

**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO**

**CARRERA DE INGENIERÍA EN TELECOMUNICACIONES CON
MENCIÓN EN GESTIÓN EMPRESARIAL EN
TELECOMUNICACIONES**

TEMA:

**ESTUDIO PARA DETERMINAR LOS MÉTODOS DE PREVENCIÓN Y
PROTECCIÓN DE LA RED DEL LABORATORIO DE
AUTOMATISMO DE LA FACULTAD TÉCNICA
DE LA UCSG**

Previa la obtención del Título de

**INGENIERIA EN TELECOMUNICACIONES
CON MENCIÓN EN GESTIÓN
EMPRESARIAL EN TELECOMUNICACIONES**

AUTOR:

MAYRA VICTORIA HERRERA HERRERA

TUTOR:

ING. LUIS PALAU DE LA ROSA, MSC

Guayaquil, Ecuador

2014



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO**

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por la Srta. **Mayra Victoria Herrera Herrera**, como requerimiento parcial para la obtención del Título de INGENIERÍA EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL EN TELECOMUNICACIONES.

TUTOR

Ing. Luis Palau de la Rosa, MSc.

REVISORES

Ing. Marcos Montenegro Tamayo, Mgs.

Ing. Miguel Heras Sánchez

DIRECTOR DE LA CARRERA

Ing. Miguel Heras Sánchez

Guayaquil, Abril de 2014



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO**

DECLARACIÓN DE RESPONSABILIDAD

Yo, Mayra Victoria Herrera Herrera

DECLARO QUE:

El Trabajo de Titulación **“Estudio para determinar los métodos de prevención y protección de la red del laboratorio de automatismo de la Facultad Técnica de la UCSG”** previa a la obtención del Título de INGENIERÍA EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL EN TELECOMUNICACIONES, ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del Trabajo de Titulación referido.

Guayaquil, a los 22 días del mes de Abril del 2014

LA AUTORA

Mayra Victoria Herrera

C.C.:0503267833



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO**

AUTORIZACIÓN

Yo, MAYRA VICTORIA HERRERA

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación en la biblioteca de la institución del Trabajo de Titulación: “Estudio para determinar los métodos de prevención y protección de la red del laboratorio de automatismo de la facultad técnica de la UCSG”, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 22 días del mes de Abril del 2014

LA AUTORA

Mayra Victoria Herrera

C.C.:0503267833

AGRADECIMIENTO

A Dios, por sus bendiciones y guía a mis Padres por su amor incondicional y constante, porque son la razón de ser quien soy, a mis hermanos por su cariño y fuerzas para seguir adelante, a Rommel Gonzalo por ser mi apoyo por su amor y entrega en los momentos más difíciles de mi vida.

Al ingeniero Manuel Romero por guiarme y brindarme sus conocimientos en la elaboración y culminación del presente proyecto.

A mis maestros de la carrera de Telecomunicaciones por compartir su tiempo y enseñanzas.

DEDICATORIA

El presente trabajo ha sido la culminación de una de las etapas más importantes y trascendentales de mi vida y por eso se las dedico a:

A mi madre Lidia a quien le debo la vida, por ser mi ejemplo de superación y constancia por enseñarme que por cada tropiezo hay más de una razón para levantarse y seguir adelante, por su infinito amor y dedicación.

A mis hermanos Erika y Cristian por ser mi apoyo constante por su amor y confianza.

Y sobre todo a Rommel Gonzalo por creer en mí por su entrega incondicional porque gracias a su inmenso amor y apoyo pude finalizar mi carrera por guiarme siempre a cada momento por ser la luz a final del túnel por el inmenso amor que le tengo mi más fiel respeto y dedicatoria.

ÍNDICE GENERAL

CARÁTULA	i
CERTIFICACIÓN	II
DECLARACIÓN DE RESPONSABILIDAD.....	III
AUTORIZACIÓN.....	IV
AGRADECIMIENTO.....	v
DEDICATORIA	vi
ÍNDICE GENERAL.....	vii
ÍNDICE DE TABLAS	x
ÍNDICE DE FIGURAS	xi
RESUMEN.....	xii
ABSTRACT	xiii
INTRODUCCIÓN	1
CAPÍTULO I: EL PROBLEMA.....	3
1.1. Planteamiento del problema	3
1.1.1. Ubicación del problema en su contexto	4
1.1.2. Situación en conflicto.....	4
1.1.3. Causas	5
1.1.4. Consecuencias	5
1.1.5. Delimitación.....	5
1.2. Formulación del problema.....	6
1.3. Objetivos de la investigación.....	6
1.3.1. Objetivo general	6
1.3.2. Objetivo específicos	6
1.4. Justificación e importancia de la investigación.....	6

CAPÍTULO II: MARCO TEÓRICO	8
2.1. Vulnerabilidad de la red	8
2.2. Tipo de ataques a redes.....	13
2.3. Seguridad informática	16
2.4. Delitos informáticos	20
2.5. Base conceptual	24
2.6. Hipótesis	24
CAPÍTULO III: MARCO METODOLÓGICO	25
3.1. Tipo de investigación	25
3.2. Diseño de la investigación.....	25
3.3. Población y Muestra	26
3.3.1. Población.....	26
3.3.2. Muestra.....	26
3.4. Técnicas e instrumentos de investigación	27
3.5. Recolección de la información	28
3.6. Procesamiento de los datos y análisis.....	28
3.7. Operacionalización de las variables	28
CAPÍTULO IV	29
4. ANÁLISIS E INTERPRETACIÓN DE LOS DATOS	29
4.1. Encuestas	29
4.2. Entrevistas	40

CAPÍTULO V: MÉTODOS DE PREVENCIÓN Y PROTECCIÓN DE LA RED DEL LABORATORIO DE AUTOMATISMO.....	43
5.1. Desarrollo de la propuesta.....	43
5.1.1. Análisis de los riesgos.....	43
5.1.2. Políticas de seguridad informática.....	52
5.1.3. Implementación de parches para gestión de vulnerabilidades.....	63
5.2. Justificación del proyecto.....	65
5.3. Objetivos del proyecto.....	66
5.3.1. Objetivo general.....	66
5.3.2. Objetivos específicos.....	66
5.4. Beneficiarios del proyecto directo e indirecto.....	67
5.5. Localización física.....	67
5.6. Seguimiento y evaluación.....	68
CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES.....	69
Conclusiones.....	69
Recomendaciones.....	70
BIBLIOGRAFÍA.....	71

ÍNDICE DE TABLAS

Tabla 2. 1 Controles de acceso del sistema.....	19
Tabla 3. 1 Operacionalización de las variables.....	28
Tabla 4. 1 Acogida de la red	29
Tabla 4. 2 Información brindada sobre la red	30
Tabla 4. 3 Información brindada por:	31
Tabla 4. 4 Conoce cómo funciona la red.....	32
Tabla 4. 5 Uso la red del laboratorio.....	33
Tabla 4. 6 Máquinas conectadas a la red.....	34
Tabla 4. 7 Quiénes usa el laboratorio.....	35
Tabla 4. 8 Políticas de seguridad.....	36
Tabla 4. 9 Sistema de seguridad para la red.....	37
Tabla 4. 10 Sistema de alta seguridad.....	38
Tabla 4. 11 Factores para proteger la red.....	39
Tabla 5. 1 Formulario de registro de amenazas	47
Tabla 5. 2 Impacto de amenazas	48
Tabla 5. 3 Determinación de contramedidas.....	51
Tabla 5. 4 Caracteres especiales.....	61

ÍNDICE DE FIGURAS

Figura 2. 1 Diagrama de identificación del riesgo de la seguridad.....	8
Figura 4. 1 Acogida de la red	29
Figura 4. 2 Información brindada sobre la red.....	30
Figura 4. 3 Información brindada por:	31
Figura 4. 4 Conoce cómo funciona la red	32
Figura 4. 5 Uso de la red del laboratorio.....	33
Figura 4. 6 Máquinas conectadas a la red	34
Figura 4. 7 Quiénes utilizan la red	35
Figura 4. 8 Políticas de seguridad	36
Figura 4. 9 Sistema de seguridad para la red	37
Figura 4. 10 Sistema de alta seguridad.....	38
Figura 4. 11 Factores para proteger la red.....	39
Figura 5. 1 Facultad Técnica para el Desarrollo	68

RESUMEN

El constante desarrollo tecnológico ha proporcionado una serie de beneficios en lo que se refiere al acceso a la información, a la aplicación de la tecnología para el desarrollo de otras ciencias, así como también es aplicable como herramienta de apoyo en el proceso de aprendizaje en instituciones de educación superior. Sin embargo, este desarrollo tecnológico va de la mano con la aparición de una serie de riesgos relacionados con la vulnerabilidad propia del sistema, esto puede afectar considerablemente el funcionamiento del sistema, considerando que la falta de aplicación de métodos de prevención de riesgos en los sistemas puede incidir que personas no autorizadas tengan acceso a información confidencial o que puedan afectar el correcto funcionamiento del sistema a través de la implementación de *malwares*. El motivo del desarrollo del presente trabajo se encuentra en que se ha podido detectar que existe un alto nivel de vulnerabilidad de los equipos del Laboratorio de Automatismo de la Facultad Técnica de la Universidad Católica Santiago de Guayaquil, por lo tanto se considera necesario investigar las principales falencias que presenta para desarrollar una propuesta que permita reducir los niveles de vulnerabilidad.

Palabras clave: Vulnerabilidad de la red, tipos de ataques a redes, seguridad informática, delitos informáticos.

ABSTRACT

The constant technological development has provided a number of benefits in terms of access to information, the application of technology for the development of other sciences, as well as it is also applicable as a support tool in the learning process in institutions of higher education. However, this technological development goes hand in hand with the emergence of a number of risks related to the vulnerability of the system itself, this can significantly affect the operation of the system, considering that the lack of implementation of methods for the prevention of risks in the systems can impact that unauthorized persons have access to confidential information or that may affect the correct operation of the system through the implementation of malwares. The reason for the development of this work lies in the fact that it has been able to detect that there is a high level of vulnerability of computers in the lab of automatism of the Technical Faculty of the Universidad Catolica Santiago de Guayaquil, therefore it is considered necessary to investigate the main shortcomings that presents to develop a proposal that allows us to reduce the levels of vulnerability.

Key Words: Vulnerability of the network, types of attacks on networks, computer security, computer crime.

INTRODUCCIÓN

En la actualidad debido al constante desarrollo tecnológico, en lo que se refiere a los sistemas de redes, una vulnerabilidad representa una debilidad o defecto que posee un sistema informático, lo que incrementa el nivel de riesgos para el sistema de redes, ya que permite a los atacantes ingresar al sistema sin autorización y dañar la integridad del mismo, es decir, su funcionamiento normal, la confidencialidad y la integridad de los datos que contiene.

Estas vulnerabilidades son el resultado de las deficiencias en el diseño, la implementación o la utilización de un componente de hardware o software del sistema, pero por lo general se debe a errores en el sistema operativo. Algunas vulnerabilidades ocurren cuando la entrada del usuario no se controla, lo que permite la ejecución de comandos permitiéndole al atacante engañar a la aplicación y acceder al sistema.

Estos desperfectos inciden en que se incrementa los riesgos para los sistemas de redes y consecuentemente hace que sea necesaria la implementación de métodos de prevención y protección, sin embargo, no en todas las instituciones en las que se utilizan redes se aplican estos métodos de prevención. Por lo tanto, el presente trabajo está encaminado a analizar la vulnerabilidad que presenta laboratorio de Automatismo de la Facultad de Educación Técnica para el Desarrollo (FET) de la Universidad Católica de Santiago de Guayaquil, para desarrollar métodos de seguridad. El trabajo estará estructurado de la siguiente manera:

En el capítulo I, se identifica y se define claramente el problema en base al cual se desarrollará la investigación, se determinarán los objetivos y la justificación correspondiente.

En el segundo capítulo, se incluirá el marco referencial del trabajo, en donde se analizarán teorías relacionadas con la vulnerabilidad de redes y los métodos de seguridad informática, lo cual proporcionará al lector un mejor entendimiento del trabajo.

En el capítulo III, se definirá la metodología de la investigación, en donde se determina el tipo de investigación, el diseño de investigación, se selecciona la población y muestra en base a la cual se desarrollará el estudio.

En el capítulo IV, se desarrollará la tabulación y el análisis de los resultados obtenidos de la investigación realizada.

En el capítulo V, se definirá la propuesta, en este caso los métodos de prevención y protección para los sistemas informáticos. Finalmente, se incluirán las respectivas conclusiones y recomendaciones, así como también la respectiva bibliografía.

CAPÍTULO I: EL PROBLEMA

1.1. Planteamiento del problema

Actualmente con el desarrollo tecnológico que se experimenta a nivel mundial, se han incorporado una serie de sistemas tecnológicos que son utilizados en diferentes áreas instituciones y en diferentes áreas debido a los beneficios que proporcionan, sin embargo, el desarrollo tecnológico ha ido de la mano con la aparición de ciertos riesgos relacionados con la vulnerabilidad de los sistemas, lo cual generalmente es ocasionado por fallos en el diseño o por la intervención de hackers.

Tal como lo indica Sommerville (2008, pág. 55), “En un sistema crítico, un fallo de funcionamiento puede provocar pérdidas económicas importantes, daños físicos o amenazas a la vida humana”.

Como lo indica Sommerville, los riesgos a los que están expuestos los sistemas informáticos pueden ocasionar grandes pérdidas, por lo que es esencial que se tomen métodos de prevención para reducir estos riesgos. Sin embargo, existen instituciones en donde a pesar de manejar sistemas informáticos a los cuales tienen acceso un número considerable de personas, y en los que almacenan información importante no se aplica ningún tipo de prevención o protección a los mismos.

Una de éstas son las instituciones académicas como la Universidad Católica de Santiago de Guayaquil en la cual se encuentra el laboratorio de Automatismo de la Facultad de Educación Técnica para el Desarrollo, el mismo que es considerado como la columna vertebral para la formación de Ingenieros en Electrónica en control y Automatismo, este laboratorio está constituido por redes de distribución, equipos electrónicos, materiales eléctricos y electrónicos así como software importante para la simulación de circuitos.

En este caso el problema que se ha podido identificar se encuentra en la falta de métodos de prevención y protección que permitan hacer frente a las vulnerabilidades que presenta el laboratorio de Automatismo de la Facultad de Educación Técnica para el Desarrollo (FET) de la Universidad Católica de Santiago de Guayaquil, puesto que, a través de una pre investigación se ha podido identificar que existen equipos que se encuentran en riesgo de sufrir algún tipo de ataques, debido a que la mayoría de los computadores del laboratorio al estar conectados a Internet y consecuentemente pueden ser un blanco para las personas no autorizadas que buscan acceder a información clasificada de la universidad.

1.1.1. Ubicación del problema en su contexto

En la actualidad, la gran mayoría de los equipos tecnológicos tienen conexión a internet, lo cual incide en que exista un mayor riesgo en que puedan ser atacados por hackers o personas mal intencionadas que busquen acceder a información clasificada, sin embargo no todas las instituciones que hacen uso de equipos tecnológicos toman las medidas necesarias para prevenir estos riesgos.

El problema de investigación se encuentra en el laboratorio de Automatismo de la Facultad de Educación Técnica para el Desarrollo (FET) de la Universidad Católica de Santiago de Guayaquil, en donde a pesar de que se manejan sistemas de redes no se han desarrollado métodos de prevención y protección para evitar los riesgos relacionados a los cuales están expuestos estos sistemas por a vulnerabilidad propia de estos sistemas.

1.1.2. Situación en conflicto

La mayor parte de la vulnerabilidad de las redes en realidad se encuentra relacionada a fallas en el sistema o al hecho de que existe una conexión a internet, por lo tanto, resulta obligatorio para todas las instituciones que hacen uso de estas redes a las cuales tienen acceso un gran número de personas, desarrollar e implementar métodos de seguridad que les permita prevenir y proteger los sistemas.

