipe Neri, provee a través de un Prestador de Servicios de Internet, el servicio de internet institucional, el cual es administrado por el comité de seguridad de la información y es el único servicio de internet autorizado.
- El acceso a INTERNET requiere de la autenticación de los usuarios, mediante el uso de usuario y contraseña.
- El uso de INTERNET está regulado por los términos de uso adecuado de la INTERNET.
- Los usuarios proceden a bloquear sus sesiones, cuando deban abandonar temporalmente su puesto de trabajo.
- Los equipos de cómputo deben apagarse al finalizar la jornada laboral o cuando exista una ausencia temporal que supere la ½ hora.

13 CRONOGRAMA DE ACTIVIDADES.

Cuadro 21. Cronograma

ACTIVIDAD	Julio				Agosto				Septiembre				Octubre				Noviembre			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Recopilación de información.																				
Clasificación de información.																				
Documentación.																				
Conformación comité de seguridad de la información.																				
Identificación de riesgos, amenazas y vulnerabilidades.																				
Definición de políticas de seguridad.																				
Definición del ciclo PHVA.																				
Elaboración digital manual con políticas de seguridad informática.																				
Socialización y capacitación de personal - políticas de seguridad informática.																				
Recomendación de políticas de seguridad informática.																				
Ejecución Políticas se seguridad informática.																				

Fuente: el autor

14 CONCLUSIONES

- La identificación de amenazas y vulnerabilidades reconocidas en los sistemas de información administrativos y académicos del colegio mixto san Felipe Neri, se hicieron las recomendaciones apropiadas a todos los directivos, docentes y demás empleados del colegio, para que se tengan en cuenta y se tome como base el manual de políticas de seguridad informática del colegio.

- Los responsables directos de la información, directivos, docentes y demás personal que labora en la institución, tomaron conciencia de ejecutar acciones de protección de la información a su cargo. Lo anterior gracias a la verificación con hechos reales, del descuido de algunos docentes, que no efectuaron el cambio de claves respecto del acceso a la plataforma SAPRED, y el evidente acto de algunos docentes de compartir la clave de acceso WIFI con los estudiantes.

- El hecho de haber realizado un análisis de la información obtenida de las amenazas y vulnerabilidades de los Sistemas de Información del colegio, permitió tomar acciones de mitigación oportunas, prestando mayor atención al acceso a la *WLAN*, y en este particular se elaboró un formato nuevo de uso exclusivo del comité de seguridad informática del colegio, para almacenar la información de las direcciones MAC de los dispositivos móviles autorizados, y al mismo tiempo hacer un uso adecuado de la conexión a INTERNET.

- El manejo y el tratamiento de los sistemas de información académicos y administrativos del colegio, queda más protegido ahora que se tiene a la mano un manual con políticas de seguridad informática exclusivo para el colegio y un comité de seguridad informática que estará a cargo de velar por el adecuado uso de la información.

- La aplicación de la metodología MAGERIT permitió revelar y planificar las medidas oportunas que se necesitaban diseñar y recomendar al interior de los sistemas de gestión de seguridad informática, para mantener los riesgos bajo control.

- Mediante la ejecución de la distribución de Linux WIFISLAX, que permitió hacer auditoría de seguridad a la red inalámbrica del colegio, se pudieron ejecutar pruebas de pen test y hacking ético, para la identificación de las vulnerabilidades y amenazas a las que se encontraba expuesta la WLAN del colegio.

15 RECOMENDACIONES

- Capacitar por los menos 2 veces al año a los docentes, administrativos y directivos docentes, en estrategias de prevención para el manejo de la red WIFI y el tráfico de información.

- Establecer como medida preventiva el cambio de clave de acceso a la red WIFI, por lo menos cada mes y hacer la respectiva divulgación únicamente por parte del comité de seguridad informática.

- Apropiar por parte de todo el personal que hace uso de la red WIFI, el manual de políticas de seguridad informática del colegio mixto san Felipe Neri, con el fin de proteger los procesos de información y la infraestructura de red LAN y WLAN.

