UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

ENERO – JUNIO 2017

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

Ingeniería en Sistemas

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERA EN SISTEMAS

TEMA:

Estudio de las Vulnerabilidades en la Red de Datos de la Unidad Educativa Zapotal

EGRESADA:

Daniela Somayra Saa Aviles

TUTOR:

Ing. Raúl Armando Ramos Morocho, MIA

AÑO 2017

I. Introducción

Debido a que las redes de datos cada vez son más útiles e importantes para cualquier entidad, es necesario conocer las amenazas con las que podría enfrentarse la red, que a causa de ciertas vulnerabilidades existentes estas amenazas pueden llegar a concretarse dejando como resultado la creación de problemas que podrían ocasionar el mal funcionamiento de la red. Las redes suelen llegar a ser muy vulnerables, al referirse a la cantidad de equipos conectados entre sí compartiendo recursos, existe la posibilidad de atacar toda la red accediendo como primera instancia a uno de los equipos y consecutivamente propagarse al resto.

En una red la prioridad es la transmisión de la información, así que todas las vulnerabilidades están relacionadas directamente con la posible intercepción de la información por personas no autorizadas.

Mediante la elaboración de este documento se presenta información real y confiable obtenida mediante el uso de herramientas para la investigación, con el fin de conocer la situación actual de la red de datos tratando de cumplir el objetivo general planteado en el desarrollo de este caso, en este punto es donde se identifican las vulnerabilidades y sus posible consecuencias que puedan afectar el área informática y el rendimiento de la red, además mediante las diferentes referencias bibliográficas se intenta obtener información relevante y actualizada que ayude a interpretar de una manera más clara y concisa temas relacionados a este proyecto.

Finalmente se expresan las respectivas conclusiones, planteadas a partir de los resultados obtenidos una vez realizada la investigación correspondiente, así como también se revelan las fuentes bibliográficas de donde se obtuvo información que forma parte de este estudio.

II. Desarrollo

La Unidad Educativa Zapotal está ubicada en la Parroquia Zapotal perteneciente al Cantón Ventanas - Prov. Los Ríos, en abril de 1977 Wilson Ramírez Supervisor de educación de Los Ríos se reunieron con un grupo de ciudadanos de Zapotal con quienes vio que en esta localidad había la necesidad de funcionamiento de un colegio fiscal. El 10 de mayo de 1979 en el triunvirato militar conformado por el general de división Guillermo Duran, Alfredo Poveda y Luis Leoro se crea el colegio nacional sin nombre de la parroquia zapotal siendo Reinaldo Echeverría el primer rector.

El colegio comenzó a funcionar con 146 alumnos, en 1980 Victoria Wellington obsequió el terreno para la construcción de las instalaciones del colegio. El 28 de agosto de 1980 según decreto 548 el ministro de educación decidió colocar el nombre de Zapotal al colegio, en honor a la parroquia donde se encontraba. El 21 de septiembre de 1993 se cambió la especialización a técnico en comercio y administración con la especialización de informática y contabilidad.

Hoy por hoy la institución cuenta con aproximadamente 600 alumnos, quienes cumplen un papel importante para lograr un buen rendimiento educativo. La infraestructura se compone de doce aulas, tres oficinas o departamentos donde se desempeñan diversas labores (rectorado y secretaria, vicerrectorado y talento humano, sala de profesores), laboratorios, bar de alimentos y áreas recreativas. La malla curricular de la Institución ofrece tres especialidades: Bachillerato Técnico; Contabilidad y Administración, Aplicaciones Informáticas. Bachillerato General; Ciencias Sociales. Esta Unidad Educativa como otras entidades públicas utiliza la plataforma del Ministerio de Educación (educarecuador.gob.ec) para el registro y reporte de calificaciones.

La institución gestiona información estudiantil en lo que corresponde a calificaciones, historial académico, información sobre asistencia y disciplina.