La vulnerabilidad de las redes es un problema que surge cuando en una institución existen varios ordenadores conectados entre sí, lo cual resulta más fácil para los hackers interferir en estos sistemas de redes e interceptar datos. Uno de los aspectos que incrementa los niveles de vulnerabilidad es la Internet que en la mayoría de los casos no prevén métodos de seguridad implícitos en su estructura, lo cual incide en que el riesgo de las violaciones a la seguridad de las redes sea mayor.

Al no existir métodos de seguridad en el laboratorio de Automatismo de la Facultad de Educación Técnica para el Desarrollo (FET) de la Universidad Católica de Santiago de Guayaquil, ha incidido en que la mayoría de los equipos existentes se encuentren vulnerables a los riesgos de violación a la seguridad, poniendo en riesgo el funcionamiento y la información que en éstos se guarden.

1.1.3. Causas

- Sistema de redes con conexión a Internet.
- Carencia de métodos de prevención y protección de las redes.
- Mayor número de ordenadores interconectados.

1.1.4. Consecuencias

- Riesgo a que el sistema de redes sea atacado por hackers.
- Los sistemas pueden ser alterados y sus datos privados pueden quedar expuestos a personas no autorizadas.
- Poco control de los sistemas de redes debido a la cantidad de equipos conectados entre sí.

1.1.5. Delimitación

Campo: Telecomunicaciones.

Área: Seguridad de redes.

Aspecto: Desarrollo de métodos de prevención y protección de la red del Laboratorio de Automatismo de la facultad Técnica de la UCSG.

Tema: Estudio para determinar los métodos de prevención y protección de la red del Laboratorio de Automatismo de la Facultad Técnica de la UCSG.

Problema: La falta de métodos de prevención y protección de la red del Laboratorio de Automatismo de la Facultad Técnica de la UCSG, provocando fallas y errores cuando los estudiantes al momento de realizar sus prácticas y utilizar las redes.

Delimitación espacial: Guayaquil– Ecuador.

Delimitación temporal: 2014.

1.2. Formulación del problema

¿Cómo analizarla vulnerabilidad de la red del Laboratorio de Automatismo de la Facultad Técnica de la UCSG?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

- Analizar las vulnerabilidades que tiene el Laboratorio de Automatismo de la Facultad Técnica de la UCSG.

1.3.2. Objetivo específicos

- Conocer el funcionamiento de los sistemas que se encuentran instalados en el laboratorio.
- Identificar las debilidades técnicas en los sistemas de la red y establecer prioridades en base a la importancia de los sistemas afectados.
- Reconocer cuáles son los principales métodos de prevención y protección de redes existentes.

1.4. Justificación e importancia de la investigación

En la actualidad el sector tecnológico ha experimentado un desarrollo significativo, lo cual a su vez ha ocasionado la aparición de riesgos informáticos a

los cuales se encuentran expuestos la mayoría de estos sistemas sobre todo cuando existe una gran cantidad de ordenadores conectados entre si o por las conexiones a Internet, las cuales generalmente no incluyen un sistema de protección que sea enteramente confiable.

Por lo tanto, el desarrollo del proyecto se justifica debido a que existe la necesidad de analizar las vulnerabilidades a las cuales se encuentra expuesto el Laboratorio de Automatismo de la Facultad Técnica de la UCSG, de modo que se puedan establecer métodos de prevención y protección que permitan contribuir a reducir estos riesgos a los cuales se encuentra actualmente expuesto y evitar que se presenten daños irreparables al sistema de redes.

Este proyecto también se justifica desde tres puntos de vista: práctico, ya que la misma propone resolver el problema planteado modificando la forma de hacer prácticas en el laboratorio de Automatismo manipulando las redes de una mejor manera, teórico porque esta investigación generará reflexión y discusión tanto sobre el conocimiento existente del área investigada, como dentro del ámbito de las Ciencias de las telecomunicaciones, ya que se aporta información teórica y de conocimientos generales de la materia y metodológico puesto que este proyecto está generando la aplicación de un método analítico de investigación para generar conocimiento válido y confiable dentro del área de esta investigación.

Por otra parte, en cuanto a su alcance, este proyecto abrirá nuevos caminos para otras ideas similares a la que aquí se plantea, sirviendo así al objetivo de análisis, enseñanza y prevención sobre utilidades y beneficios que brindan las redes de telecomunicaciones que actualmente se encuentran instaladas en nuestra institución y ayudara a la formación del estudiante. Así mismo, le permitirá a la autora poner en manifiesto los conocimientos adquiridos durante sus años de estudio y le permitirá contribuir a estudios posteriores que se realicen en base a temas similares.

CAPÍTULO II: MARCO TEÓRICO

2.1. Vulnerabilidad de la red

Según (Areitio, 2008), los siguientes criterios de vulnerabilidad se aplican a todas las redes identificadas y elementos de red en el ámbito de la valoración:

- Alta vulnerabilidad: la vulnerabilidad existe, es probable su explotación, la detección es difícil y la corrección es costosa.
- Vulnerabilidad media: la vulnerabilidad existe, la explotación es posible, la detección es posible y la corrección puede ser costosa.
- Baja vulnerabilidad: la vulnerabilidad existe, es posible su explotación, es posible la detección y los costes de corrección son mínimos. (2008, pág. 80)

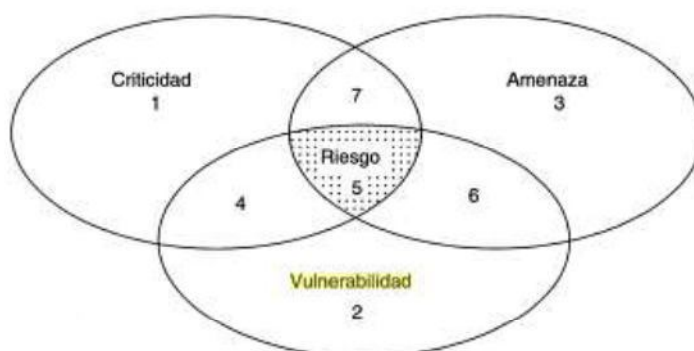


Figura 2. 1 Diagrama de identificación del riesgo de la seguridad

Fuente: (Areitio, 2008)

La evaluación de la vulnerabilidad se define como una mejor estimación de la susceptibilidad de algo al riesgo o daño. Las evaluaciones de vulnerabilidad no son específicas de la seguridad de la TI (tecnología de información) y son utilizados por una amplia gama de otras industrias. Cuando se aplican a la TI se utilizan los estudios de vulnerabilidad de seguridad para evaluar, o proporcionar una mejor estimación de la susceptibilidad de un objetivo a correr un riesgo o daño. A diferencia de las pruebas de penetración, evaluaciones de vulnerabilidad

no validan vulnerabilidades aunque la explotación y por lo que sus informes contienen a menudo son falsos positivos.

La industria de la seguridad informática ha confundido la definición de la evaluación de la vulnerabilidad. En la mayoría de los casos los proveedores de seguridad definen incorrectamente las evaluaciones de vulnerabilidad mediante el uso de las descripciones de la metodología. Esto es un problema, ya que los diferentes proveedores utilizan diferentes metodologías y así la definición parece cambiar entre los vendedores. Lo que es aún un problema más grande es que muchos vendedores confunden evaluaciones de vulnerabilidad con ensayos de penetración, cuando en realidad los dos servicios son completamente diferentes.

Los escáneres de vulnerabilidad de la época de los noventa eran simples puntos y soluciones de tiro a menudo basadas en software de libre acceso en los repositorios de archivos de las universidades. Por lo general, se instalaba el escáner en una estación de trabajo Unix o PC y se escaneaban manualmente redes específicas a nivel local o a través de la WAN. En definitiva, fue un proceso sencillo y rudimentario.

Actualmente con los constantes avances, muchas organizaciones grandes cuentan con miles de servidores de seguridad además de políticas de gran tamaño en cuestión a vulnerabilidad de redes, transmitir información a través mediante la red de una organización a menudo requiere atravesar varios dominios de seguridad y DMZ encadenados. Además de esto, la mayoría de las grandes organizaciones han desplegado balanceadores de carga, tecnologías de optimización WAN, otra aceleración y soluciones de calidad de servicio que desgarran los datos en pedazos y los reconstruyen muchas veces más.

Los escáneres de vulnerabilidad modernos tienden a hacer un buen trabajo de envío de paquetes a través de la red de una manera no intrusiva para perfilar un dispositivo habilitado para IP, estos escáneres utilizan una variedad de técnicas y protocolos para lograr esta tarea Sin embargo, incluso la calidad de servicio y técnicas pueden interferir con los paquetes enviados por el escáner, lo que resulta en corrientes distorsionadas de paquetes de datos.

Las soluciones de calidad de servicio potencialmente pueden descartar paquetes o aminorar su velocidad. Esto a menudo da lugar a tiempos de espera y la mala interpretación de los flujos de datos enviados por el escáner. De manera similar, los equilibradores de carga y dispositivos de optimización WAN pueden crear interacciones casi al azar entre los escáneres y los dispositivos de destino que resulta en imprecisiones adicionales.

Los problemas con las tecnologías de optimización WAN e IPS descritos anteriormente pueden ser identificadas y planificadas para cuando la organización diseña su estrategia de análisis de vulnerabilidades y el despliegue de los escáneres de la red.

Además de los desafíos iniciales de diseño, los procesos de gestión de vulnerabilidad necesitan un par de años en madurar y los ajustes deben hacerse para adaptarse a las cambiantes condiciones de la red.

Pasos para la valoración de vulnerabilidades en redes.

1.- Logística y controles

La logística y los controles son un componente importante, aunque a menudo son pasados por alto en la entrega de pruebas de penetración de calidad . El propósito de este paso es reducir la tasa de falsos positivos y falsos negativos, asegurando que los ajustes adecuados se hagan a todos los módulos de pruebas antes del lanzamiento. Este módulo funciona de forma perpetua durante todo el curso de pruebas. Su propósito es identificar los problemas que puedan existir antes de la prueba, o para identificar la red o el estado del sistema cambia durante la prueba.

2.- Avanzado de Reconocimiento

Todas las evaluaciones de vulnerabilidad comienzan con una combinación de reconocimiento social y técnico.

De reconocimiento social, que no debe confundirse con la ingeniería social, se centra en la extracción de información de sitios web personales, sitios de redes sociales como LinkedIn y Facebook, foros técnicos, salas de Internet Relay Chat, las oportunidades de trabajo de la empresa, los documentos que han sido filtrados o publicados, etc. El objetivo del reconocimiento social es identificar la información que pueda poner en peligro a la meta. Históricamente esta información ha incluido el código fuente, archivos confidenciales, contraseñas, preguntas sobre la solución de problemas de TI, entre otros.

Reconocimiento técnico se centra en el descubrimiento de los ejércitos, las huellas digitales de servicios, análisis de la configuración, la enumeración de directorios del servidor web, la identificación de los portales administrativos, la identificación de los portales de clientes, la identificación de los puntos finales ocultos tales como módems de cable o líneas DLS, el uso de terceros servicios prestados por los proveedores de alojamiento, proveedores de servicios de seguridad gestionados, y mucho más, este puede o no utilizar analizadores de puertos, escáner de aplicaciones web, escáneres de vulnerabilidad, etc., dependiendo de los niveles de amenaza y la intensidad de los servicios que se prestan.

3.- Matriz de Vulnerabilidad

Una vez que las etapas iniciales de reconocimiento son completas comenzamos el proceso de evaluación. Debido a que las evaluaciones de la vulnerabilidad permiten mejor conjetura en cuanto a la susceptibilidad de un objetivo que es atacar o dañar, no se validan vulnerabilidades a través de la explotación. En su lugar, se utiliza un proceso de investigación-peso ligero, para tratar de determinar la validez. Este proceso puede o no puede incluir el uso de la automatización.

Consideraciones de política para la evaluación de la vulnerabilidad

Dependiendo del tamaño y la estructura de la institución, el enfoque de análisis de vulnerabilidades puede ser diferente. Las instituciones pequeñas que tienen un buen conocimiento de los recursos de TI se pueden centralizar el análisis de vulnerabilidades en toda la empresa. Las instituciones más grandes son más

propensas a tener un cierto grado de descentralización, por lo que el análisis de vulnerabilidades podría ser responsabilidad de las unidades individuales. Algunas instituciones pueden tener una mezcla de evaluación de la vulnerabilidad, tanto centralizada como descentralizada. En cualquier caso, antes de iniciar un programa de escaneo de vulnerabilidades, es importante contar con la autoridad para llevar a cabo los análisis y comprender los objetivos que se van a analizar.

Debido a que el sondeo de una red en busca de vulnerabilidades puede alterar los sistemas y exponer datos privados, instituciones de educación superior necesitan una política en el lugar y comprar a partir de la parte superior antes de realizar evaluaciones de la vulnerabilidad. Muchos colegios y universidades abordan esta cuestión en sus políticas de uso aceptable, por lo que el consentimiento para la vulnerabilidad de escanear un estado de conexión a la red. Además, es importante aclarar que el objetivo principal de buscar vulnerabilidades es la defensa contra ataques externos.

También hay una necesidad de aclarar cómo una red de la Universidad se integra con Internet en general. Algunas escuelas tienen clases de direcciones IP que se encuentran dentro del espacio público (IP- wise) y no tienen un firewall perimetral o traducción de direcciones NAT. Estos tipos de entornos abiertos podrían considerar que no tienen en el interior v paradigma exterior.

También hay una necesidad de políticas y directrices éticas para los que tienen acceso a los datos de los análisis de vulnerabilidades. Estas personas tienen que entender la acción apropiada cuando los materiales ilegales se encuentran en su sistema durante el análisis de la vulnerabilidad. La acción apropiada variará entre las instituciones. Algunas organizaciones pueden querer escribir detalles en las políticas, mientras que otros dejan política más abierta a la interpretación y abordar temas específicos a través de procedimientos como la consulta un abogado.

Se debe mantener la conciencia sobre las amenazas y las vulnerabilidades actuales. Muchos de los recursos de alerta y de asesoramiento están disponibles.

Los vendedores suelen notificar a los clientes acerca de las vulnerabilidades a través de las listas de distribución de correo electrónico oa través de la web.

2.2. Tipo de ataques a redes

Clases de ataques pueden incluir el monitoreo pasivo de las comunicaciones, los ataques de redes activas, los ataques de cerca en la explotación por medios internos, y los ataques a través del proveedor de servicios. Los sistemas de información y las redes ofrecen objetivos atractivos y deben ser resistentes al ataque de la gama completa de agentes de amenaza, frente a los piratas a los Estados-nación. Un sistema debe ser capaz de limitar el daño y recuperarse rápidamente cuando se producen ataques. Existen cinco tipos de ataque:

Ataque pasivo

Un ataque pasivo supervisa el tráfico sin cifrar y busca contraseñas en texto y la información sensible que se puede utilizar en otros tipos de ataques. Los ataques pasivos incluyen el análisis del tráfico, la vigilancia de las comunicaciones desprotegidos, al descifrar el tráfico cifrado débil, y la captura de la información de autenticación tales como contraseñas. Intercepción pasiva de operaciones de la red permite a los adversarios para ver los próximos actos. Ataques pasivos tiene como resultado la divulgación de información o archivos de datos a un atacante sin el consentimiento o conocimiento del usuario.

Ataque Activo

En un ataque activo, el atacante intenta eludir o irrumpir en los sistemas garantizados. Esto se puede hacer a través de sigilo, virus, gusanos o troyanos. Ataques activos incluyen intentos de eludir o romper las características de protección, para introducir código malicioso, y para robar o modificar información. Estos ataques están montados sobre un backbone de la red, explotar la información en tránsito, por vía electrónica penetrar un enclave, o atacar a un usuario remoto autorizado durante un intento de conexión a un enclave. Ataques

activos dan lugar a la divulgación o difusión de archivos de datos o la modificación de datos.