- Realizar periódicamente auditorías informáticas a la red inalámbrica del colegio, de tal manera que se pueda visualizar en tiempo real los posibles problemas que estén ocurriendo y así buscar soluciones oportunas.

- Recomendar que por ningún motivo se establezca en el Router la protección WEP, en vista que ofrece un mínimo nivel de protección y en un entorno de tráfico de información como el que se maneja en el colegio, podría permitir con facilidad que se puedan romper las claves WEP.

- Actualizar cada dos mes o cuando se crea conveniente por parte del comité de seguridad informática, la información contenido en el formato “Información Dispositivos Móviles Empleados CMSFN”

BIBLIOGRAFÍA

ALVAREZ BASALDÚA, Luis Daniel. Seguridad en informática (auditoría de sistemas). Tesis de grado para obtener el título de maestro en ingeniería de sistemas empresariales. México, D. F. 2005. Universidad iberoamericana.

CENTRO CRIPTOLÓGICO NACIONAL CN-CERT – España, {En Línea}. {Consultado diciembre 2016}. Disponible en: https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar/pilar.html

CORREA LÓPEZ, Jhullián. Manual de Políticas y Estándares en seguridad informática versión 1. INTENALCO educación superior. Disponible en: http://www.intenalco.edu.co/MP_V01.pdf

ECURED conocimiento con todos y para todos – Cuba, {En Línea}. {Consultado octubre de 2017}. Disponible en: https://www.ecured.cu/Pruebas_de_caja_blanca

EL MUNDO DE LAS TICS.net, {En Línea}. {Consultado octubre 2016}. Disponible en INTERNET: http://www.elmundodelastics.net/2009/07/9-pasos-para-implementar-la-seguridad.html#.WA12OGVX_IU

ESQUIVEL SUAZO, María Luisa. Seguridad informática. Instituto tecnológico de Tijuana, Tijuana México mayo de 2011. Disponible en: https://sites.google.com/site/scesquivelsuazomarialuisa/7-conclusiones/5-2-marco-historico.

GALLO OÑATE, Antonio Rafael, Diagnóstico de cumplimiento del modelo gestionado por el sistema de administración de la seguridad de la información de

gobierno en línea – SASIGEL alineado con la norma 27000 para el instituto nacional de formación técnica profesional de la guajira. Monografía Trabajo de Grado para optar al Título Académico de Especialista en Seguridad Informática. Valledupar, Cesar 2014. Universidad Nacional Abierta y a Distancia – UNAD. Escuela de ciencias básicas, tecnología e ingeniería (ECBTI).

GAONA VASQUEZ, Karina del Rocio. Aplicación de la metodología MAGERIT para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa pesquera e industrial BRAVITO S.A. en la ciudad de Machala. Universidad politécnica salesiana sede cuenca, {En Línea}. {Consultado diciembre 2016}. Disponible en: http://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf

INSTITUTO COLOMBIANO DE CRÉDITO EDUCATIVO Y ESTUDIO TÉCNICO EN EL EXTERIOR ICETEX, Manual seguridad de la información {En Línea}. {Consultado octubre 2016}. Disponible en: https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manualseguridadinformacion.pdf

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS ICONTEC, Documentación. Presentación de tesis, trabajos de grado y otros trabajos de investigación. Norma técnica colombiana NTC 1486 (Sexta actualización), editada agosto 4 de 2008, actualizada Julio 23 de 2008.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS ICONTEC, Referencias bibliográficas, contenido, forma y estructura. Norma técnica colombiana NTC 5613, editada agosto 4 de 2008.