La seguridad es uno de los aspectos fundamentales para obtener un adecuado funcionamiento de la red de datos, ya que mediante la seguridad se respalda la integridad y confidencialidad de los datos. Un abuso a la seguridad implica generar serios daños en la estabilidad de la red. La exclusión de políticas de seguridad podría generar la perdida de datos importantes dentro de una organización. De tal manera se plantea la necesidad de identificar las vulnerabilidades en la red de datos y a qué tipo de amenazas se encuentra expuesta, para tener así una percepción sobre la situación actual de la red.

El objetivo general es identificar las vulnerabilidades en red de datos de la Unidad Educativa Zapotal.

Este caso se basa en tratar la seguridad de la red de la manera más asequible posible, para facilitar el estudio de las vulnerabilidades, así como también se procura no indagar sobre la existencia (cantidad y descripción) de equipos y software, que posea la institución.

La línea de investigación bajo la cual está regido este caso es desarrollo de sistemas de la información, comunicación y emprendimientos empresariales y tecnológicos; como sub línea, procesos de transmisión de datos y telecomunicaciones.

La Unidad Educativa Zapotal en la actualidad no cuenta con un estudio previo que ayude a determinar las vulnerabilidades que pueda tener la red de datos.

La investigación se desarrolló mediante la metodología cualitativa, por lo que se usó herramientas como cuestionario de preguntas para la ejecución de la entrevista realizada al

Director de la TIC´S de la Unidad Educativa Zapotal, así como también se obtuvo información mediante un estudio de campo con la visita realizada a la institución donde se pudo observar los equipos sus conexiones y otros componentes que forman parte de la red dentro de la institución.

Según la investigación realizada por el Téc. Eduardo Adalberto Guillén explica que:

La comunicación de la información de una institución a través de redes de datos, producen riesgos de ataque y se torna difícil controlar aquellos puntos de la red de datos identificados como vulnerables, especialmente los dispositivos intermediarios, que son los encargados de suministrar y administrar el flujo de tráfico a través de la red. Estos dispositivos suelen ser objeto de frecuentes ataques; ya sea por software o código malicioso, así también ataques realizados por personas que se dedican a dañar estos dispositivos, lo que genera pérdida de información y retraso en los procesos de la institución. (Guillén, 2013)

La seguridad informática dentro de una organización es un tema que cobra mucha importancia a la hora de proteger la información que estas poseen. Según un artículo publicado por CCM expresa que el objetivo principal de la seguridad informática "consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto" (CCM , 2016).

"Convirtiéndose en una disciplina imprescindible para un buen profesional y necesaria para prácticamente cualquier persona, venga del campo y disciplina que venga" (Castro Gil, Díaz Orueta, Alzórriz Armendáriz, & Sancristóbal Ruiz, 2014).

"Aplicando todas las medidas necesarias para evitar riesgos y perdidas de la información y de los equipos en que reside" (Castallanos, 2015).

El dilema básico de la seguridad informática es cuestión de la existencia de diferentes medios de ataque. Podemos ser atacados mediante nuestra red, de forma inalámbrica, visitando páginas infectadas, por virus a través de USB infectados, etc., y de alguna manera existen herramientas para la defensa de ciertos tipos de ataques, pero esto conlleva a contar con un presupuesto considerable para obtener todas las herramientas de defensa para la seguridad informática. (Castro Reynoso, Los 27 controles críticos de la seguridad informática, 2012)

En el tema de redes se exponen conceptos básicos como lo explica el autor Moro Vallina: "Una red está formada por el conjunto de elementos necesarios para que se establezca la comunicación; en su sentido más amplio, incluye los emisores, receptores, nodos intermedios, conmutadores, enlaces, etc." (Moro Vallina, 2013).

Para cualquier empresa la red de datos es de vital importancia ya que pueden compartir recursos importantes, específicamente información.

El autor Isidoro Berral Montero presenta en su libro que: "las primeras redes de datos estaban limitadas a intercambiar información basada en caracteres alfanuméricos entre sistemas informáticos conectados. Las redes actuales han evolucionado para añadir texto y gráficos, voz, video, multimedia, etc., a los diferentes tipos de dispositivos" (Berral Montero, 2014).