Ataque Distribuido

Un ataque distribuido requiere que el adversario introduzca un código, como un caballo de Troya o un programa de puerta trasera, a un componente "de confianza" o software que luego se distribuye a muchas otras empresas y usuarios. Los ataques de distribución se centran en la modificación malintencionada de hardware o software en la fábrica o durante la distribución. Estos ataques presentan códigos maliciosos como una puerta trasera a un producto para obtener acceso no autorizado a información o para una función del sistema en una fecha posterior.

Ataque Insider

Un ataque interno involucra a alguien desde el interior, como un empleado descontento, atacando a los ataques de los ejecutivos de la red puede ser malicioso o no malicioso. *Insiders* maliciosos intencionalmente espiar, robar o dañar información, utilizar la información de manera fraudulenta, o denegar el acceso a otros usuarios autorizados. No hay ataques maliciosos generalmente son el resultado de la negligencia, falta de conocimiento, o la elusión intencional de seguridad por razones tales como la realización de una tarea.

Ataque Primer

Un primer en el ataque involucra a alguien tratando de acercarse físicamente a los componentes de red, datos y sistemas con el fin de aprender más acerca de una red. Los ataques Primer consisten en individuos normales que alcanzan la proximidad física para redes, sistemas o instalaciones con el propósito de modificar, recolección, o denegar el acceso a la información. Muy cercano física se logra mediante la entrada subrepticia en la red, el acceso abierto, o ambos.

Una forma popular de cerca en el ataque es la ingeniería social en un ataque de ingeniería social, el atacante pone en peligro la red o sistema a través de la interacción social con una persona, a través de un mensaje de correo electrónico o por teléfono. Varios trucos se pueden utilizar por el individuo para revelar información acerca de la seguridad de la empresa. La información que la víctima revela que el hacker lo más probable ser utilizado en un ataque posterior para obtener acceso no autorizado a un sistema o red.

Ataque de *phishing*

En ataque de *phishing* que el hacker crea un sitio web falso que se ve exactamente como un sitio popular como *paypal*. La parte de *phishing* del ataque es que el hacker envía un mensaje de correo electrónico que intenta engañar al usuario para que haga clic en un vínculo que lleva a la página web falsa. Cuando el usuario intenta iniciar sesión con su información de la cuenta, el hacker registra el nombre de usuario y contraseña, y luego trata de que la información en el sitio real.

Ataque secuestro

En un ataque de secuestro, un hacker se hace cargo de una sesión entre usted y otra persona y desconecta la otra persona de la comunicación. Usted todavía cree que está hablando con la persona original y puede enviar información privada a los hackers por accidente.

Ataque de la parodia

Ataque de la parodia es un ataque simulado, el hacker modifica la dirección de origen de los paquetes que él o ella está enviando de modo que parecen venir de otra persona. Esto puede ser un intento de eludir las reglas del firewall.

Desbordamiento de búfer

Un ataque de desbordamiento de búfer es cuando el atacante envía más datos a una aplicación de lo que se esperaba. Un ataque de desbordamiento de búfer por

lo general resulta en el atacante obtener acceso administrativo al sistema de comandos.

Exploit ataque

En este tipo de ataque, el atacante sabe de un problema de seguridad dentro de un sistema operativo o una pieza de software y aprovecha ese conocimiento mediante la explotación de la vulnerabilidad.

Ataque Contraseña

Un intruso intenta descifrar las contraseñas almacenadas en una base de datos de cuentas de red o de un archivo protegido por contraseña. Hay tres tipos principales de ataques de contraseña: ataque de diccionario, un ataque de fuerza bruta, y un ataque híbrido. Un ataque de diccionario utiliza un archivo de lista de palabra, que es una lista de contraseñas potenciales. Un ataque de fuerza bruta es cuando el atacante intenta todas las combinaciones posibles de caracteres.

2.3. Seguridad informática

Según (Benchimol, 2011), la seguridad informática es un conjunto de normas de prevención, localización y corrección, dirigidas a proteger la confidencialidad, la integridad y la disponibilidad de los recursos informáticos. (Pág. 12)

La seguridad informática es un vocablo utilizado para dar a entender la seguridad que se tiene con los ordenadores, debido a la vulnerabilidad y algunos riesgos ya que los equipos están conectados por una red. La seguridad informática tiene muchas semejanzas con la seguridad aplicada a otros entornos, ambas tratan de minimizar los riesgos asociados al acceso y el uso de los sistemas de forma no autorizada o malintencionada. La visión de la seguridad informática involucra básicamente la gestión de riesgo, para ello se evalúa y cuantifica los bienes a proteger, en función a los resultados se implantan medidas preventivas y correctivas que eliminen los posibles riesgos o que los reduzcan a niveles manejables.

Básicamente la seguridad informática se enfoca en proteger la infraestructura computacional y todo lo que se relacione a esta, especialmente la información contenida o circulante. Comprende software, hardware y todo lo que signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose en información privilegiada. La seguridad informática se encarga de diseñar las normas, procedimientos, métodos y técnicas destinadas a que la información este segura y confiable.

- **Confidencialidad:**

Según (Sánchez, 2003), la confidencialidad es la asistencia de protección para que los datos no estén utilizables para usuarios no autorizados. También se la conoce como secreto o privacidad, es la capacidad del método para impedir que usuarios no autorizados accedan a los datos guardados en él. (pág. 101)

La confidencialidad es una cualidad que posee un documento o archivo para que sea comprendido o leído por la persona o sistema que esté autorizado, es así como se le denomina a un documento, entiéndase archivo o mensaje, que es confidencial porque solo es comprendido por la persona o entidad a quien va dirigida o este autorizada. Para garantizar la confidencialidad se utiliza un mecanismo de cifrado y de ocultación de la comunicación, digitalmente se puede mantener seguro un documento con el uso de una llave asimétrica.

- **Integridad:**

En (PARANINFO, 2011)se indica que la integridad de los datos es la garantía de la exactitud de la información, asegurando que los datos estarán completos y sin errores. (pág. 10)

La integridad es la condición que tiene un archivo o documento que no ha sido alterado y que además se puede probar que no ha sufrido alguna manipulación, aplicando esta idea en la base de datos seria la correspondencia entre los datos y los hechos que refleja. Resumiendo en una frase lo que significa la integridad en

la información se puede decir que la información no debe perderse o alterarse, ni los servicios.

Fundamentalmente la integridad busca mantener los datos libres de modificaciones no autorizadas, se considera violación de la integridad cuando un empleado, programa o proceso por accidente o malintencionado modifica o borra datos importantes que son parte de la información. La integridad en un mensaje se logra adjuntando con otro conjunto de datos de comprobación de la integridad, es decir con la firma digital.

- **Disponibilidad:**

Según (Pacheco & Jara, 2009), la disponibilidad avala que las técnicas del método y los datos estén utilizables solo para personas autorizadas cuando los requieran. (pág. 19) Se entiende por disponibilidad es acceso que tienen las personas autorizadas que acceden a tiempo a la información, si no se dispone de la información dentro de un tiempo determinado esto equivale a la falta de disponibilidad. Certificar la disponibilidad involucra además la prevención de ataque de denegación de servicio, la disponibilidad es importante en el proceso de información, es variada en el sentido que existen varios mecanismos para cumplir con los niveles de servicio que se requiera. Una excepción a esta regla son los sistemas operativos de escritorio que se han convertido en lo más común entre las computadoras personales.

- **No repudio:**

De acuerdo a (Gómez J. , 2009), se brinda protección a un usuario ante otro que después niega que se efectuó una comunicación. El no repudio de origen resguarda al receptor de que el emisor niegue haber enviado el mensaje y el no repudio de recepción salvaguarda al emisor de que el receptor niegue haber recibido el mensaje. Las firmas digitales son el mecanismo más usado para esto. (pág. 1)

Protege a un usuario frente a otro usuario que después niegue la realización de la comunicación, la protección es respaldada por evidencias irrefutables que

permitan dar la resolución de cualquier disputa. El no repudio de origen protege al receptor del emisor, en el caso de que el emisor niegue haber enviado el mensaje, el no repudio de recepción protege al emisor del receptor, en caso de que este último niegue haber recibido el mensaje. Las firmas digitales son de mucha ayuda en este proceso. Se puede decir que el respaldo del no repudio son las firmas que aseguran que esta corresponde realmente a su propietario, así de controlar que el mensaje llega al receptor es en verdad el que se envió.

- **Controles de acceso del sistema:**

Permite asegurar que los usuarios no autorizados no puedan acceder al sistema, y crea conciencia en los usuarios autorizados en la seguridad, como es el caso del cambio de contraseñas en una base regular. El sistema protege los datos de contraseñas y hace un seguimiento de quien está haciendo uso del sistema sobre todo si se relaciona con la seguridad. (Sommerville, Ingeniería del software, 2005, pág. 54) Realiza un cuadro en el cual se titula terminología sobre protección:

Tabla 2. 1 Controles de acceso del sistema

Fuente: Elaboración propia

Término	Descripción
Exposición	Posible pérdida o daño en un sistema informático. Un ejemplo puede ser la pérdida o daño de los datos o la pérdida de tiempo y esfuerzo si es necesaria una recuperación del sistema después de una violación de protección.
Vulnerabilidad	Debilidad en un sistema informático que se puede aprovechar para provocar pérdidas o daños.
Ataque	Aprovechamiento de la vulnerabilidad de un sistema. Generalmente, se produce desde fuera del sistema y con una intención deliberada de causar algún daño.
Amenazas	Circunstancias que potencialmente pueden provocar pérdidas o daños. Se pueden entender como una vulnerabilidad del sistema que está expuesto a un ataque.
Control	Medida de protección que reduce la vulnerabilidad del sistema. La encriptación podría ser un ejemplo de un control que reduce una vulnerabilidad de un sistema de control de acceso deficiente.

- **Controles de acceso a datos:**

Por medio del monitoreo de quien puede suscribir a que datos y con qué intención, el sistema de seguridad puede aceptar inspecciones de acceso facultativo, con ellos, ayuda a establecer si otras personas pueden leer o cambiar sus fichas. El método también podría afirmar las inspecciones de acceso necesario, con ellos el medio fija las reglas de acceso basados en los niveles de seguridad de las personas, los registros, y los otros objetos en el sistema.

- **Administración de Sistemas de Seguridad:**

El objetivo es lograr exactitud, integridad y protección de los procesos y recursos de los sistemas de información, de esta manera se busca minimizar los errores, fraudes y pérdidas en los sistemas de información que se interconectan a las empresas actuales, así como sus clientes, proveedores y otras partes interesadas. Al realizar la conexión permite hacer o deshacer un sistema seguro que sirve para delinear claramente las responsabilidades de administrador del sistema.

- **Diseño de sistemas:**

Ciertas empresas aprovechando las capacidades básicas del hardware y características e software de seguridad, por ejemplo suelen emplear arquitectura de sistema que es capaz de utilizar un segmento de memoria, aislando así los procesos privilegiados y los no privilegiados.

2.4. Delitos informáticos

Con respecto a este tema, (Del Peso, 2001) indica que la acción culpable efectuada por una persona, que produzca un daño a otros aunque no se beneficie el autor o si causa un bien ilegal a este, aunque no perjudique de forma directa o indirecta a la víctima, que se realiza en el medio informático y es sancionado. (pág. 162)

El delito informático no solo se lo encuentra en los hechos punibles, también en los actos que dan lugar a responsabilidad penal o civil, el delito informático es un acto que produce daños e involucra sistemas informáticos realizados con malicia, constituye fraude informático y genera responsabilidad.

Las consecuencias de las amenazas varían considerablemente: algunos les afecta confidencialidad o en la integridad de los datos, mientras que a otros les afecta en la disponibilidad del sistema. Los sistemas informáticos suelen ser explotados tanto para el fraude y el robo, los delitos son realizados mediante métodos tradicionales de fraude y mediante el uso de nuevos métodos.

Por ejemplo, una persona para realizar un robo lo realiza desde su ordenador y sustrae pequeñas cantidades de dinero de varios números de cuentas financieras, sin embargo los sistemas financieros no son los únicos amenazados. También se considera delito informático a los delitos no monetarios, como la creación y distribución de virus a través de web o dar a conocer información condicional, robo de identidad, el acecho, el acoso y el terrorismo.

La forma más conocida de la delincuencia informática implica el hacking, la práctica de irrumpir en las redes de ordenadores privados. Los hackers pueden acceder a grandes cantidades de información privada en poblaciones enteras. A veces esta información es utilizada para el robo de identidad, en otras ocasiones, simplemente filtran la información a los sitios públicos, donde otros delincuentes la pueden explotar. Incluso a veces los gobiernos son sospechosos de piratería de los sitios de empresas o de otras naciones, una práctica llamada guerra cibernética.

El robo de identidad implica la utilización de un ordenador y conexión a un software especialmente desarrollado para robar identidades, tarjetas de crédito, números u otros datos que el criminal pueda utilizar para su ventaja. Utilizando los datos obtenidos ilegalmente, el criminal puede abrir cuentas, cargar una amplia gama de bienes y servicios, y abandonar las cuentas, esto deja a la víctima en la posición de tener que hacer frente a las enormes deudas que él o ella no se generan.

Según García y Alegre (2011) el móvil del delito informático es diverso, desde destruir la información que contiene un sistema informático, colapsar la red, e incluso cualquier delito de los conocidos habitualmente, como puede ser robo, chantaje, fraude, falsificación o incluso algunos que se han visto incrementados con el desarrollo de Internet.⁵⁹ (Pág. 136)

Una de las categorías de delitos informáticos es el de delitos cibernéticos contra todas las formas de propiedad. Estos crímenes incluyen vandalismo informático o la destrucción de la propiedad ajena, la transmisión de programas dañinos.

Los delitos cibernéticos cometidos contra personas incluyen diversos delitos como la transmisión de pornografía infantil, el acoso a cualquier persona con el uso de un ordenador, como el correo electrónico. El tráfico, la distribución, publicación y difusión de material obsceno incluida la pornografía y la exposición indecente, constituye uno de los delitos cibernéticos conocidos más importantes en la actualidad.

Los delitos informáticos cometidos contra el gobierno incluyen el cyber terrorismo es una especie distinta de la delincuencia en esta categoría. El crecimiento de internet ha demostrado que el medio del ciberespacio está siendo utilizado por los individuos y los grupos para amenazar a los gobiernos internacionales como también para aterrorizar a los ciudadanos de un país.

El espionaje industrial también es un delito informático, ya que se refiere al acto de recogida de datos de propiedad de empresas privadas o el gobierno con el propósito de ayudar a otra empresa. El espionaje industrial puede ser perpetrado por empresas que buscan mejorar su ventaja competitiva o por gobiernos que buscan ayudar a sus industrias nacionales. El espionaje industrial extranjero llevado a cabo por un gobierno se refiere a menudo como el espionaje económico, dado que la información es procesada y almacenada en los sistemas informáticos, la seguridad informática puede ayudar a proteger contra estas amenazas.

El chantaje es un acto ilegal que ha sido un problema desde hace varios años, el cual ha dado un nuevo giro en la era moderna, ya que el chantajista puede amenazar con revelar información perjudicial o vergonzosa a través de Internet o una red privada si la víctima no cumple con las exigencias de los criminales. Un delito cibernético de este tipo puede ir tan lejos como tener los fondos de transferencia de las víctimas a una cuenta bancaria imposible de rastrear

utilizando algún tipo de programa de pago en línea, aprovechando así al máximo la tecnología moderna para cometer el crimen.

Además los delitos informáticos incluyen todo tipo de virus informáticos, los cuales son programas diseñados para introducirse en la computadora de un usuario, propagarse a otros ordenadores. Algunos virus son llamados spyware, ya que envían la información privada del usuario a otra ubicación. Incluso existen anuncios o programas que pretenden detectar un virus inexistente en la computadora de un usuario, y a continuación, dirigen al usuario a un sitio o programa en donde en realidad contiene un virus.

La piratería es otro delito informático lo que ha causado grandes pérdidas económicas a aquellas empresas dedicadas a la elaboración de software, ya que la piratería es una violación a la propiedad intelectual de estas empresas. La piratería de software, involucra que una persona obtenga de forma ilegal software, y lo emplee ya sea para uso personal o para obtener ganancias con la venta del mismo.