LEY 1341 DE 2009, {En Línea}. {Consultado agosto 2015}. Disponible en: http://www.mintic.gov.co/portal/604/articles-3707_documento.pdf

LINSET: Manual para crackear una red WI-FI con WPA y WPA2 rápidamente, {En Línea}. {Consultado octubre de 2017}. Disponible en: https://www.redeszone.net/seguridad-informatica/linset-manual-para-crackear-una-red-wi-fi-con-wpa-y-wpa2-rapidamente/

MAGERIT {En Línea}. {Consultado diciembre 2016}. Disponible en: https://www.youtube.com/watch?v=JrYfIPs9EXQ

METODOLOGÍA DE ANÁLISIS DE RIESGOS MEDIANTE MATRIZ DE EVALUACIÓN Y RESPUESTA, {En Línea}. {Consultado diciembre 2016}. Disponible en: https://www.youtube.com/watch?v=pa4dSPDwhac

MINISTERIO DE DEFENSA NACIONAL POLICÍA NACIONAL, Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional, {En Línea}. {Consultado noviembre 5 de 2016}. Disponible en: http://www.policia.edu.co/documentos/normatividad_2016/manuales/Manual%20del%20sistema%20de%20gestión%20de%20seguridad%20de%20la%20información%20para%20la%20Policía%20Nacional.pdf

MINTIC, (2016), Ley 1273, {En Línea}. {Consultado septiembre 2016}. Obtenido de: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Amenazas y Riesgos en el manejo de la Información, {En Línea}. {Consultado septiembre 2016}. Disponible en INTERNET: http://www.fiduagraria.gov.co/wp-content/uploads/2014/12/Amenazas-y-riesgos-en-el-manejo-de-la-informacion.pdf

NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001, Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la

información (SGSI). Requisitos, {En Línea}. {Consultado agosto 2016}. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

PLATAFORMA SAPRED – Colombia, {En Línea}. {Consultado de abril a octubre de 2017}. Disponible en: www.sapred.com, propiedad de SITI soluciones S.A.S

PORTAFOLIO SAPRED – Colombia, {En Línea}. {Consultado noviembre de 2017}. Disponible en: http://www.sapred.com/wp-content/uploads/pdf/portafolio.pdf

PRESIDENCIA DE LA REPÚBLICA, Manual de la política de seguridad para las tecnologías de la información y las comunicaciones – tics, {En Línea}. {Consultado noviembre 4 de 2016}. Disponible en: http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/M-TI-01-Manual-Sistema-Seguridad-Informacion.pdf

VIDEO REALIZADO SOBRE EL LIBRO 1: Método de MAGERIT versión 2 Metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, {En Línea}. {Consultado diciembre 2016}. Disponible en: https://www.youtube.com/watch?v=czgBuaokK-Y

WELIVESECURITY en español (2016), {En Línea}. {Consultado septiembre 2016}. ¿Qué es una Declaración de Aplicabilidad (SoA) y para qué sirve? Obtenido de: http://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa

ANEXOS

ANEXO A. Solicitud dirigida al presbítero Esteban Solarte

Ipiales, Mayo 20 de 2015.

Presbítero.
ESTEBAN SOLARTE
Prepósito congregación del Oratorio de San Felipe Neri.
Ipiales.

Apreciado padre, reciba un atento y caluroso saludo.

Muy respetuosamente quiero comentarle que actualmente estoy cursando estudios de posgrado en "**ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA**" con la Universidad Nacional Abierta y a Distancia – UNAD.

Dada la oportunidad de poner en práctica los conocimientos que he venido adquiriendo a lo largo de este proceso formativo, quiero solicitarle muy formalmente se me autorice realizar mi proyecto de grado al interior de los sistemas de información académicos y administrativos del colegio.

Dicho proyecto tiene por título:

"Implementar medidas de seguridad informática a los sistemas de información administrativos y académicos del colegio Mixto San Felipe Neri de Ipiales, en relación a las amenazas y vulnerabilidades identificadas en cada uno de los sistemas."

Por lo anterior, pongo en consideración esta propuesta, esperando que mi solicitud pueda ser evaluada y en lo posible aprobada.