"La función de las redes es mover los datos entre servidores, PC´s, y demás aparatos" (Castro Reynoso, Arquitectura de la seguridad informática, 2013). Y que "a través del tiempo han sido objetivo de constantes amenazas y ataques por ser un recurso indispensable en la labor cotidiana de toda empresa o institución" (Guillén, 2013).

"La seguridad de redes es un nivel de seguridad que garantiza que el funcionamiento de todas las máquinas de una red sea óptimo y que todos los usuarios de estas máquinas posean los derechos que les han sido concedidos" (CCM, 2016).

Para proteger la información que poseen las organizaciones existe una normativa o estándar que acoge todos los aspectos que deben tener en consideración las organizaciones para asegurar eficientemente sus datos frente a todos los probables incidentes que pudieran afectarla.

ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.
El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.
La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002. (ISOTools)

Definir una política de seguridad de una red significa desarrollar procedimientos y planes que resguarden los recursos de la red en contra de la pérdida y daño de la misma. Para la creación de estas políticas se debe tomar en cuenta, los recursos que se tratan de proteger, de quiénes se deben proteger, las probables amenazas, la importancia del recurso a proteger, y las medidas que se pueden ejecutar para proteger los recursos. Posteriormente examinar periódicamente la red para observar si deben realizar cambios en los objetivos de trabajo de la política de seguridad.

"El impacto de las diferentes amenazas varía considerablemente según el efecto sobre la empresa; algunas tienen un impacto sobre la confidencialidad o la integridad de datos, otras actúan sobre la disponibilidad de los sistemas" (Carpentier, 2016).

Los riesgos se conceptualizan como "la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. No constituye una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma" (Aguilera López, 2011).

Según autores las vulnerabilidades se definen como:

- "Probabilidades que existen de que una amenaza se materialice contra un activo. No todos los activos son vulnerables a las mismas amenazas" (Aguilera López, 2011).
- "Estado de insuficiencia en un sistema informático o conjunto de sistemas que permiten la materialización de una amenaza afectando las propiedades de disponibilidad, confidencialidad, integridad, autenticidad, no repudio" (Medina, 2014).

Resultados obtenidos mediante la encuesta realizada por ESET Latinoamérica expone que: La explotación de vulnerabilidades se ha convertido en la mayor preocupación de las empresas en cuanto a seguridad se trata, seguida de otros incidentes como infección por malware, fraudes. Dado esto, la evaluación cobra mucha importancia para evitar percances relacionados con la explotación de las mismas y como un medio para la aplicación de un elemento de la denominada seguridad ofensiva, a través de los escáneres de vulnerabilidades. (Mendoza, 2014)

Kali Linux, es casi sin lugar a dudas, la suite más completa en de su clase, habiendo conseguido su objetivo de agrupar las herramientas de este campo en un solo sitio, facilitando su uso. Kali está basada en Debian, y fue diseñada principalmente para la auditoria y seguridad informática

en general. Actualmente es mantenida por Offensive Security Ltd. que desarrolló la distribución a partir de la re-escritura de BackTrack (también desarrollada por ellos), una distribución predecesora a Kali, y que gozó de mucho éxito entre las personas que se dedicaban a esta actividad. (Martinez, 2015)

Kali Linux trae preinstalados una gran cantidad de programas relacionados con el tema de la seguridad informática (más de 600 programas), siendo algunas de las más conocidas Nmap (un escáner de puertos), Wireshark (un sniffer), John the Ripper (Un crackeador de passwords) y la suite Aircrack-ng (Software para pruebas de seguridad en redes inalámbricas), además del inigualable Metasploit, la gran suite de explotación de vulnerabilidades. (Martinez, 2015)

En el trabajo realizado por Andrés Paúl Gonzáles Orellana y Diego Rolando Tenemaza Arias describe los tipos de vulnerabilidades tales como:

- Vulnerabilidades Físicas

  Instalaciones inadecuadas del espacio de trabajo, falta de organización de los cables de energía y de red, etc.

- Vulnerabilidades Naturales

  Ambientes propensos a incendios, inundaciones, incapacidad de resistir terremotos entre otros desastres provocados por la naturaleza.