El fraude es diferente del robo porque la víctima voluntariamente entrega el dinero a los criminales, al desconocer el hecho de que el delincuente tergiversó los bienes o su oferta. El fraude también es parte de los delitos informáticos, aparte de estafas directas, el fraude puede incluir actos como la modificación de datos para obtener un beneficio.

El lavado de dinero, es otro delito informático donde los delincuentes abren cuentas bancarias legítimas a la apariencia legítima de negocios que en realidad son frentes de lavado de dinero. Cientos de miles de dólares son depositados en estas cuentas con frecuencia y días o semanas más tarde transferidos a otras cuentas, sin ningún propósito obvio, que asciende a millones de dólares lavados en unos pocos meses.

Al haber grandes cantidades de información personal disponibles en internet, sobre todo desde el auge de las redes sociales. Los delincuentes a veces aprovechan esta información para acechar o acosar a las personas. La explotación infantil es un ejemplo de esto, otros usos criminales de redes sociales incluyen el *cyberbullying* o incluso asesinato por encargo, cualquier caso sospechoso de delito

informático debe ser inmediatamente reportado a una agencia de aplicación de la ley y para los administradores de la red informática relacionados.

Últimamente organismos de seguridad estiman que puede surgir nuevos métodos de delincuencia, algunos de ellos como el asesinato a través de dispositivos conectados a la red, ya que pueden ser hackeado, lo cual es algo preocupante. Estas nuevas amenazas incluyen la utilización de dispositivos conectados a Internet para llevar a cabo crímenes de realidad física.

En la actualidad, con casi todos los dispositivos, de la asistencia sanitaria al transporte, siendo controlado o comunicarse de algún modo con a través de Internet, algunos criminales aprovechar esto para llevar a cabo asesinatos. Los ejemplos incluyen un marcapasos que puede ajustarse a distancia, un coche conectado a Internet que puede tener sus sistemas de control alterado, o un goteo intravenoso que se puede cerrar con un clic.

2.5. Base conceptual

Amenazas: (Sommerville, Ingeniería del software, 2008, pág. 54), “Circunstancias que potencialmente pueden provocar pérdidas o daños. Se puede entender como una vulnerabilidad del sistema que está expuesto a un ataque”

Ataque: (Sommerville, Ingeniería del software, 2008, pág. 54), “Aprovechamiento de la vulnerabilidad de un sistema. Generalmente, se produce desde fuera del sistema y con una intención deliberada de causar algún daño”.

Control: (Sommerville, Ingeniería del software, 2008, pág. 54), “Medida de protección que reduce la vulnerabilidad del sistema”.

Exposición: (Sommerville, Ingeniería del software, 2008, pág. 54), “Posible pérdida o daño en un sistema informático”.

Vulnerabilidad: (Sommerville, Ingeniería del software, 2008, pág. 54), “Debilidad en un sistema informático que se pueda aprovechar para provocar pérdidas o daños”.

2.6. Hipótesis

La hipótesis se establece de la siguiente forma: Si se analiza la vulnerabilidad de la red del Laboratorio de Automatismo de la Facultad Técnica de la UCSG, entonces se podrán diseñar y recomendar métodos de prevención y protección que contribuyan a corregir errores y minimizar los riesgos a los cuales se encuentra expuesto el sistema.

CAPÍTULO III: MARCO METODOLÓGICO

3.1. Tipo de investigación

Considerando la definición de Best (2008, pág. 91), la investigación descriptiva refiere minuciosamente e interpreta *lo que es*. Está relacionada a condiciones o conexiones existentes; prácticas que prevalecen, opiniones, puntos de vista o actitudes que se mantienen; procesos en marcha; efectos que se sienten o tendencias que se desarrollan.

En lo que se refiere al tipo de investigación, se determina la utilización de una investigación descriptiva, ya que es la que más se ajusta a los objetivos de investigación definidos por la autora. A través de la investigación descriptiva no solo se podrá analizar el funcionamiento actual de los sistemas del Laboratorio de Automatismo de la Facultad Técnica de la UCSG, sino que además se podrá conocer la percepción de estudiantes y docentes con respecto a los fallos en el sistema y la vulnerabilidad que presenta, lo cual permitirá obtener la información necesaria para plantear una propuesta que permita contribuir a dar una solución al problema encontrado.

Además, se determina que la investigación descriptiva será de corte transversal, debido a que se desarrollará en un lugar determinado, es decir, en el Laboratorio de Automatismo de la Facultad Técnica de la UCSG, y concluyente considerando que la información que se obtenga permitirá a la autora llegar a conclusiones en base al problema de vulnerabilidad en el laboratorio.

3.2. Diseño de la investigación

En lo que respecta al diseño de la investigación, se considera la aplicación de una investigación cuali-cuantitativa, la cual referenciando lo que definen Dávila, et al (2008, pág. 137), investigación cualitativa permite la obtención de información en base a la percepción de los involucrados; mientras que la investigación cuantitativa se define como una “Metodología de investigación Metodología de

investigación que busca cuantificar los datos y, en general, aplicar alguna forma de análisis estadístico”.

Se determina la aplicación de un diseño de investigación cuali-cuantitativa, ya que permite expresar de manera estadística los resultados obtenidos del análisis, en base a esto se podrá conocer el porcentaje de vulnerabilidad en la que se encuentra el sistema del Laboratorio de Automatismo de la Facultad Técnica de la UCSG, e identificar la percepción de los involucrados en cuanto a la necesidad de la implementación de métodos de seguridad para el sistema. Además de la aplicación de este diseño cuali-cuantitativo, se determina que la investigación que se realizará será de campo, ya que es necesario que la información se obtenga de manera directa en el lugar de estudio.

3.3. Población y Muestra

3.3.1. Población

Para el desarrollo del estudio, será necesario que se considere como población a los estudiantes de la Facultad Técnica de la UCSG, puesto que son quienes hacen uso del Laboratorio de Automatismo y consecuentemente son quienes conocen acerca de los fallos presentados. Además, se considerará a los responsables del Laboratorio de Automatismo para el desarrollo de la investigación cualitativa. La población según datos obtenidos de la Facultad de Educación Técnica para el Desarrollo de la UCSG (2013), está constituida por 480 estudiantes de la facultad, mientras que los responsables del laboratorio son 4 docentes.

3.3.2. Muestra

Según lo determina Gómez (2008, pág. 111), “La muestra debe ser, en esencia, un subgrupo representativo de la población. Es un subconjunto de elementos que pertenecen a ese conjunto definido por sus características al que llamamos población”.

En este caso, para la selección de la muestra para el estudio cuantitativo será necesario de la aplicación de la fórmula para población finita, mientras para el desarrollo de la investigación cualitativa se considerará la población en su totalidad, puesto que es menor a 100 personas. Se determina además que el tipo de muestra será no probabilística, puesto que se considerarán sólo a los estudiantes y responsables del laboratorio de la Facultad de Educación Técnica para el Desarrollo de la UCSG. A continuación se desarrollará el cálculo de la muestra para el estudio cuantitativo:

$$n = \frac{z^2 * P * Q}{E^2}$$

Z = Valor normal

E = Error

P = Proporción

Q = 1-P

n= 214

Es preciso realizar 214 encuestas.

3.4. Técnicas e instrumentos de investigación

Para Reza (2008, pág. 293), “Una técnica de investigación consiste en cómo se realiza la recopilación de la información y cómo se necesita que ésta sea recopilada”.

Para el desarrollo de la investigación cuali-cuantitativa, será necesaria la aplicación de la encuesta, la entrevista y la observación como técnicas de investigación; en cuanto a la encuesta permitirá recopilar la información y presentarla de manera cuantitativa, para lo cual se aplicará el cuestionario como instrumento de investigación; mientras que en el caso de las entrevistas, se realizará para la obtención de la información cualitativa y consecuentemente será necesaria la aplicación del guion como instrumento de investigación.

3.5. Recolección de la información

En lo que se refiere a la recolección de la información, se determina el desarrollo de la recopilación de datos de manera presencial, es decir, se realizará face to face in situ, para lo cual la autora deberá acudir a la facultad y particularmente al Laboratorio de Automatismo para realizar la investigación correspondiente.

3.6. Procesamiento de los datos y análisis

El procesamiento de los datos cuantitativos se realizará a través de la herramienta de Microsoft Excel, puesto que, esta herramienta proporciona mayores facilidades para la tabulación de los datos y para presentarlos de manera estadística a través de gráficos. La información que se obtenga tanto de la investigación cuantitativa y la información cualitativa serán debidamente analizadas.

3.7. Operacionalización de las variables

En la tabla 3.1 se presentan los datos correspondientes a la operacionalización de las variables.

Tabla 3. 1 Operacionalización de las variables

Elaborado por: Mayra Victoria Herrera

Variable	Tipo de Variable	Dimensión	Indicadores
Análisis de la vulnerabilidad del Laboratorio de Automatismo de la Facultad Técnica de la UCSG	Independiente	Análisis del mercado	100% desarrollado el análisis
Métodos de prevención y protección	Dependiente	Diseño de métodos de prevención y protección de redes	100% diseñada la propuesta

CAPÍTULO IV

4. ANÁLISIS E INTERPRETACIÓN DE LOS DATOS

4.1. Encuestas

1. ¿Disponer de una red del laboratorio de automatismo interna en la facultad técnica de la UCSG, le resulta?

Tabla 4. 1 Acogida de la red

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

	FRECUENCIA ABSOLUTA.	FREC. ABS. ACUMULADA	FRECUENCIA RELATIVA	FRECUENCIA REL. ACUMULADA
MUY IMPORTANTE	153	153	71%	71%
IMPORTANTE	61	214	29%	100%
NADA IMPORTANTE	0	214	0%	100%
TOTAL	214		100%	

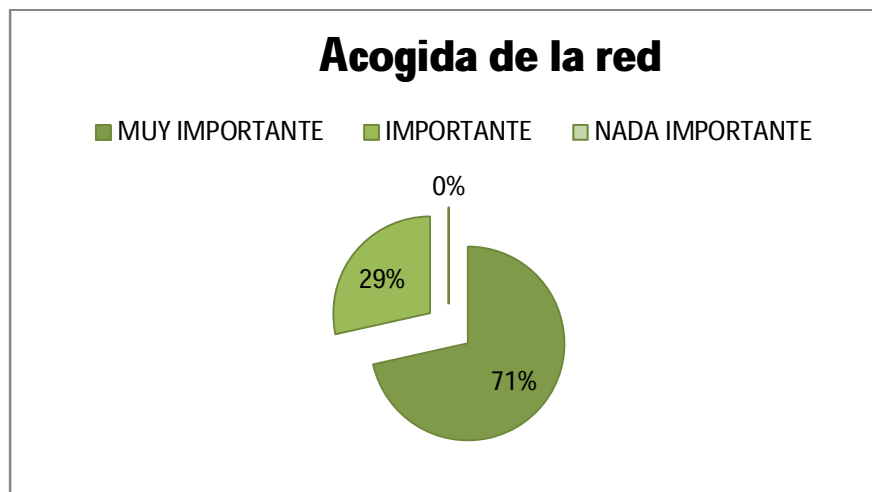


Figura 4. 1 Acogida de la red

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

Según la encuesta efectuada a los estudiantes de la Facultad Técnica de la UCSG, sobre qué les parece disponer de una red en el laboratorio de automatismo respondieron lo siguiente: el 71% dijo muy importante; el 29% dijo que les parece

importante. Por ello, según la encuesta, el disponer de una red en el laboratorio de automatismo es de suma importancia para su carrera.

2. ¿Le han proporcionado la suficiente información sobre esta red del laboratorio de automatismo?

Tabla 4. 2 Información brindada sobre la red

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

	FRECUENCIA ABSOLUTA.	FREC. ABS. ACUMULADA	FRECUENCIA RELATIVA	FRECUENCIA REL. ACUMULADA
TOTALMENTE DE ACUERDO	131	131	61%	61%
DE ACUERDO	71	202	33%	94%
NI DE ACUERDO NI EN DESACUERDO	8	210	4%	98%
EN DESACUERDO	4	214	2%	100%
TOTAL DESACUERDO	0		0%	100%
TOTAL	214		100%	

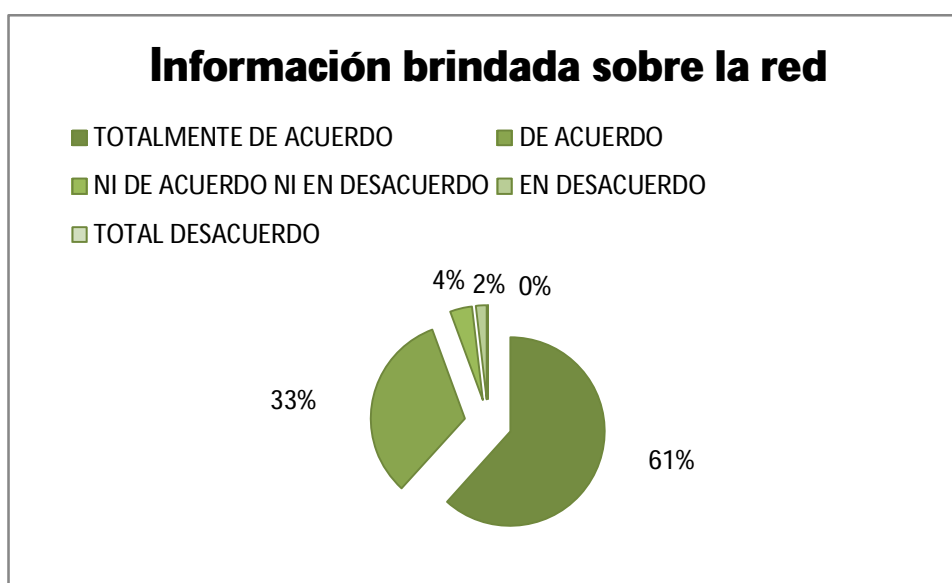


Figura 4. 2 Información brindada sobre la red

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

Según la encuesta efectuada a los estudiantes de la Facultad Técnica de la UCSG, en cuanto si han recibido la suficiente información sobre la red del laboratorio de automatismo respondieron: el 61% dijo totalmente de acuerdo; el 33% dijo de acuerdo; el 4% ni de acuerdo ni en desacuerdo. Por lo tanto en base a los

resultados obtenidos, si les han informado a los estudiantes sobre la red en el laboratorio de automatismo.

3. ¿Quién le ha brindado información sobre esta red del laboratorio de automatismo?

Tabla 4. 3 Información brindada por:

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

	FRECUENCIA ABSOLUTA.	FREC. ABS. ACUMULADA	FRECUENCIA RELATIVA	FRECUENCIA REL. ACUMULADA
PROFESORES	173	173	81%	81%
COMPAÑEROS	15	188	7%	88%
TÉCNICOS EN REDES	17	205	8%	96%
OTROS	9	214	4%	100%
TOTAL	214		100%	

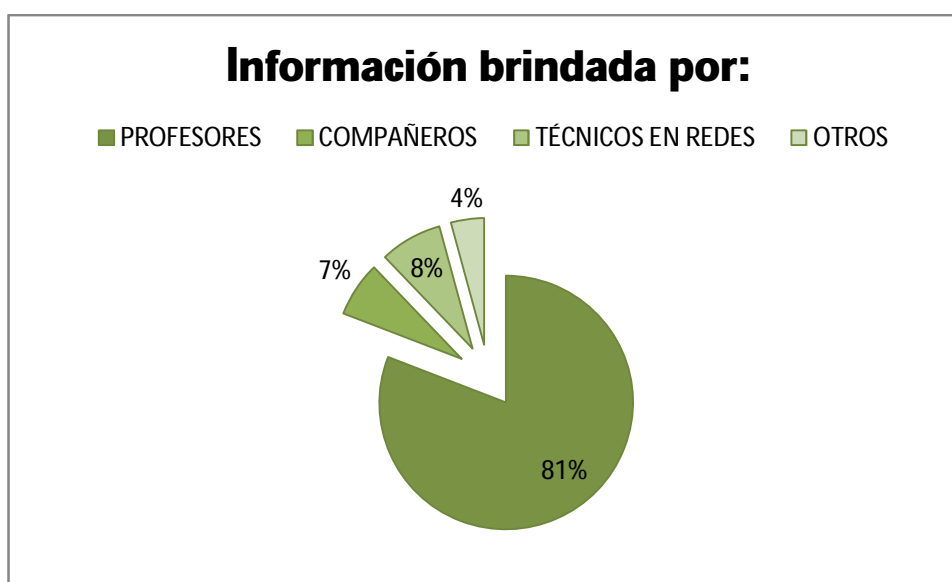


Figura 4. 3 Información brindada por:

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

Según la encuesta practicada a los estudiantes de la Facultad Técnica de la UCSG, sobre quién o quiénes les han informado sobre la red en el laboratorio de automatismo respondieron: el 81% indicó que los profesores, mientras que el 8% mencionó a técnicos en redes de la facultad, y el 7% mencionó que los mismos compañeros. Por ello en base a los resultados, los profesores son quiénes ofrecen la información a los alumnos acerca de la red en el laboratorio de automatismo.