Igualmente quiero agradecerle por la oportunidad que se me pueda brindar, puesto que este es un requisito ineludible exigido por la universidad para la continuidad del proyecto de grado y la futura aprobación de la especialización que estoy cursando.

Quedo muy agradecido con usted y con la congregación del oratorio de san Felipe Neri de Ipiales.

Atentamente,

Ing. Pablo Aníbal Velásquez Rosales.
Coordinador académico y de convivencia.
Colegio mixto san Felipe Neri – Ipiales.

COLEGIO MIXTO SAN FELIPE NERI
RECTORIA

ANEXO B. Solicitud dirigida al presbítero Roberto Melo - Rector

Ipiales, Mayo 20 de 2015.

Presbítero.
ROBERTO FLORENCIO MELO BRAVO
Rector Colegio Mixto San Felipe Neri.
Ipiales.

Estimado rector, reciba un atento y caluroso saludo.

Muy respetuosamente quiero comentarle que actualmente estoy cursando estudios de posgrado en "**ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA**" con la Universidad Nacional Abierta y a Distancia – UNAD.

Dada la oportunidad de poner en práctica los conocimientos que he venido adquiriendo a lo largo de este proceso formativo, quiero solicitarle muy formalmente se me autorice realizar mi proyecto de grado al interior de los sistemas de información académicos y administrativos del colegio.

Dicho proyecto tiene por título:

"Implementar medidas de seguridad informática a los sistemas de información administrativos y académicos del colegio Mixto San Felipe Neri de Ipiales, en relación a las amenazas y vulnerabilidades identificadas en cada uno de los sistemas."

Por lo anterior, pongo en consideración esta propuesta, esperando que mi solicitud pueda ser evaluada y en lo posible aprobada.

Igualmente quiero agradecerle por la oportunidad que se me pueda brindar, puesto que este es un requisito ineludible exigido por la universidad para la continuidad del proyecto de grado y la futura aprobación de la especialización que estoy cursando.

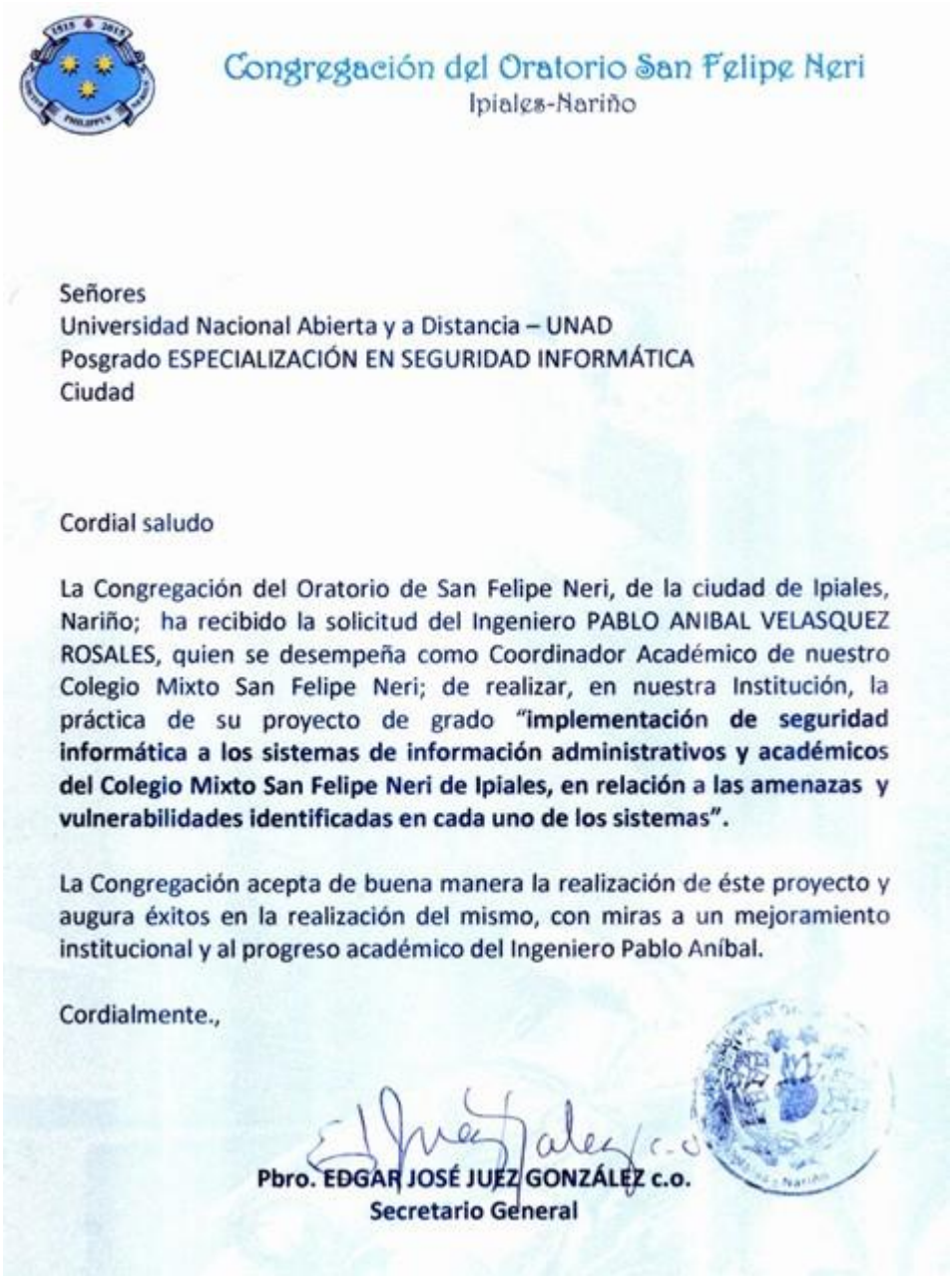
Quedo muy agradecido con usted y con la congregación del oratorio de san Felipe Neri de Ipiales.