- Vulnerabilidad de Hardware

  Conservación inadecuada de los equipos, falta de equipos de contingencia. (Gonzáles Orellana & Rolando Tenem, 2012)

- Vulnerabilidad de Software

  Configuración e instalación indebida de programas en las organizaciones.

- Vulnerabilidad de Almacenamiento

  Medios no utilizados de forma adecuada, el contenido podría ser vulnerables a diferentes factores.

- Vulnerabilidad en la Comunicación

  La información debe transitar de la manera más segura posible. (Gonzáles Orellana & Rolando Tenem, 2012)

También pueden generarse otro tipo de vulnerabilidades dependiendo su naturaleza, estos tipos pueden ser:

- Vulnerabilidad de diseño

  Mal diseño de la arquitectura de la red, debido a este tipo de vulnerabilidad lo que se debería hacer para enfrentar las diferentes amenazas que se puedan presentar, es volver a diseñar una arquitectura adecuada para la red.

- Vulnerabilidad organizacional

  No existen políticas de seguridad dentro de la organización, o tal vez al existir estas políticas no son correctamente cumplidas.

La determinación de requerimientos para la seguridad dentro de una institución permite crear normas que puedan evitar eventos perjudiciales, como el deterioro en los equipos, entre otros; aunque es casi inevitable que ocurran ciertas situaciones de riesgo lo más acorde seria que el personal de la institución esté preparada o capacitada para sobrellevar estos problemas.

Puede llegar a ser difícil la implementación de una política de seguridad si no cuentan con los conocimientos necesarios sobre lo que se desea proteger y de los orígenes de amenazas.

En el estudio realizado por Rodríguez Duque & Gonzáles Rogel manifiesta que:

Es de gran importancia conocer sobre la inseguridad y los riesgos que puedan afectar a una red de datos dentro de una institución por lo tanto sin la búsqueda de vulnerabilidades en una las organizaciones crean una idea equivocada de su seguridad, cave recalcar que algunas de las debilidades que se generan en frecuentemente son el hecho de usar contraseñas predeterminadas o débiles en seguridad. (Rodríguez Duque & Gonzáles Rogel, 2015)

Es necesario obtener una visión general del funcionamiento de la red en la institución, a continuación se detalla la entrevista que se le realizo al Director de TIC´S de la Institución Ing. Bayron Suarez C., quien expreso lo siguiente:

"Ingrese en el mes de agosto del 2016 como docente de informática, posteriormente fui designado como Director de TIC´S, la primera vulnerabilidad con la que me encontré fue que el acceso a la red mediante el router no estaba protegido por lo que la clave del dispositivo estaba expuesta, esto generaba que la red se vuelva lenta e inconsistente, opte por reforzar la seguridad configurando el dispositivo y asignándole una clave como administrador para mantener un acceso restringido a la red. La institución tiene dos laboratorios, pero uno de ellos es usado solo para realizar prácticas de ensamblaje y para el uso de herramientas ofimáticas en clases debido a que las computadoras son de baja capacidad y no cuenta con conexión a internet."

Posteriormente el entrevistado respondió un cuestionario de preguntas mediante las cuales se obtuvo la siguiente información:

- Adaptación nuevas tecnologías dentro de la institución como, por ejemplo, lector de huellas para el control de asistencia de docentes, personal administrativo, y auxiliares.

- Utiliza firewalls, para proteger la red contra ataques o infecciones por virus. “Firewall o cortafuegos, programa que monitoriza el tráfico y las conexiones de red y bloquea aquellas conexiones o programas que no se hayan autorizado de antemano, controlando tanto el tráfico entrante de Internet como el saliente hacia Internet” (Cabello García, 2014).
- Uso de antivirus.
- Realiza evaluaciones de la seguridad del entorno de forma interna anualmente
- Dispone de conexión inalámbrica.
- Conexión a internet siempre activa, por lo que podría existir una entrada abierta para intrusos o virus.
- No usa sistema de detección de intrusos para identificar los ataques a la seguridad.
- No posee un sistema de alarma para detectar e informar las intrusiones.
- Los equipos de red como el cableado, conmutador o switch, conexiones a internet no se encuentran en lugares cerrados y con llave.
- No realiza evaluaciones de la seguridad del entorno a través de terceros, estas evaluaciones podrían facilitar soluciones más objetivas de seguridad.
- Déficit en el acondicionamiento de aire para los equipos, lo que pudiera causar el deterioro o bajo rendimiento de los mismos.
- No existen políticas de seguridad.