4. ¿Conoce a cabalidad sobre el funcionamiento de esta red?

Tabla 4. 4 Conoce cómo funciona la red

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

	FRECUENCIA ABSOLUTA.	FREC. ABS. ACUMULADA	FRECUENCIA RELATIVA	FRECUENCIA REL. ACUMULADA
SI	209	209	98%	98%
NO	5	214	2%	100%
NO SABE	0	214	0%	100%
NO RESPONDE	0	214	0%	100%
TOTAL	214		100%	



Figura 4. 4 Conoce cómo funciona la red

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

Según la encuesta practicada a los estudiantes de la Facultad Técnica de la UCSG, sobre si conocen a cabalidad el funcionamiento de la red en el laboratorio de automatismo respondieron lo siguiente: el 98% dijo sí; el 2% dijo que no. Por ello es claro observar que la mayoría de los estudiantes conocen el funcionamiento de esta red en el laboratorio de automatismo, en cuanto a ese 2% que no conoce muy

bien el funcionamiento de la misma, será importante que se les imparta la información de esta red.

5. ¿Frecuencia en que tiene acceso a la red del laboratorio de automatismo?

Tabla 4. 5 Uso la red del laboratorio

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

	FRECUENCIA ABSOLUTA.	FREC. ABS. ACUMULADA	FRECUENCIA RELATIVA	FRECUENCIA REL. ACUMULADA
DIARIAMENTE	172	172	80%	80%
SEMANALMENTE	28	200	13%	93%
QUINCENALMENTE	12	212	6%	99%
MENSUALMENTE	2	214	1%	100%
TOTAL	214		100%	

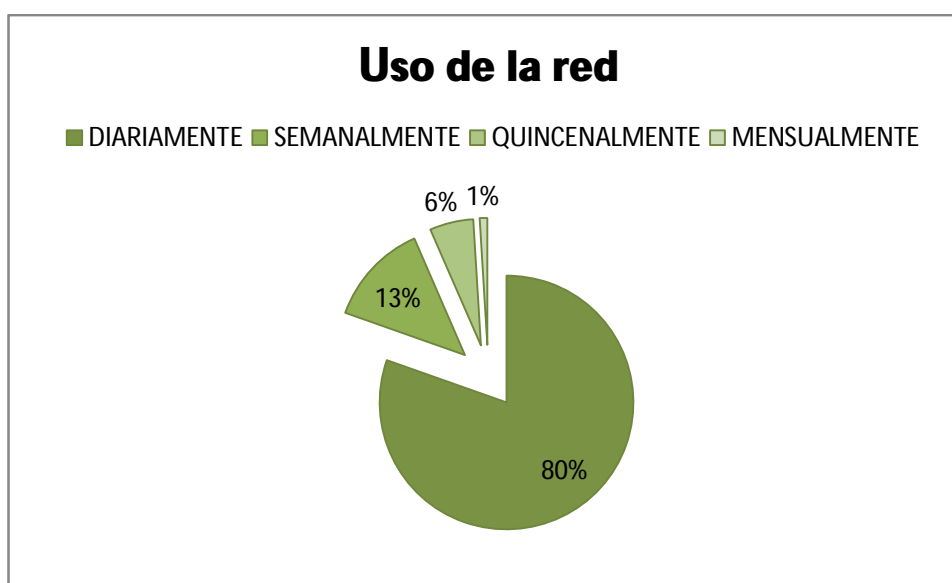


Figura 4. 5 Uso de la red del laboratorio

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

Según la encuesta practicada a los estudiantes de la Facultad Técnica de la UCSG, sobre las veces que utiliza la red del laboratorio de automatismo, respondieron lo siguiente: el 80% dijo diariamente; el 13 mencionó semanalmente, apenas el 6% dejo quincenal, y un 1% dijo q usaba esta red mensualmente. Por ello el índice de

uso de la red del laboratorio de automatismo es usada diariamente por los estudiantes.

6. ¿Se ha percatado de cuantas máquinas se encuentra conectadas a esta red?

Tabla 4. 6 Máquinas conectadas a la red

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

	FRECUENCIA ABSOLUTA.	FREC. ABS. ACUMULADA	FRECUENCIA RELATIVA	FRECUENCIA REL. ACUMULADA
SI	156	156	73%	73%
NO	36	192	17%	90%
NO SABE	13	205	6%	96%
NO RESPONDE	9	214	4%	100%
TOTAL	214		100%	

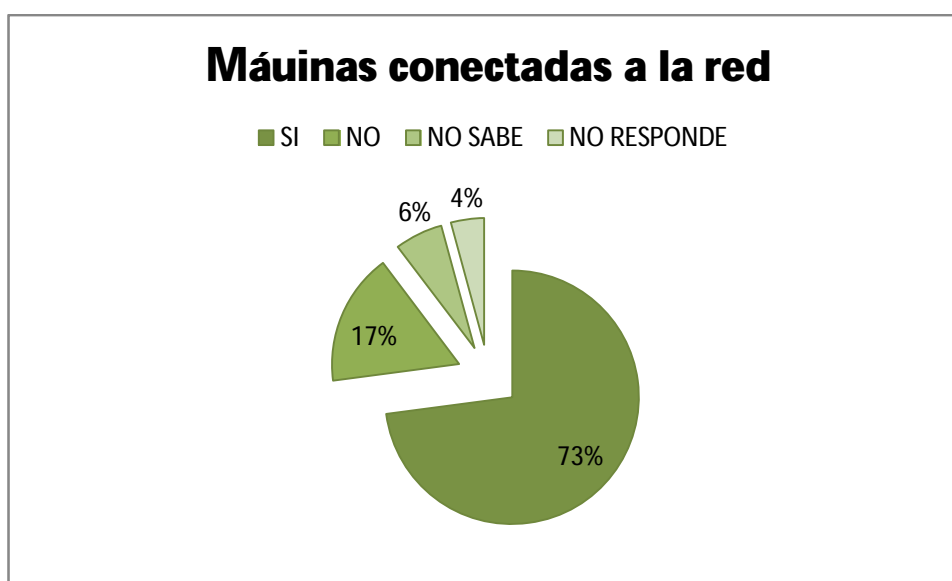


Figura 4. 6 Máquinas conectadas a la red

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

Según la encuesta efectuada a los estudiantes de la Facultad Técnica de la UCSG, respecto a si conoce el número de computadoras conectadas a esta red, respondieron lo siguiente: el 73% dijo si, apenas el 4% no respondió: Por lo tanto

en base a las encuestas, la mayoría de los estudiantes conocen cuantas máquinas están conectadas a la red del laboratorio de automatismo.

7. ¿Quiénes hacen uso de la red del laboratorio de automatismo?

Tabla 4. 7 Quiénes usa el laboratorio

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

	FRECUENCIA ABSOLUTA.	FREC. ABS. ACUMULADA	FRECUENCIA RELATIVA	FRECUENCIA REL. ACUMULADA
ALUMNOS Y PROFESORES DE LA FACULTAD TÉCNICA	208	208	97%	97%
ALUMNOS Y PROFESORES DE OTRAS FACULTADES DE LA UCSG	6	214	3%	100%
DIRECTIVOS DE LA UCSG	0	214	0%	100%
TOTAL	214		100%	

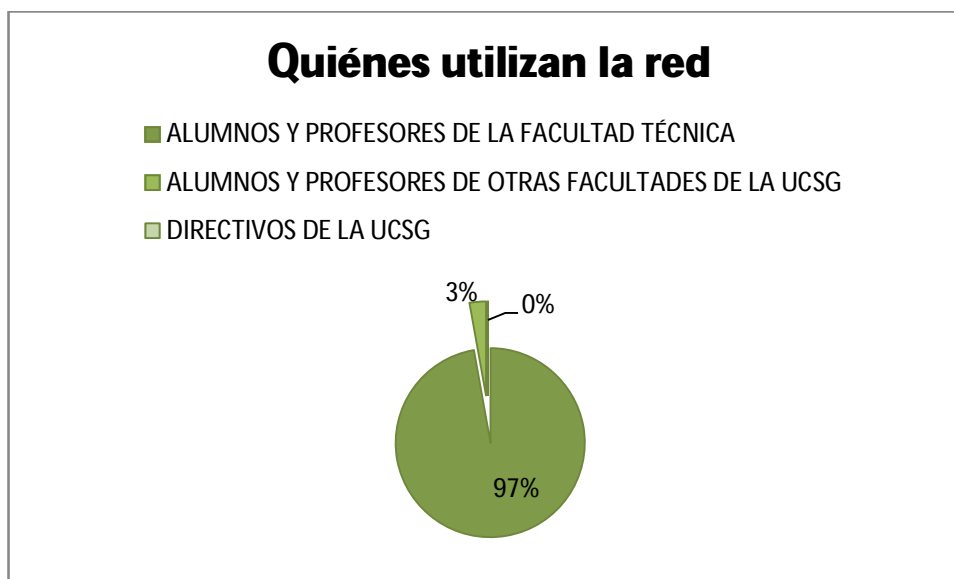


Figura 4. 7 Quiénes utilizan la red

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

Según la encuesta efectuada a los estudiantes de la Facultad Técnica de la UCSG, sobre quiénes utilizan la red del laboratorio de automatismo, respondieron lo siguiente; el 97% mencionó que solo los alumnos y profesores de la facultad, mientras que el 3% dijo que también usan esta red, alumnos y profesores de otras

facultades. Por lo tanto quiénes hacen uso exclusivo de esta red, son los estudiantes y maestros de la facultad técnica de la UCSG.

8. En cuanto a la seguridad de esta red ¿Existen políticas que permitan hacer uso la red del laboratorio de automatismo?

Tabla 4. 8 Políticas de seguridad

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

	FRECUENCIA ABSOLUTA.	FREC. ABS. ACUMULADA	FRECUENCIA RELATIVA	FRECUENCIA REL. ACUMULADA
SI	5	5	2%	2%
NO	205	210	96%	98%
NO SABE	3	213	1%	100%
NO RESPONDE	1	214	0%	100%
TOTAL	214		100%	

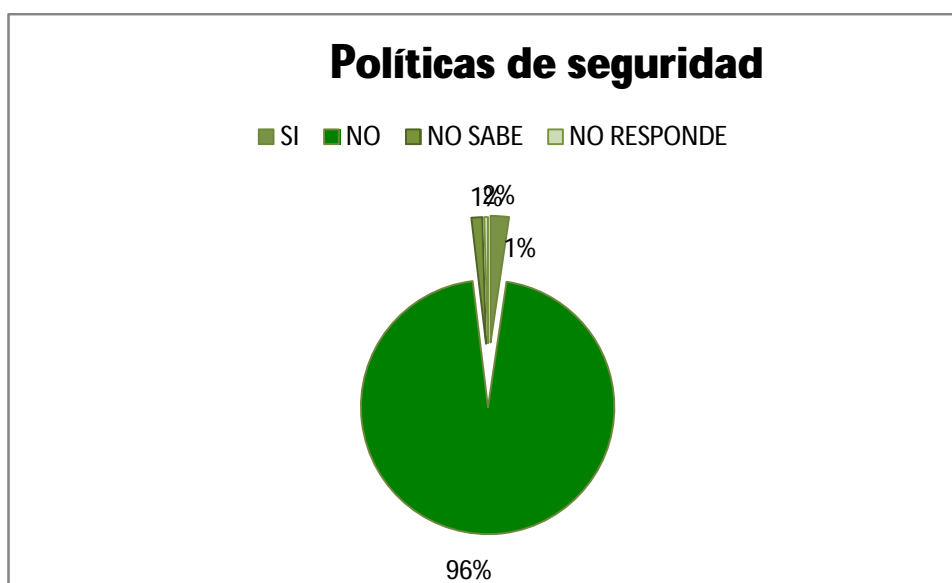


Figura 4. 8 Políticas de seguridad

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

Según la encuesta efectuada a los estudiantes de la Facultad Técnica de la UCSG, respecto a si existen políticas que permitan hacer uso de la red del laboratorio de automatismo, respondieron lo siguiente: El 96% dijo no, mientras que el 2%

respondió sí, y apenas un 1% no sabe si se aplican políticas para usar esta red. Por lo tanto, según los resultados no existen políticas que permitan hacer uso de la red del laboratorio del automatismo.

9. ¿El contar con un sistema de alta seguridad para proteger esta red le resulta?

Tabla 4. 9 Sistema de seguridad para la red

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

	FRECUENCIA ABSOLUTA.	FREC. ABS. ACUMULADA	FRECUENCIA RELATIVA	FRECUENCIA REL. ACUMULADA
MUY IMPORTANTE	149	149	70%	70%
IMPORTANTE	65	214	30%	100%
NADA IMPORTANTE	0	428	0%	100%
TOTAL	214		100%	

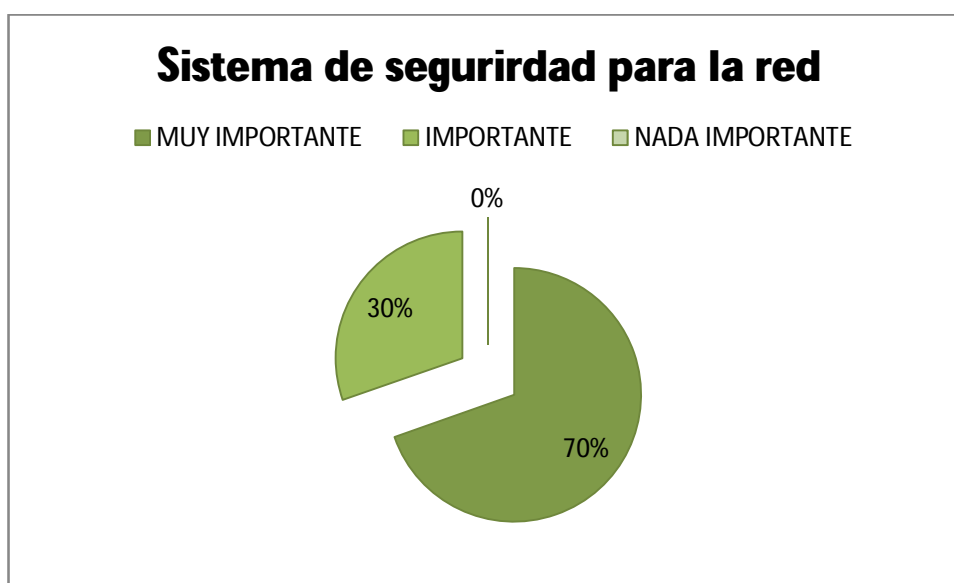


Figura 4. 9 Sistema de seguridad para la red

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

Según la encuesta efectuada a los estudiantes de la Facultad Técnica de la UCSG, sobre qué le parece contar con un sistema de seguridad para proteger esta red, respondieron lo siguiente: el 70% dijo muy importante; el 30% le parece

importante. Por ello, es claro ver en los resultados que para los estudiantes de muy importante que esta red tenga un sistema de alta seguridad.