Atentamente,

Ing. Pablo Aníbal Velásquez Rosales.
Coordinador académico y de convivencia.
Colegio mixto san Felipe Neri – Ipiales.

Recibido:
Doris Mejía
Hora 12:43

ANEXO C. Aprobación de proyecto por parte de la Congregación del Oratorio de San Felipe Neri



Congregación del Oratorio San Felipe Neri
Ipiales-Nariño

Señores
Universidad Nacional Abierta y a Distancia – UNAD
Posgrado ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
Ciudad

Cordial saludo

La Congregación del Oratorio de San Felipe Neri, de la ciudad de Ipiales, Nariño; ha recibido la solicitud del Ingeniero PABLO ANIBAL VELASQUEZ ROSALES, quien se desempeña como Coordinador Académico de nuestro Colegio Mixto San Felipe Neri; de realizar, en nuestra Institución, la práctica de su proyecto de grado **"implementación de seguridad informática a los sistemas de información administrativos y académicos del Colegio Mixto San Felipe Neri de Ipiales, en relación a las amenazas y vulnerabilidades identificadas en cada uno de los sistemas".**

La Congregación acepta de buena manera la realización de éste proyecto y augura éxitos en la realización del mismo, con miras a un mejoramiento institucional y al progreso académico del Ingeniero Pablo Aníbal.

Cordialmente.,

Pbro. EDGAR JOSÉ JUEZ GONZÁLEZ c.o.
Secretario General

ANEXO D. Acta de conformación comité de seguridad de la información

COLEGIO MIXTO SAN FELIPE NERI
PADRES DEL ORATORIO

ACTA

TEMA	Comité de Seguridad informática		CONVOCA	Rector.	
UBICACIÓN	Rectoría.		OBJETIVO	Conformar el comité de Seguridad informática del Colegio Mixto San Felipe Neri.	
HORA INICIO	8:00 a.m				
HORA FIN	9:00 am		PARTICIPANTES	Pablo A. Velásquez R, Óscar Zúñiga Botina. Víctor Daniel Obando.	
FECHA	14	04 2017			

ASPECTOS A TRATAR

Saludo.
Motivos citación a reunión – Necesidad de proteger la información del Colegio.
Conformar el comité de seguridad de la información
Acuerdos
Firma de Acuerdos.