Según la información obtenida existe una cantidad considerable de falencias que pueden causar o provocar situaciones que pongan en riesgo el funcionamiento o rendimiento de los equipos informáticos que posee la institución, así como también lo que podría ocasionar un grave incidente seria la desorganización de los cables eléctricos y de red, claramente este punto es tomado como vulnerable, por otra parte el que exista una persona encargada del área de la TIC´S

es de mucha importancia ya que es quien podrá tomar acciones puntuales que ayuden a contrarrestar dichas falencias. La función del responsable del área de la TIC´S es la "asegurar el funcionamiento de los sistemas de información y en gestionar los nuevos proyectos informáticos que puedan surgir ante las necesidades de su empresa o de los avances del sector" (Selta, 2013).

En el documento desarrollado por Mejía Londoño, Ramírez Galvis, & Rivera Cardona, expresa que: "muchos administradores en el área de sistemas ven únicamente la parte superficial de lo que son las vulnerabilidades y los ataques sobre los sistemas de información; veneran los antivirus, y los firewalls como típicos medios de prevención ante amenazas en los datos, pudiendo desconocer cuál es la realidad de fondo" (Mejía Londoño, Ramírez Galvis, & Rivera Cardona, 2012).

En la siguiente tabla se muestra de forma detallada las vulnerabilidades identificadas para la red de datos de la Unidad Educativa Zapotal, que podrían hacer que ciertas amenazas lleguen a concretarse teniendo consecuencias perjudiciales.

Tabla 1. Identificación de vulnerabilidades

Amenazas	Vulnerabilidades	Consecuencias
Fenómenos naturales	– No disponente de un Programa de Contingencia.	El funcionamiento del equipamiento físico podría ser perjudicado.
Desperfecto eléctrico	– Falla en ciertos reguladores de voltaje usado para los equipos de computación. – Desorganización de los cables de energía y red.	Los equipos podrían tener un mal funcionamiento.
Suciedad	– Mantenimiento irregular de los equipos.	Los equipos podrían bajar su rendimiento o dejar de funcionar.
Sobrecalentamiento de equipos	– Déficit de acondicionamiento de aire para los equipos.	
Delito informático	– Insuficiente personal especializado en el área de seguridad informática. – No existen políticas de seguridad. – No utilizan sistemas de detección de intrusos para identificar los ataques a la seguridad.	La información correría el riesgo de bajar los niveles óptimos de confidencialidad, integridad y disponibilidad.

Actos vandálicos	– Carencia de cámaras de vigilancia. – Insuficiente personal de vigilancia.	Los equipos corren el riesgo de ser perjudicados.
Desperfecto de los equipos	– No se encuentran registrados los equipos con mal funcionamiento. – No existe un cambio regular de los equipos deteriorados. – Insuficiente personal para resolver los inconvenientes ante cualquier desperfecto. – Los equipos de red como el cableado, conmutador o switch, conexiones a internet no se encuentran en lugares cerrados y con llave.	Los equipos estarían en riesgo de perder su funcionalidad con eficiencia.
Deficiencia en el servicio de internet	– Inestabilidad del servicio de internet.	La conectividad de la red de datos queda inactiva temporalmente.

Desprotección contra virus	– Uso de software antivirus desactualizado.	La información podría ser dañada por la infección de virus y afectar su confidencialidad, integridad y disponibilidad.
Carencia de tácticas para gestionar la red	– No disponen de políticas para una adecuada gestión de red.	Los servicios podrían ser afectados.

Elaboración propia.

Las vulnerabilidades identificadas en la red de datos de la Unidad Educativa Zapotal son clasificadas en:

Vulnerabilidades Naturales

- No disponente de un Programa de Contingencia.