10. ¿La red del laboratorio de automatismo de la Facultad Técnica, cuenta con un sistema de alta seguridad?

Tabla 4. 10 Sistema de alta seguridad

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

	FRECUENCIA ABSOLUTA.	FREC. ABS. ACUMULADA	FRECUENCIA RELATIVA	FRECUENCIA REL. ACUMULADA
SI	48	48	22%	22%
NO	51	99	24%	46%
NO SABE	109	208	51%	97%
NO RESPONDE	6	214	3%	100%
TOTAL	214		100%	



Figura 4. 10 Sistema de alta seguridad

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

Según la encuesta efectuada a los estudiantes de la facultad técnica de la UCSG, respecto a si la red del laboratorio de automatismo cuenta con un sistema de alta seguridad respondieron lo siguiente: el 51% no sabe; el 24% dijo no, el 22% dijo

que sí cuenta con un sistema de alta seguridad, apenas el 3% no respondió. Por ello, según los resultados, es claro observar que los estudiantes no saben si la red del laboratorio de automatismo cuenta con un sistema de alta seguridad.

11. ¿De los siguientes factores cual considera más importante para proteger esta red?

Tabla 4. 11 Factores para proteger la red

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

	FRECUENCIA ABSOLUTA.	FREC. ABS. ACUMULADA	FRECUENCIA RELATIVA	REL. ACUMULAD
MEJORAR EL SISTEMA OPERATIVO	24	24	11%	11%
USAR SOFTWARE MÁS SEGURO	86	110	40%	51%
DARLE MANTENIMIENTO SEGUIDO A LA RED	33	143	15%	67%
INCREMENTAR LAS POLÍTICAS DE USO DE LA RED	71	214	33%	100%
TOTAL	214		100%	

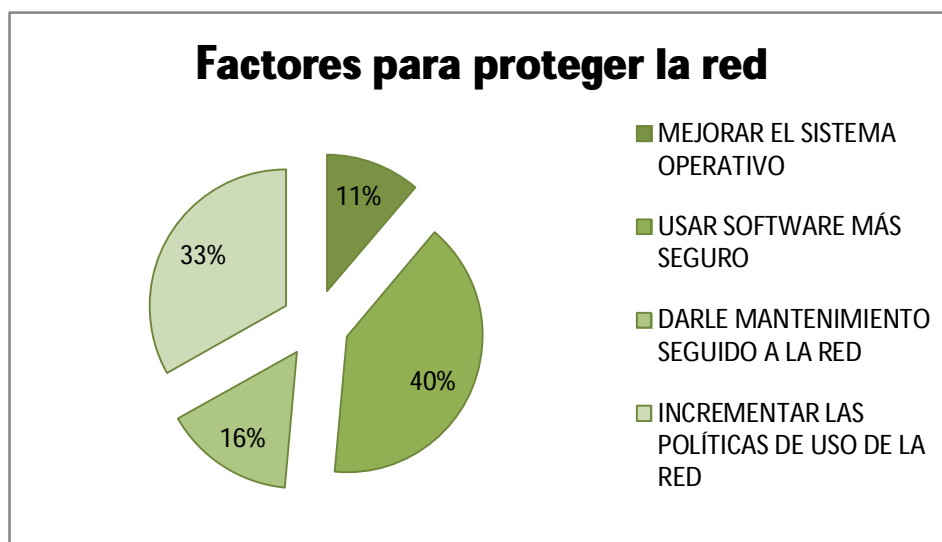


Figura 4. 11 Factores para proteger la red

Fuente: Encuestas realizadas a los estudiantes de la Facultad Técnica de la UCSG

Elaboración: Victoria Herrera

Según la encuesta efectuada a los estudiantes de la Facultad Técnica de la UCSG, sobre los factores de mayor importancia para proteger la red, respondieron lo

siguiente; el 40% dijo usando un software más seguro; el 33% dijo incrementando la política de uso de la red; el 16% respondió darle mantenimiento más seguido; apenas el 11% dijo mejorar el sistema operativo. Por ello, el usar un software más seguro representa un factor importante para proteger esta red.

4.2. Entrevistas

Las entrevistas fueron realizadas a cuatro responsables del Laboratorio de Automatismo de la Facultad Técnica de la UCSG, con el objetivo de tener el punto de vista de cada uno de ellos, sobre la protección de la red del laboratorio de automatismo.

1) ¿El disponer de una red en el laboratorio de automatismo en la facultad técnica de la UCSG que ha generado?

E1: Por lo general ha generado ciertos problemas en lo que respecta a la disposición de la red con la que cuenta el laboratorio de automatismo, debido a que genera riesgos con los cuales ciertos beneficios que se vieron de un principio ahora se los determina como prejuicios en el ámbito informático.

E2: Este laboratorio ha creado una serie de beneficios pero a su mismo tiempo ha generado inconvenientes debido a que es una red muy propensa a crear una serie de inconvenientes que puede afectar la información de los estudiantes.

E3: Bueno, a pesar de los beneficios que podría proporcionar el manejar una red dentro del laboratorio, puesto que hemos podido establecer un sistema al cual se puede acceder desde todos los equipos, también ha habido aspectos negativos, principalmente debido a que al encontrarse una gran cantidad de equipos conectados a la misma red, los niveles de vulnerabilidad son mayores, además del hecho de que en muchos casos es complicado poder controlar a todos los usuarios, esto incide en que algunos equipos presenten inconvenientes.

E4: Más que beneficios, ha generado inconvenientes, ya que los equipos son más vulnerables debido al número de usuarios que tienen acceso a la red, nosotros no podemos controlar a todos quienes ingresan y consecuentemente se incrementa la vulnerabilidad de la red y los equipos, incluso existe el riesgo que terceras personas intenten acceder a información clasificada de la universidad a través de la red.

2) ¿Cómo maestros en el área técnica, ofrecen la suficiente información a los alumnos sobre esta red del laboratorio de automatismo?

E1: La mayor parte de las veces sí, cada vez que el estudiante lo requiera, para eso es mi trabajo, sin embargo

E2: En la mayoría de casos no, debido a que los alumnos realizan las cosas por su propia cuenta uno nunca sabe cuando la necesiten, pero si se ha ayudado a los alumnos que requieren de ella.

E3: En la mayoría de los casos, los estudiantes acuden al laboratorio realizan sus prácticas y más nada, principalmente debido al tiempo no se suele proporcionar información relacionada a la red, ya que solo se proporciona la información en relación a las clases correspondientes.

E4: En pocas ocasiones ha habido algún estudiante que me ha consultado sobre el funcionamiento de la red, puesto que, generalmente los estudiantes no se preocupan por esto solo acuden al laboratorio a escuchar sus clases y realizar las prácticas.

3) ¿Mantener la seguridad de la red del laboratorio de automatismo representa un reto?

E1: Sin dudar si, debido a que es una red que no puede ser controlada del todo y como docente me encuentro capacitado pero en muchas ocasiones se me escapa de las manos obtener la plena seguridad de la red

E2: Sinceramente si, sin embargo se trata de sobrellevarlo, como se dijo anteriormente es un sistema muy vulnerable y de mucho cuidado, de esta razón si representa un reto para los profesores encargado de este laboratorio

E3: En realidad sí, puesto que, al encontrarse varios equipos conectados a la red incrementa la vulnerabilidad de la red, a pesar de que es imposible que se maneje una red 100% segura, debido a que siempre existen fallos en el diseño de los sistemas, tampoco se ha podido establecer un sistema de protección del sistema de red del laboratorio.

E4: Sí, porque no hemos podido implementar un sistema de seguridad que se ajuste a las necesidades del sistema, debido a esto existen equipos que presentan fallas.

4) ¿En algún momento se han generado problemas en la red del laboratorio de automatismo?

E1: claro que sí, debido a que existen demasiados servidores a cargo de esta red la cual empieza a colapsar y genera problemas para poder realizar una serie de trabajos la cual la institución se encuentra desarrollando.

E2: Si, al momento que los estudiantes maniobran esta red que, a muchos le favorece, existen problemas que se presentan tanto externo como interno esto requiere de mucho cuidado por cada uno de nosotros.

E3: Si, en varias ocasiones ya que hay equipos que tienen virus, a pesar de que le pasamos antivirus existen usuarios que ingresan dispositivos infectados lo cual afecta al sistema de red. Además, hay fallas que aún no se han solucionado, principalmente por falta de iniciativa y tiempo, es necesario que planifiquemos.

E4: Si, de hecho en la actualidad los estudiantes han reportado fallas en el funcionamiento de algunos equipos, por lo que es necesario que se tomen medidas para solucionar estos inconvenientes.

5) ¿Existen políticas de uso de la red del laboratorio de automatismo?

E1:Exacto debido a que existen problemas dentro de la red, por esta razones la institución ha desarrollado políticas de seguridad, para el bien del laboratorio y de los estudiantes que se encuentran a disposición de su uso.

E2: Se puede decir que no, porque existen las políticas pero no se las utilizan y esto hace que el uso de la red sea un poco defectuoso, pero el laboratorio cuenta con políticas depende de los profesores poderlas realizar para una mejora total.

E3: No, actualmente no hemos definido ninguna política que contribuya a lograr una mayor seguridad en el sistema.

E4: Bueno, una política enfocada en la seguridad del laboratorio no existe, puesto que a pesar de que hay normativas son muy básicas y muchos estudiantes no la conocen o si la conocen no la respetan. Sin embargo, sí es necesario que se

determine una política en la que se consideren todos los puntos para solucionar las vulnerabilidades del sistema.

CAPÍTULO V: MÉTODOS DE PREVENCIÓN Y PROTECCIÓN DE LA RED DEL LABORATORIO DE AUTOMATISMO

5.1. Desarrollo de la propuesta

Actualmente existen factores que determinan la necesidad de contar con una seguridad informática adecuada, de modo que se puedan minimizar los riesgos a los cuales están expuestos los sistemas informáticos. La supervivencia misma de la institución en muchos casos depende de la información que se maneja en esta, para lo cual la red deberá estar protegida contra las amenazas que pueden afectar la continuación de la actividad.

Por lo tanto, a continuación se establece una serie de procedimientos de seguridad que permitirán reducir los niveles de vulnerabilidad en la que se encuentran los equipos del Laboratorio de Automatismo de la Facultad de Educación Técnica para el Desarrollo, para ello se consideran los siguientes parámetros de protección de modo que se pueda garantizar la seguridad de las redes:

- Confidencialidad.
- Integridad.
- La disponibilidad de la información.

5.1.1. Análisis de los riesgos

El análisis de riesgo constituye en la evaluación de todas las posibles amenazas en términos de probabilidad de ocurrencia y su daño potencial, por lo general precede a la etapa para la seguridad del sistema informático, lo que permite estimar el

riesgo relativo en función de este valor decidir qué contramedidas de seguridad serán adoptadas.

Los principales métodos de seguridad y análisis de riesgos se determinan en la forma en que los sistemas pueden ser seguros, la forma de medir el riesgo y de cómo la institución podrá asegurarse de que los niveles adecuados de la privacidad de la información se mantienen para los usuarios del laboratorio. Para realizar un adecuado análisis de los riesgos, se debe considerar factores de seguridad cibernética, desde la forma en que se utiliza la red, la utilización de los sistemas operativos y la conexión a Internet.

Un análisis de riesgo implica la identificación de las amenazas más probables a la cual se encuentra expuesta la red del laboratorio y el análisis de las vulnerabilidades relacionadas de la organización a estas amenazas. Considerando que el funcionamiento del Laboratorio de Automatismo de la Facultad Técnica de Desarrollo depende en gran medida del uso de la tecnología y los sistemas automatizados, su interrupción, incluso por un par de días puede causar graves daños.

Un objetivo primordial del análisis de riesgos es proteger la red en caso de que todo o parte de sus operaciones y/o servicios informáticos resultara inutilizable. Cada área funcional de la organización debería ser analizada para determinar el riesgo potencial y el impacto relacionado con diversas amenazas de desastres.

Proceso de análisis de riesgos

Independientemente de los métodos de seguridad informática, las posibles amenazas que puedan surgir debido a la vulnerabilidad del sistema deben ser evaluadas. Aunque la naturaleza exacta de los riesgos o sus consecuencias resultantes son difíciles de determinar, es beneficioso realizar una evaluación exhaustiva del riesgo de todas las amenazas que pueden ocurrir de manera realista.

Aunque el sistema de ordenador principal puede ser el más vulnerable, deben ser analizados todos los equipos del laboratorio, incluso si estos son los más automatizados. El proceso de análisis de riesgos da la información que se necesita para tomar las decisiones relativas a la seguridad de la información, el procedimiento identifica la existencia de controles de seguridad, calcula vulnerabilidades y evalúa el efecto de las amenazas en cada área vulnerable.

Este análisis de riesgos del sistema o de la red, es un proceso que consta de varias etapas separadas, pero relacionadas entre sí. Sin embargo, cabe destacar que la evaluación de los riesgos deberá realizarse de forma constante. A continuación se determinan las etapas de análisis de riesgos:

1. Identificar y valorar los activos

El primer paso que se deberá seguir para el análisis de riesgos es identificar y asignar un valor a los activos en necesidad de protección. El valor de los activos es un factor importante en la decisión de hacer concesiones operativas para aumentar la protección de la red. El punto esencial es hacer una lista de todas las cosas que podrían verse afectados por un problema de seguridad. Estos incluyen: hardware, software, datos, usuarios, la documentación, y los suministros.

2. Identificar amenazas aplicables

Después de identificar los activos del laboratorio que requieren protección, las amenazas a esos equipos deben ser identificadas y examinadas para determinar su nivel de vulnerabilidad. Este paso consiste en la identificación y descripción de las amenazas para el sistema o la red, así como también la estimación de la frecuencia con que es probable que ocurran. Estos incluyen: el acceso no autorizado, la revelación de información, la denegación de servicio, el acceso desde puntos remotos, sistemas mal configurados, errores de software y las amenazas internas, como mínimo.

Amenaza

Existen dos axiomas válidos para las amenazas:

Axioma 1: El mismo tipo de amenazas existen para todos los sistemas y redes. La población de las amenazas es infinito en número y variedad. Cualquier amenaza en el sistema y la red ocurrirá en una frecuencia no determinada y sin control, sólo la posibilidad de ocurrencia de la amenaza varía entre sistemas y localizaciones.

Axioma 2: La frecuencia de aparición de una amenaza no deberá ser alterada. La aparente alteración de la frecuencia de ocurrencia de una amenaza es, en realidad, alterar el impacto de ocurrencia de las amenaza a través de la aplicación de contramedidas. Las contramedidas aplicadas en el laboratorio permitirán reducir el nivel de vulnerabilidad frente a la amenaza manifestada, no la frecuencia con que la amenaza ocurre.


Amenazas aplicables

La determinación de las amenazas a las cuales se encuentra expuesta la red del laboratorio requerirá de la investigación de registros históricos, fórmulas matemáticas y las conclusiones empíricas. La identificación de amenazas, requiere del registro en un formulario, incluye un título, una breve definición, y escrita racional para la inclusión de la amenaza en el proceso de evaluación. Una justificación por escrito para la frecuencia estimada de ocurrencia también debe ser proporcionada.

Tabla 5. 1 Formulario de registro de amenazas

Fuente: Victoria Herrera

Elaborado por: Victoria Herrera

 FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO			
FORMULARIO DE REGISTRO DE AMENAZA			
TIPO DE AMENAZA	VULNERABILIDAD DEL SISTEMA	VALORACIÓN	
		Nivel de riesgo	Frecuencia de ocurrencia

Identificar / describir vulnerabilidades

El nivel de riesgo deberá ser determinado mediante el análisis de la interrelación de las amenazas y las vulnerabilidades del sistema del Laboratorio de Automatismo. Es necesario que se considere que cuando una amenaza tiene una vulnerabilidad correspondiente, ya que incluso las áreas de alta vulnerabilidad pueden considerarse de poco riesgo en caso de que no se produzcan amenazas. El siguiente axioma deberá ser aplicado para la identificación de las vulnerabilidades:

Axioma 3: El nivel de vulnerabilidad disminuye a medida que aumentan las contramedidas. Es preciso considerar que algunas contramedidas tienen una mayor propensión a compensarla vulnerabilidad que otras. El nivel de vulnerabilidad y el valor relativo de cada contramedida deberá expresarse numéricamente del 1 al 5 considerando que el 1 representa menor amenaza y menor vulnerabilidad.