DESARROLLO

Se da inicio a la reunión saludando a los participantes Ingeniero. Óscar Zúñiga docente de Tecnología e Informática, y al Licenciado Víctor Daniel Obando, Coordinador académico y de convivencia de la institución.

Posteriormente se socializa que el colegio está exponiendo la información digital que se procesa en las diferentes dependencias a muchos riesgos y amenazas; Que igualmente podríamos ser víctimas de delincuentes informáticos que pueden aprovechar nuestras vulnerabilidades para atacar nuestros sistemas de información y ocacionarnos muchos problemas sino se toman las medidas apropiadas a tiempo.

Que por este motivo se hace necesario conformar un comité de seguridad de la información, que trabaje paralelamente con los demás proyectos institucionales, con el fin de orientar un apropiado manejo de la información, que permita de alguna manera identificar amenazas y mitigar los riesgos existentes.

Se acuerda socializar la conformación con el comité y el Consejo académico de las funciones y actividades a realizar.

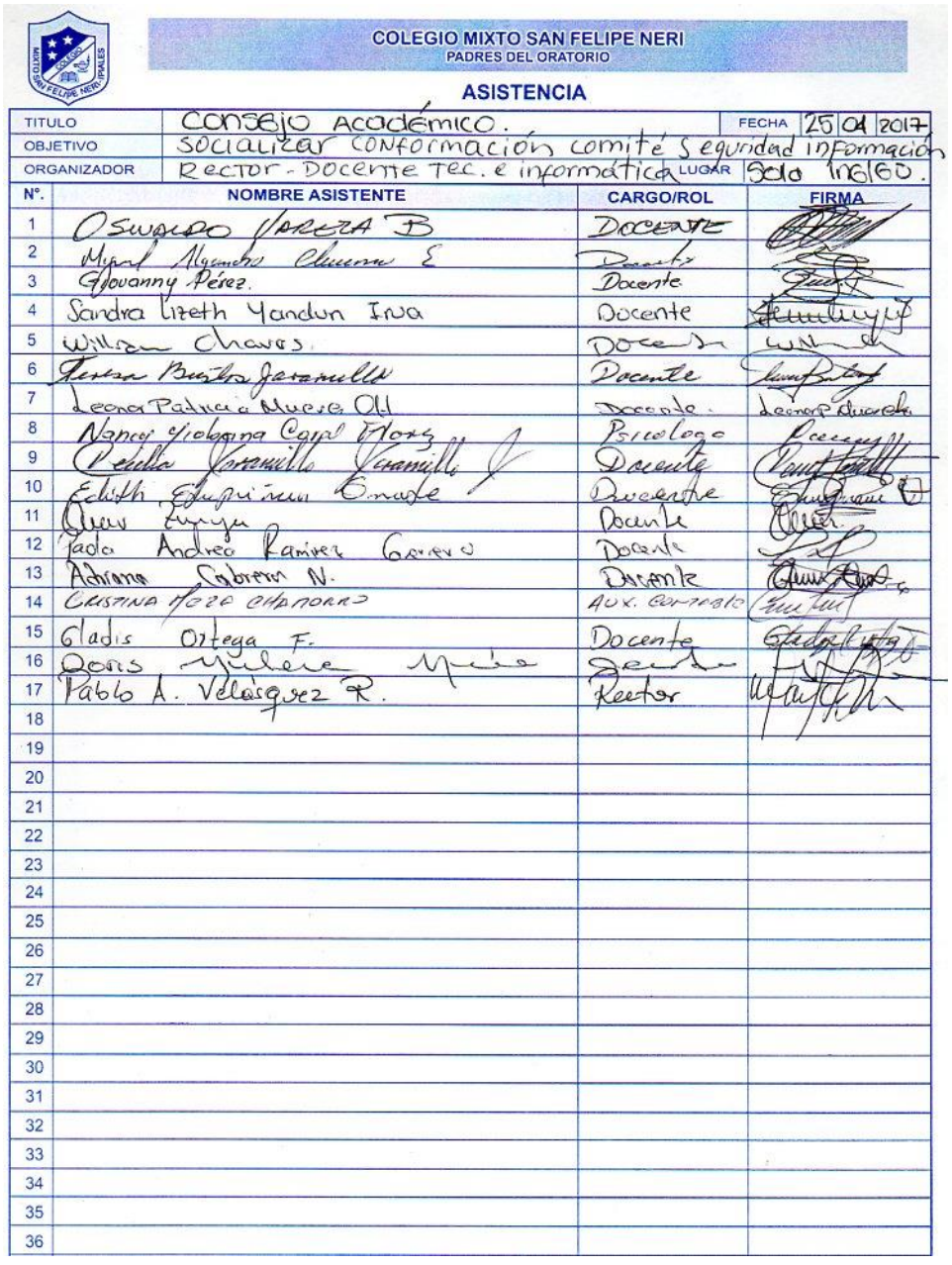
ACUERDOS

Los participantes se comprometen a velar por el apoyo del Comité de seguridad de la información.

87714.305 87247424. 87.775.047 Ipiales

PREPARÓ	REVISÓ

ANEXO E. Socialización del comité de seguridad de la información con el consejo académico



COLEGIO MIXTO SAN FELIPE NERI
PADRES DEL ORATORIO

ASISTENCIA

TITULO	Consejo Académico.	FECHA	25 04 2017
OBJETIVO	Socializar conformación comité Seguridad Información		
ORGANIZADOR	Rector - Docente Tec. e informática	LUGAR	Sala TIC 60.

N°.	NOMBRE ASISTENTE	CARGO/ROL	FIRMA
1	Oswaldo Jaramillo B	Docente	
2	Miguel Alejandro Chamorro E	Docente	
3	Giovanny Pérez.	Docente	
4	Sandra Lizeth Yandun Inua	Docente	
5	William Chaves.	Docente	
6	Teresa Beatriz Jaramillo	Docente	