Vulnerabilidades Físicas

- Desorganización de los cables de energía y red.
- Carencia de cámaras de vigilancia.
- Insuficiente personal de vigilancia.
- Insuficiente personal para resolver los inconvenientes ante cualquier desperfecto.
- Los equipos de red como el cableado, conmutador o switch, conexiones a internet no se encuentran en lugares cerrados y con llave.

Vulnerabilidad de Hardware

- Mantenimiento irregular de los equipos.
- Déficit de acondicionamiento de aire para los equipos.
- Falla en ciertos reguladores de voltaje.
- No existe un cambio regular de los equipos deteriorados.

Vulnerabilidad organizacional

- Insuficiente personal especializado en el área de seguridad informática.
- No existen políticas de seguridad.
- No se encuentran registrados los equipos con mal funcionamiento.

- Inestabilidad del servicio de internet.
- No disponen de políticas para una adecuada gestión de red.

Vulnerabilidad de Software

- No utilizan sistemas de detección de intrusos para identificar los ataques a la seguridad.
- Uso de software antivirus desactualizado.

A continuación mediante un análisis FODA se identifican las principales debilidades, fortalezas, amenazas y oportunidades que tiene la red de datos y la institución, este análisis se representa en la siguiente matriz cuadrada.

Análisis FODA

FORTALEZAS	OPORTUNIDADES
– Uso de antivirus. – Realiza evaluaciones de la seguridad del entorno de forma interna anualmente. – Uso firewalls, para proteger la red contra ataques o infecciones por virus.	– Adaptación nuevas tecnologías dentro de las institución como por ejemplo, lector de huellas para el control de asistencia de docentes, personal administrativo, y auxiliares. – Existencia una persona responsable en el área de las TIC´S.
DEBILIDADES	**AMENAZAS**
– No existen políticas de seguridad. – Los equipos de red como el cableado, conmutador o switch, conexiones a internet no se encuentran en lugares cerrados y con llave. – Desorganización de los cables de energía y red. – Falta de cámaras de vigilancia para la seguridad de los equipos. – Déficit en el acondicionamiento de aire para los equipos	– Desperfecto eléctrico – Suciedad en el área donde se encuentran los equipos. – Carencia de tácticas para gestionar la red.

III. Conclusiones

Las redes en general se caracterizan por ser un medio de trasmisión de datos, que permiten habilitar el uso compartido de recursos dentro de una empresa o institución, pero también se enfrentan a diferentes factores que pueden bajar el nivel de funcionamiento. Esto debido a la inexistencia de normas o políticas de seguridad, ciertas amenazas pueden llegar a precisarse a causa de las vulnerabilidades que tenga la red como ya ha sido mencionado anteriormente en el desarrollo del estudio, esto conlleva a deducir criterios sobre la importancia de identificar dichas vulnerabilidades.

La conservación inapropiada de los equipos, en lo que se refiere a la temperatura del ambiente al momento de trabajar con las PC’s, es considerado un punto vulnerable que puede generar desgaste en el funcionamiento del equipo e, incluso, dañar la máquina, por lo tanto es indispensable tomar medidas necesarias para proteger los equipos del calor excesivo, ya que las computadoras son el elemento principal para conformar una red.

Las vulnerabilidades identificadas mediante este estudio dan a conocer como se encuentra la red y sus componentes, estos resultados muestra un nivel bajo de seguridad y alto en vulnerabilidad, debido a la poca atención que se le da a la seguridad informática en general, aunque la persona encargada del área de las TIC´S es quien puede llegar a conseguir que esta situación mejore, empezando por la creación de políticas de seguridad que pueden variar según la infraestructura de la red y la necesidad de la institución, sería factible también organizar un grupo de trabajo especializado que se encargue de administrar y gestionar la red, mitigando los problemas que se puedan presentar.

Bibliografía

CCM. (2016). Protección - Introducción a la seguridad de redes. *CCM (es.ccm.net)*, 1.

Aguilera López, P. (2011). *Seguridad informática.* Editex.

Berral Montero, I. (2014). *Instalación y mantenimiento de redes para transmisión de datos.* Madrid: Paraninfo.