Determinar el impacto de la aparición de amenazas

Cuando se produce la explotación de una vulnerabilidad, el sistema sufre un impacto (pérdida). Las pérdidas se clasifican según las áreas de impacto titulado divulgación, modificación, destrucción, y denegación de sistema.

Tabla 5. 2 Impacto de amenazas

Fuente: Victoria Herrera

Elaborado por: Victoria Herrera

 FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO				
IMPACTO DE AMENAZA				
TIPO DE AMENAZA	ÁREAS DE IMPACTO			
	Divulgación	Modificación del sistema	Destrucción	Denegación del sistema

Revelación

Esta área se refiere a la confidencialidad, se debe hacer mayor hincapié en esta área de impacto en donde se analizará si la información del sistema del laboratorio es sensible o clasificada y se determinará el nivel de vulnerabilidad que presenta en relación a acceso de terceras personas.

Modificación

Se considera cuando un activo se cambia desde su estado original por el efecto de la manifestación de la amenaza denominada modificación. Esto deberá ser considerado especialmente cuando una amenaza pueda modificar el contenido de una base de datos.

Destrucción

En este caso, el activo se daña más allá de su uso práctico por la actividad amenazada. Se deberá hacer énfasis en esta área de impacto cuando la vulnerabilidad implica la pérdida total del sistema. La evaluación deberá realizarse considerando que esta área de impacto puede afectar en mayor medida que la modificación o la no disponibilidad temporal del sistema del Laboratorio de Automatismo.

Denegación de servicio

Este impacto deberá ser evaluado considerando las amenazas que son más propensas a causar la destrucción total del sistema. Al hacer hincapié en una o más áreas de impacto en el proceso de evaluación, la gestión deberá concentrarse en la reducción del impacto en el área de mayor preocupación.

Determinación de contramedidas

Una vez realizada la evaluación de los riesgos a los cuales están expuestos los equipos del Laboratorio de Automatismo se deberá establecer las contramedidas correspondientes, las cuales se designarán considerando la valoración asignada al riesgo y el impacto que podría causar. La identificación en el lugar contramedidas será parte del proceso de recolección de datos por adelantado en el análisis de riesgos. Las contramedidas se categorizarán como técnicas o administrativas con sus categorías de cada tipo de la siguiente manera:

Preventivo

Este tipo de contramedida está diseñada para evitar el daño o el impacto de una acción o evento que se produzcan.

Detective

Estas medidas proporcionan algún tipo de notificación en caso de que existan errores en el sistema.

Correctivo

Algunas contramedidas tienen la capacidad de corregir los problemas identificados.

Contramedidas requeridas

Todas las medidas de esta categoría se podrán remontar a una o más reglas escritas o regulaciones. La sensibilidad de los datos que se almacenan y/o procesan en el sistema o red del Laboratorio de Automatismo y su modo de funcionamiento, esto a su vez, determinará las contramedidas necesarias.

Preparar un informe de análisis de riesgo

El proceso de análisis de riesgos permitirá identificar los activos de la información de riesgo y adjuntar una valoración de los riesgos. Determinará las medidas de protección que permitirán minimizar los efectos del riesgo y asignar contramedidas. El proceso de análisis de riesgos también permitirá determinar si las contramedidas son eficaces, una vez que el análisis se haya completado, se debe preparar un informe que documente la evaluación de riesgos realizada.

En el informe del análisis se centrará en la información resumida y sólo se deberán utilizar los detalles técnicos si son necesarios para apoyar una decisión o hacer una elección entre las recomendaciones.

Detalles técnicos que el informe deberá incluir:

- Los niveles de vulnerabilidad
- Amenazas aplicables y su frecuencia.
- El entorno de uso
- Conectividad del sistema del laboratorio.
- Nivel de sensibilidad de los datos.
- Riesgo residual, expresado sobre una base de vulnerabilidad individual.

5.1.2. Políticas de seguridad informática

El Laboratorio de Automatismo de la Facultad Técnica de Desarrollo, con la finalidad de asegurar el desarrollo y el mantenimiento de los mecanismos adecuados para proteger la confidencialidad, integridad y disponibilidad de sus datos y recursos de información computarizados, establece la siguiente política que deberá ser adoptada por los responsables del laboratorio y los que hacen uso del mismo.

Propósito

En el laboratorio se procesan y manejan la información y los materiales sensibles para el aprendizaje de los estudiantes, consecuentemente será responsabilidad de todos el cuidado de los equipos y del sistema. Los datos y los sistemas creados y gestionados son de propiedad de la Universidad Católica Santiago de Guayaquil y como tal deben ser seguros de uso y los docentes responsables deberán proporcionar las instrucciones de las actividades que se consideran inapropiadas. El propósito de esta norma es establecer los requisitos de seguridad para todos los sistemas informáticos y los datos que se encuentran en el laboratorio y proporcionar un marco de rendición de cuentas para los usuarios del mismo.

Recursos cubiertos

- Red central de ordenadores a través de campus o de acceso remoto.
- Todos los programas y sistemas de software.
- Toda la información mantenida en los archivos del laboratorio.

Esta política se aplica a todos los docentes de la Facultad Técnica de Desarrollo de la UCSG, el personal y los estudiantes, especialmente a los a los docentes responsables del Laboratorio de Automatismo, así como proveedores, contratistas, o cualquier otras personas que tienen acceso a los sistemas o datos que se manejan en el laboratorio.

Definiciones

Recursos de información: Sistemas informáticos, equipos, software y datos.

Red: Las computadoras y dispositivos asociados conectados a la línea central de comunicaciones del Laboratorio de Automatismo de la Facultad Técnica de Desarrollo, incluye todas las direcciones dentro del campus.

Sistema: Ordenador que proporciona servicios a múltiples usuarios o de otros equipos.

Usuario: Cualquier persona que acceda a la red de sistemas informáticos o de datos del Laboratorio de Automatismo de la Facultad Técnica de Desarrollo.

Responsabilidades

El Decano de la Facultad de Educación Técnica para el Desarrollo, en conjunto con los docentes responsables del Laboratorio de Automatismo, tiene la autoridad y responsabilidad de establecer las políticas de seguridad de la información, pautas y estándares.

Todos los usuarios de los sistemas de propiedad o gestionados por la facultad, ya sea o no conectado a la red del Laboratorio de Automatismo, deberán seguir los siguientes requisitos para los dispositivos de la facultad o dispositivos de conexión a la Red del laboratorio.

Físico

El acceso a los centros de los sistemas de información de vivienda de datos y salas de cableado de redes de la infraestructura estará restringido para los usuarios, solo tendrá acceso a éste el personal autorizado y requerirá la autorización a través de la utilización de tarjetas emitidas por la facultad.

Los visitantes de estas áreas restringidas deben ser autorizados y acompañados en todo momento. Se deberá realizar un registro de acceso de los visitantes al laboratorio y a las áreas restringidas.

- El cableado del edificio se oculta y portales de acceso bloqueados.
- Los equipos informáticos obsoletos serán eliminados de acuerdo con la disposición del equipo informático.

Red

Se instalarán todos en los equipos de red y software mantenidos por los recursos de información del laboratorio. Los usuarios no pueden instalar concentradores,

puntos de acceso inalámbricos, servicios de terminal u otro equipo a través del que se extienda la red y tampoco podrán acceder, modificar, eliminar, conectar, o alterar de cualquier equipo dirigido por recursos informáticos.

Los programas que interfieren con el funcionamiento adecuado de la red o que cree una interferencia sustancial o riesgo no serán permitidos.

Todos los puntos de acceso a la red estarán protegidos por unos cortafuegos y sistemas de prevención de intrusión y control de comunicaciones. Los patrones de coincidencia de tráfico de reconocimiento específico, de intrusión o virus se verá impedido de entrar o salir de la red del laboratorio. Todos los sistemas de protección de frontera serán administrados y supervisados por el personal de recursos de información.

El flujo de información entre los sistemas de información (en particular entre los sistemas de las diferentes clasificaciones de sensibilidad) será restringido mediante el uso de listas de control de acceso y filtrado según sea necesario, las cuales se aplicarán dependiendo del nivel de vulnerabilidad del equipo.

El acceso remoto a los sistemas y dispositivos de red sólo se permitirá como se especifica en la política de seguridad de acceso remoto.

Servidores y aplicaciones

Todos los sistemas basados en el servidor del deberán ser administrados por el docente responsable del laboratorio (profesional de la tecnología de la información calificado), así como también deberá cumplir con los lineamientos de seguridad establecidos para cada nivel de clasificación de la sensibilidad.

Los servidores del laboratorio se podrán configurar y mantener de acuerdo con las líneas de base de seguridad desarrollados por la presente política de seguridad. Siempre que sea posible, el cumplimiento de estas líneas de base se aplicará automáticamente. En caso de que exista cualquier inconveniente en el

cumplimiento de estos parámetros deberá ser reportado de manera oportuna al director de la carrera y al decano de la Facultad Técnica de Desarrollo.

- Todos los servidores deben estar certificados por la seguridad de la información antes de ponerse en uso.
- Todos los servidores del laboratorio se encuentran dentro de uno de los centros de datos seguros de la universidad y se encuentran registrados como recursos de información.
- La información confidencial no debe residir en los servidores abiertos a Internet (debe estar ubicado en la red privada).
- Todos los servidores y las aplicaciones a las que se accede a través de la red deben utilizar mecanismos de autenticación sólo cifrados que sean autorizados por las políticas de seguridad de la información.
- Los servidores y las aplicaciones se pueden configurar para notificar al personal adecuado en el caso en que se realice una actividad inapropiada, inusual y/o sospechosa.

Estaciones de trabajo

Todas las estaciones de trabajo, independientemente del sistema operativo, se deben configurar con la configuración y las aplicaciones estándar de la Universidad Católica Santiago de Guayaquil, (Por política deben contar con los siguientes programas: McAfee, el software de apoyo anti-malware; LANDesk, software de control remoto.

Las estaciones de trabajo recibirán actualizaciones regulares de parches de seguridad de acuerdo con la política de administración de vulnerabilidad de la Universidad Católica Santiago de Guayaquil y la Facultad Técnica.

Compu Trace es un software de seguimiento de robo y el software McAfee Endpoint Encryption estarán activos en las estaciones de trabajo móviles, siempre que sea posible.

Las estaciones de trabajo que contengan o a través de las cuales se pueda acceder a la información confidencial, incluida la información administrativa de la carrera que se encuentre protegida e información que se considere sensible, deberán estar situados fuera de la vista pública y deben ser protegidos por protectores de pantalla protegidos por contraseña de acuerdo al protocolo de seguridad.

Datos

- Las copias de seguridad se llevarán a cabo de acuerdo a los horarios determinados por el tipo, la sensibilidad, la importancia y el valor.
- El cifrado se aplicará en función del tipo, la sensibilidad, la importancia y el valor.
- El programa de retención de registros gobernará el almacenamiento de datos.

Los datos confidenciales transmitidos dentro o fuera de la red del laboratorio a través de la Internet deben estar cifrados. El cifrado se puede realizar a través de VPN, SSL, SSH u otros métodos seguros aprobados por el Director de la carrera. El cifrado no se necesita para los datos transmitidos a través de línea dedicada cuando la ubicación fuera del sitio está protegida por unos cortafuegos.

Usuario

- Con la excepción de los sistemas de información pública, de cara al acceso a los sistemas y datos se requerirá la autenticación con usuario y contraseñas individuales y únicas para los equipos del Laboratorio de Automatismo.
- Los usuarios deben tener sólo el acceso mínimo a los sistemas y los datos que se requieren para llevar a cabo sus funciones académicas.
- Los propietarios de datos deben autorizar el acceso a sus respectivos sistemas.
- Las contraseñas para todas las cuentas de usuario se adherirán a la norma se indica en la política de seguridad de contraseña.

- El acceso para usuarios que cambian de papeles, tendrá su acceso revisado y actualizado, según sea necesario.
- El acceso se dará por terminado de inmediato cuando un usuario sale del laboratorio. Las cuentas inactivas serán desactivadas o eliminadas después de la revisión.

Todos los usuarios podrán completar la formación en temas de seguridad del ordenador dentro de los 30 días siguientes al comienzo de sus actividades académicas dentro del Laboratorio de Automatismo y con carácter anual a partir de entonces hasta que éste haya culminado sus estudios. La finalización de la formación incluirá la aceptación documentada de políticas relacionadas con la tecnología del Laboratorio de Automatismo de la Facultad Técnica de Desarrollo.

Excepciones

Las solicitudes de excepciones a esta política sólo podrá concederse por los sistemas en que estos requisitos pueden comprometer la disponibilidad o la facilidad de uso de una aplicación o sistema informático dentro del Laboratorio de Automatismo y cuando otras medidas de seguridad (por ejemplo, el filtrado de red, firewall, entre otros) están en marcha para mitigar los riesgos. Las solicitudes deben ser presentadas por escrito al docente responsable del laboratorio quien evaluará la solicitud en conjunto con el Directos de la Carrera para su aprobación. El formulario de Excepción Información de Seguridad estará disponible en el área administrativa de la carrera para este propósito.

Las excepciones sólo se permitirán en la recepción de la aprobación por escrito de la Seguridad de la Información. Seguridad de la Información conservará la documentación de las excepciones permitidas en la actualidad y las revisará una vez al año.

5.1.2.1. Políticas de seguridad de contraseña

La protección por contraseña es uno de los principios más importantes de la seguridad informática que serán considerados para mejorar la seguridad de la red

del Laboratorio de Automatismo, las contraseñas constituyen la primera línea y a menudo sólo de defensa contra el acceso no autorizado o inapropiado para la investigación o la información académica y el sistema que se guarda en los equipos del laboratorio.

Propósito

El propósito de esta política es establecer las normas para la creación y gestión de las contraseñas utilizadas en cualquier equipo del Laboratorio de Automatismo de la Facultad Técnica de Desarrollo en la Universidad Católica Santiago de Guayaquil.

Recursos cubiertos

Se aplica a todos los dispositivos electrónicos conectados a la red del laboratorio, incluyendo pero no limitado a las estaciones de trabajo y servidores, *switches* y *routers* de red, dispositivos técnicos especializados, entre otros.

Usuarios

Todo el que tiene o desea adquirir, una cuenta válida en los sistemas de la red, así como a los usuarios que tienen acceso a estos sistemas desde una ubicación fuera del campus. No hay exenciones.

Definiciones

Contraseña: Una serie de letras, números y/o símbolos que se utiliza para autenticar la identidad de un usuario y que se utiliza para permitir el acceso a la red del laboratorio.

Contraseña curso de la vida: La longitud de tiempo que una contraseña puede ser utilizada antes de que se pueda cambiar.

Historial de contraseñas: Una lista de contraseñas anteriores que utiliza una cuenta de usuario específica.

Usuario: Cualquier persona que tiene una cuenta válida en los sistemas de la red del laboratorio y el correo electrónico de la Universidad Católica Santiago de Guayaquil.

Responsabilidades

Los administradores de sistema del Laboratorio de Automatismo y usuarios asumen las siguientes responsabilidades:

- El administrador (Docente responsable) debe proteger la confidencialidad de las contraseñas en los sistemas y configurar los sistemas para cumplir con los requisitos establecidos en esta política.
- Los usuarios deben crear y administrar contraseñas de acuerdo con las normas descritas a continuación.
- Cada usuario es responsable de todas las acciones y funciones realizadas por su cuenta dentro del laboratorio.
- Cualquier sospecha de compromiso contraseña debe ser reportada al docente responsable del laboratorio de manera inmediata.