7	Leona Patricia Muese Ott	Docente	
8	Nancy Viviana Capal Mora	Psicologo	
9	Cecilia Jaramillo Jaramillo	Docente	
10	Edith Esperanza Erazo	Docente	
11	Diana Eunice	Docente	
12	Jada Andrea Ramirez Guerrero	Docente	
13	Adriana Cabrera N.	Docente	
14	Cristina Rosa Chamorro	Aux. Contable	
15	Gladis Ortega F.	Docente	
16	Doris Muñoz Muñoz	Docente	
17	Pablo A. Velásquez R.	Rector	
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			
35			
36			

ANEXO F. Encuesta aplicada a los responsables del manejo de la Información

Pregunta	SI	NO
¿Considera adecuada la seguridad de la información en la oficina a su cargo?		
¿Conoce usted las normas de Seguridad Informática que debe considerar al manejar la información académica del colegio?		
¿Sabe a quién dirigirse cuando se presenta un incidente informático, para buscar una solución oportuna?		
¿Ha recibido capacitación y concientización sobre Seguridad Informática dentro del colegio?		
¿Cree que el nivel de Seguridad Informática dentro del colegio es apropiado?		
¿Considera que la seguridad informática de la que dispone en su dependencia es suficiente para salvaguardar la información a su cargo?		
¿Conoce usted de la existencia de políticas de Seguridad de la Información, establecidas por el colegio?		
¿Realiza copias de seguridad de la información que maneja en sus labores diarias de acuerdo a lo establecido en la organización?		
¿Maneja contraseñas Alfanuméricas para el acceso a la red?		
¿Maneja contraseñas Alfanuméricas para el acceso al sistema operativo?		
¿Maneja contraseñas Alfanuméricas para el acceso al software contable, de notas o de tesorería?		
¿Cuándo se presenta un inconveniente de software o hardware en el equipo informático a su cargo, este se soluciona oportunamente?		
¿Usted cree que es segura la conexión a la red de datos del colegio?		

Pregunta	SI	NO
¿Aplica usted las normas establecidas por el colegio, para evitar la fuga de información?		
¿Cree usted que la organización debería invertir para la implementación de un Sistema de Gestión en Seguridad de la Información?		

ANEXO G. Medidas de seguridad según el nivel de clasificación de la información

Procedimiento		**Niveles de Clasificación**				
Tratamiento	Medidas de Seguridad	Secreto	Reservado	Confidencial	Interno	Público
Acceso y Divulgación	Cifrado	X	X	X		
	Controles de acceso Físico y lógico	X	X	X		
	Acuerdo de Confidencialidad	X	X	X		
Generación de copias de medios físicos e impresión	La obtención del consentimiento del propietario, se recomienda	X	X	X		
	Restricción en número de copias por parte del propietario.	X	X	X		
Transmisión a Través de redes Públicas	Cifrado	No se puede enviar esta información.	X	X		
Rotulado	Sello o Sticker según su clasificación.	X	X	X	X	
	Marca de agua o pie de página que	X	X	X	X	

Procedimiento		Niveles de Clasificación				
Tratamiento	Medidas de Seguridad	Secreto	Reservado	Confidencial	Interno	Público
	indique su clasificación					
Destrucción	Destructoras de papel.	X	X	X	X	
	Papelera	X	X	X	X	
	Borrado seguro de la información	X	X	X	X	X
Divulgación a terceros	Consentimiento del propietario y acuerdo de confidencialidad	X	X	X	X	
	Divulgación fecha y clasificación	X	X			
	Requiere etiquetado	X	X	X	X	X
Embalaje correo interno y externo	Dirigido a un destinatario específico y se coloca dentro de dos sobres, con la etiqueta de clasificación en el sobre interno solamente.	X	X	X		

Procedimiento		Niveles de Clasificación				
Tratamiento	Medidas de Seguridad	Secreto	Reservado	Confidencial	Interno	Público
	Un solo sobre sin ningún tipo específico de etiquetado				X	

ANEXO H. Inventario de activos de información, software, hardware y servicios

INVENTARIO DE ACTIVOS DE INFORMACIÓN, SOFTWARE, HARDWARE Y SERVICIOS												
Nombre Del Proceso												
Líder Del Proceso (Responsable De Los Activos De Información)												
Dependencia Responsable							Fecha de elaboración:					
Nombre del activo de información	Descripción del activo de información	Tipología			Clasificación del activo de información						Estado y custodia del activo de información	
		Software	Hardware	Servicios	El activo es crítico para las operaciones de la dependencia			El activo es crítico para las operaciones del colegio.			Custodio del activo de información	Localización del activo de información
					Bajo	Medio	Alto	Bajo	Medio	Alto		
Elaborado por:								Firma Responsable.				
Cargo:												
Lugar y Fecha:												

ANEXO I. Información Dispositivos Móviles Empleados CMSFN

INFORMACIÓN DISPOSITIVOS MÓVILES Colegio Mixto San Felipe Neri						
Nombre Del Proceso						
Líder responsable del Proceso						
Dependencia Responsable						
Fecha inicio captura de información:			**Fecha finalización:**			
Nombre del empleado	Dependencia	Descripción del dispositivo	. Dirección MAC	Acceso WIFI		
				Denegado	Aplazado	Aprobado
Elaborado por:			Firma Responsable.			
Cargo:						
Lugar y Fecha:						

ANEXO J. Acceso a SAPRED con claves de docentes NO actualizadas