Norma I. Contraseña

Las contraseñas de acceso a las redes y los sistemas informáticos del Laboratorio de Automatismo deben cumplir con los siguientes requisitos:

- Consta de un mínimo de 8 y un máximo de 16 caracteres.
- Contener un mínimo de una mayúscula.
- Contener al menos un número.
- Contener al menos un carácter especial de la serie siguiente:

Tabla 5. 4 Caracteres especiales

Fuente: Victoria Herrera

Elaborado por: Victoria Herrera

E+D FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO															
CARACTERES ESPECIALES PARA CONTRASEÑA															
!	"	#	\$	%	Y	'	()	*	+	,	-	.	/	:
;	<	=	>	?	@	[\]	^	_	'	{		}	~

Las contraseñas tienen una vida útil máxima de 365 días. (Las contraseñas deben cambiarse una vez al año). Las contraseñas no deben volver a utilizarse durante un mínimo de 10 ciclos. Para minimizar el riesgo de que alguien pueda adivinar la contraseña:

- Se puede utilizar dos o tres palabras cortas que no están relacionados.
- Deliberadamente escribir mal las palabras.
- Tomar la primera letra de cada palabra de una frase.
- No use ninguna parte del identificador de cuenta (su ID de inicio de sesión, nombre, entre otros).
- No utilizar un nombre propio o cualquier palabra en el diccionario sin que ésta haya sido cambiada de alguna manera.

Norma II. Requisitos de protección con contraseña

- Las contraseñas no deben ser compartidas o reveladas a nadie que no sea el titular autorizado de la cuenta de usuario (a no ser que se haya aprobado por el docente responsable del Laboratorio de Automatismo).
- Las contraseñas no deben ser escritas o almacenadas de una manera en que puedan ser vistas por una persona distinta del titular de la cuenta autorizada. Si una contraseña debe ser almacenada, debe ser cifrada usando un método de cifrado aprobados por la seguridad de la información.

- Los usuarios no deben utilizar su contraseña de red para otro tipo de cuentas personales, que se manejen fuera del Laboratorio de Automatismo.
- Las contraseñas iniciales para una cuenta de usuario deben ser únicas y deben estar configuradas para requerir que la contraseña se cambie inmediatamente cuando el usuario inicia sesión por primera vez.
- El sistema será configurado para bloquear las cuentas de usuario después de 5 intentos fallidos de ingresar. La cuenta permanecerá bloqueada durante 15 minutos o hasta que se restablezca por el docente responsable.
- Las contraseñas deben ser cambiadas inmediatamente si se sospecha que el ID de usuario y la contraseña han sido revelados a una persona no autorizada o si el sistema ha sido comprometido o está bajo la sospecha de haber sido comprometido.
- Las contraseñas se utilizan para aplicaciones, scripts, sitios web de Internet, los procesos del sistema, y otros procesos automatizados. No se deben almacenar en un formato legible, donde un individuo no autorizado pueda verlas.
- Todas las contraseñas por defecto suministradas por el proveedor de software de aplicaciones o dispositivos de hardware se deben cambiar inmediatamente después de ser colocado en la red del laboratorio.

Procedimientos

Los procedimientos para la tramitación de solicitudes de contraseña se esforzarán por equilibrar los requisitos de seguridad y comodidad del usuario del Laboratorio de Automatismo. Estos procedimientos serán seguidos por el personal docente responsable del Laboratorio de Automatismo.

1. Los usuarios del laboratorio deberán responder a varias preguntas de seguridad de contraseña que les permitan restablecer su propia contraseña en caso de que la han olvidado. Para configurar sus preguntas y respuestas los usuarios deben iniciar sesión en el portal del sistema del laboratorio y seleccionar "Cambiar las preguntas de seguridad de contraseña" en la ficha de Informática.

2. El personal docente responsable del laboratorio deberá atender las solicitudes de restablecimiento de contraseñas:

- Las solicitudes se pueden hacer en persona la Facultad Técnica de Desarrollo. Se requiere de la presentación de una identificación con fotografía.
- El docente debe aprobar cualquier cambio de contraseña solicitada por el supervisor de un usuario. La confirmación será enviada al usuario cuando se haya completado el cambio de contraseña a solicitud del docente responsable.

Excepciones

Las solicitudes de excepciones a esta política sólo podrán concederse en circunstancias especiales. Las solicitudes deben ser presentadas por escrito al docente responsable del laboratorio para su aprobación.

5.1.3. Implementación de parches para gestión de vulnerabilidades

La prueba del parche

La prueba del parche es vital para determinar si este afectará al normal funcionamiento de cualquier software existente en la red del Laboratorio de Automatismo. Es importante que esta prueba se lleve a cabo en un sistema de espejo que tiene una configuración idéntica o muy similar al sistema de destino. Esto permite asegurar que la instalación de la revisión no conducirá a consecuencias no deseadas en el sistema del laboratorio.

Además de contribuir a identificar los problemas no deseados en el laboratorio, los parches mismos deberán ser aprobados para asegurarse de que han corregido la vulnerabilidad identificada y el problema de rendimiento del sistema. Esto se logrará por:

1. La comprobación de que los archivos o las opciones de configuración en el parche están destinadas a la correcta adaptación al sistema como se indica en la documentación del fabricante.
2. La exploración del sistema host con un escáner de vulnerabilidad que es capaz de detectar las vulnerabilidades conocidas. Esta técnica, sin embargo no siempre es eficaz, porque los escáneres de vulnerabilidad no pueden comprobar la presencia real de la vulnerabilidad en cuestión. Muchos escáneres de vulnerabilidades sólo verifican los números de versión de software o los niveles de parche para determinar si las vulnerabilidades existen o no.

Si no es factible instalar el parche porque, por ejemplo, los resultados de las pruebas muestran que el parche se bloqueará o podría alterar seriamente el sistema del laboratorio, se deberán implementar controles de seguridad alternativos.

Implementación de parches y verificación

La aplicación de los parches para la gestión de las vulnerabilidades en el sistema puede ser tan simple como modificar una configuración en el sistema, o puede requerir la instalación de una nueva versión del software. Ningún método de parche solo se puede aplicado en todas las aplicaciones de software y del funcionamiento del sistema.

El análisis de los riesgos puede proporcionar las instrucciones específicas para la aplicación despaches de seguridad y su actualización, se recomienda que los docentes responsables lean toda la documentación pertinente proporcionada por los distribuidores antes de proceder con la instalación de parches.

Además, los parches de seguridad deben implementarse a través de un control de cambios establecido proceso. Antes de aplicar un nuevo parche, los administradores deberán realizar una completa copia de seguridad del sistema a ser parcheado. Esto permitirá una restauración rápida y fácil del sistema a un estado anterior si el parche tiene un impacto no deseado o inesperado en el sistema. Después de implementar la revisión, los administradores de sistemas y los usuarios deben verificar que todos los sistemas y aplicaciones estén

funcionando normalmente, y que cumplen con lo establecido en las políticas y directrices de seguridad.

Selección del parche

LANDesk Security Suite ofrece protección en tiempo real contra spyware, malware y otras amenazas que ponen en peligro los datos de los usuarios y que puedan dañar la integridad y la eficiencia de la red del Laboratorio de Automatismo y permite aumentar la carga de trabajo del laboratorio.

Las capacidades de detección y eliminación permitirán proteger el sistema en tiempo real gracias a las definiciones de la base de datos constantemente actualizada de LANDesk, utilizando las fuentes de información estándar de la industria, incluida la información sobre los programas espía, malware, troyanos, keyloggers y otros tipos de software malicioso. Las alertas en tiempo real le permitirán al docente responsable manejar fácilmente las necesidades de seguridad y las nuevas definiciones basadas en el tipo e importancia.

5.2. Justificación del proyecto

Considerando el constante desarrollo tecnológico que se experimenta actualmente ha generado resultados tanto positivos como negativos, ya que a pesar de los beneficios que proporcionan a los usuarios un mayor y fácil acceso a la información, también ha incidido en que se genere un mayor número de riesgos a los cuales están expuestos los sistemas de redes, debido a la vulnerabilidad en la que se encuentran.

Estas vulnerabilidades pueden deberse a varios factores como fallos en el sistema operativo, el poco control que se realiza de los usuarios que tienen acceso al sistema, entre otros. Sin embargo, tales vulnerabilidades pueden ocasionar grandes pérdidas para los propietarios del sistema, ya que se encuentran expuestos a que personas no autorizadas accedan al sistema y puedan robar información confidencial, por lo tanto es necesario que se apliquen métodos que permitan reducir el nivel de vulnerabilidad de los sistemas, sobre todo en aquellas

instituciones donde existe un mayor número de personas que tienen acceso al sistema.

La seguridad informática debe ser una responsabilidad de todos quienes tienen acceso a los sistemas, sin embargo, en la mayoría de los casos no basta sólo con la aplicación de programas que protejan al sistema en contra de virus, puesto que, existen otro tipo de riesgos que pueden incrementarse debido al desconocimiento o debido al poco control que se ejerce sobre el uso del sistema.

A través del diseño de métodos de prevención y protección para la red de Laboratorio de Automatismo de la facultad Técnica de la UCSG se logrará minimizar los riesgos a los cuales están expuestos los equipos del laboratorio, de modo que se pueda evitar la pérdida de información y el daño del sistema a lo cual actualmente se encuentran expuestos.

5.3. Objetivos del proyecto

5.3.1. Objetivo general

- Diseñar métodos de prevención y protección para la red del Laboratorio de Automatismo de la Facultad Técnica de la UCSG.

5.3.2. Objetivos específicos

- Proteger los recursos informáticos de la red del Laboratorio de Automatismo de la Facultad Técnica de la UCSG.
- Preservar las características de confidencialidad e integridad de la red del laboratorio.
- Proporcionar un reglamento sobre seguridad informática para el Laboratorio de Automatismo de la Facultad Técnica de la UCSG.

5.4. Beneficiarios del proyecto directo e indirecto

En lo que respecta a los beneficiarios del proyecto, se considera como beneficiarios directos a la Facultad Técnica de la UCSG, puesto que, con la aplicación de las normas de prevención y protección se logrará minimizar los riesgos a los que actualmente se encuentra expuesta la red del laboratorio de dicha facultad debido a los niveles de vulnerabilidad en que se encuentran los equipos.

Además, serán beneficiados los estudiantes de la facultad que hacen uso del Laboratorio del Automatismo, ya que podrán hacer uso de los equipos y acceder a información de manera más segura, evitando que la utilización de componentes como memorias USB que puedan infectarse con algún tipo de software malicioso. Así como también, podrán hacer uso de los equipos sin que estos presenten constantes fallas que dificulten el trabajo de los estudiantes.

En lo que se refiere a los beneficiarios indirectos, se considera a la Universidad Santiago de Guayaquil, puesto que el desarrollo de los métodos de prevención y protección para la red del laboratorio de automatismo de la Facultad de Automatismo, no solo se logrará asegurar la información que maneja esta facultad, sino que además podrá obtener las pautas para aplicar tales métodos de prevención en otras facultades y en la universidad en general.

5.5. Localización física

La localización física del proyecto se encuentra en la Facultad Técnica para el Desarrollo de la Universidad Católica Santiago de Guayaquil, específicamente en el Laboratorio de Automatismo, puesto que es en este laboratorio en donde se ha podido identificar la vulnerabilidad de la red informática y consecuentemente es a donde está orientada la propuesta.



Figura 5. 1 Facultad Técnica para el Desarrollo

Fuente: (Google Maps, 2014)

5.6. Seguimiento y evaluación

Para realizar el seguimiento del proyecto se asignará un manual para los docentes responsables del Laboratorio de Automatismo de la Facultad Técnica para el Desarrollo, puesto que son quienes están encargados de gestionar quienes hacen uso del laboratorio. Se deberá hacer una evaluación para determinar los resultados de los métodos de prevención y protección propuestos, de esta manera se podrá identificar si se ha logrado reducir la vulnerabilidad de la red.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- A través del desarrollo de la investigación se ha podido identificar que no existe una política de seguridad que regule el manejo de los equipos del Laboratorio de Automatismo en la Facultad Técnica de Desarrollo.
- Así mismo, se ha podido identificar que es muy importante la implementación de un sistema de alta seguridad para proteger los equipos que se encuentran en el Laboratorio de Automatismo que se encuentran vulnerables actualmente.
- Para elaborar el diagnóstico y establecer la problemática del mismo, fue necesario conocer el funcionamiento de los sistemas que se encuentran instalados en el laboratorio
- En base al diagnóstico establecido, fue posible identificar las debilidades técnicas en los sistemas de la red y establecer prioridades en base a la importancia de los sistemas afectados.
- Para las debilidades determinadas, se estableció los principales métodos de prevención y protección de redes existentes.
- Con los antecedentes expuestos, fue posible analizar las vulnerabilidades que tiene el Laboratorio de Automatismo de la Facultad de Educación Técnica para el Desarrollo de la UCSG, cumpliendo así el objetivo general propuesto.

Recomendaciones

- Se recomienda que se realice la evaluación de los equipos existentes en el Laboratorio de Automatismo, de acuerdo a lo establecido en la propuesta.
- Se recomienda también que la política de seguridad sea difundida tanto a docentes como a los estudiantes de la Facultad Técnica de Desarrollo, puesto que su cumplimiento es de responsabilidad de todos quienes forman parte de esta facultad.
- Es recomendable que se solicite a los usuarios del Laboratorio de Automatismo que establezca una clave de usuario de acuerdo a los parámetros establecidos en las políticas de seguridad.

BIBLIOGRAFÍA

- Areitio, J. (2008). *Seguridad de la informacion: redes, informatica y sistemas de información*. Madrid : Paraninfo.
- Benchimol, D. (2011). *Hacking* . Buenos Aires: USERSHOP.
- Best, J. (2008). *Cómo investigar en educación*. Madrid: Ediciones Morata.
- Dávila, J., Malhotra, N., & Teviño, M. (2008). *Investigación de mercados*. Naucalpan de Juárez, Edo. de México: Pearson Educación.
- Del Peso, E. (2001). *Peritajes informáticos*. Madrid: Ediciones Díaz de Santos.
- García, A., & Alegre, M. d. (2011). *SEGURIDAD INFORMATICA ED.11 Paraninfo*. Madrid: Editorial Paraninfo.
- Gómez, J. (2009). *Optimización de sistemas de detección de intrusos en red utilizando técnicas computacionales avanzadas*. Almería: Universidad Amería.
- Gómez, M. (2008). *Introducción a la metodología de la investigación científica*. Córdoba: Editorial Brujas.
- Google Maps. (15 de Enero de 2014). *Google Maps*. Recuperado el 20 de Enero de 2014, de Parroquia Tarqui: <https://www.google.com.ec/maps/place/Facultad+Tecnica+para+el+Desarrollo/@-2.1812032,-79.9042779,17z/data=!4m5!1m2!2m1!1sfacultad+tecnica+universidad+catolica+santiago+de+guayaquil!3m1!1s0x0:0xf553c4061fc19f4f?hl=es>
- Pacheco, F., & Jara, H. (2009). *Hackers al descubierto*. México: USERSHOP.
- PARANINFO. (2011). *Seguridad informatica*. Madrid: Editorial Paraninfo.
- Reza, F. (2008). *Ciencia, metodología e investigación*. Naucalpan de Juárez, Edo. de México: Pearson Educación.
- Sánchez, J. (2003). *Ingeniería de proyectos infotmáticos: actividades y procedimientos*. Castellón: Universitat Jaume I.
- Sommerville, I. (2005). *Ingeniería del software*. Madrid: Pearson Educación.
- Sommerville, I. (21 de Abril de 2008). *Ingeniería del software*. Madrid: Pearson Educación.

Universidad Católica Santiago de Guayaquil. (15 de Enero de 2013). *Facultad de Educación Técnica para el Desarrollo* . Obtenido de <http://www2.ucsg.edu.ec/tecnica/>