Cabello García, J. M. (2014). *Operaciones auxiliares con Tecnologías de la Información y la Comunicación. IFCT0108.* IC.

Carpentier, J.-F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas.* Ediciones ENI.

Castallanos, L. R. (2015). *Seguridad en Informatica.*

Castro Gil, M. A., Díaz Orueta, G., Alzórriz Armendáriz, I., & Sancristóbal Ruiz, E. (2014). *PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES.* Madrid: UNED.

Castro Reynoso, S. (2012). *Los 27 controles críticos de la seguridad informática.*

Castro Reynoso, S. (2013). *Arquitectura de la seguridad informática.*

CCM . (2016). Introducción a la seguridad informática. *CCM (es.ccm.net)*, 1.

Gonzáles Orellana, A. P., & Rolando Tenem, D. (Diciembre de 2012). *bibdigital.* Obtenido de bibdigital.epn.edu.ec: http://bibdigital.epn.edu.ec/bitstream/15000/6020/1/CD-4774.pdf

Guillén, T. E. (Enero de 2013). *redicces.* Obtenido de redicces.org.sv: https://www.google.com.ec/url?sa=t&source=web&rct=j&url=http://www.redicces.org.sv/jspui/bitstream/10972/1667/1/07-%2520Estudio%2520de%2520la%2520seguridad%2520de%2520la%2520red%2520de%2520datos%2520de%2520ITCA-FEPADE.pdf&ved=0ahUKEwiiu6H1nIvTAhUCySYKHeLw

ISOTools. (s.f.). Obtenido de ISOTools: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Martinez. (17 de Julio de 2015). *DesdeLinux*. Obtenido de https://blog.desdelinux.net/kali-linux-suite-seguridad-informatica/

Medina, J. (2014). *Evaluacion de Vulnerabilidades TIC.*

Mejía Londoño, C. A., Ramírez Galvis, N. J., & Rivera Cardona, J. S. (2012). *repositorio.utp.* Obtenido de repositorio.utp.edu.co: https://www.google.com.ec/url?sa=t&source=web&rct=j&url=http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2734/0058R173.pdf%3Fsequence%3D1&ved=0ahUKEwjxqK7pzonTAhUBNSYKHZXcD6wQFggjMAE&usg=AFQjCNFeOB27MZnS5fnbX36cSoa0GiOmJQ

Mendoza, M. Á. (12 de Noviembre de 2014). *welivesecurity*. Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2014/11/12/identificar-analizar-evaluar-vulnerabilidades/

Moro Vallina, M. (2013). *Infraestructuras de redes de datos y sistemas de telefonía.* Madrid: Paraninfo.

Rodríguez Duque, D. V., & Gonzáles Rogel, E. (2015). *eumed.* Obtenido de www.eumed.net/entelequia: https://www.google.com.ec/url?sa=t&source=web&rct=j&url=http://www.eumed.net/entelequia/pdf/2015/e18a07.pdf&ved=0ahUKEwi_vdqPtOrSAhUGNiYKHX8UCcMQFggyMAI&usg=AFQjCNF4cIsi6qAu_5wSezbmeF9V2j8DGQ&sig2=0AmePPq0cdB16vnMet1Znw

Selta. (18 de Junio de 2013). *Selta tu blog de tecnología*. Obtenido de http://www.selta.es/blog/gestion/la-funcion-del-responsable-tic.html

Anexos

- Cuestionario utilizado para la entrevista.

1. ¿La institución tiene conexión permanente a Internet?

    Si

    No

2. ¿Cree que la institución participa en la adopción de nuevas tecnologías?

    Si

    No

3. ¿Qué tipo de tecnología ha adoptado la institución en los últimos cinco años?

    _____

    _____

4. ¿Existen políticas de seguridad informática?

    Si

    No

5. ¿Los equipos informáticos cuentan con un acondicionamiento de aire adecuado?

    Si

- No

6. ¿La institución utiliza firewalls para proteger la red contra ataques o infecciones por virus?
   - Si
   - No

7. ¿La institución usa hardware o software de detección de intrusos para identificar los ataques a la seguridad?
   - Si
   - No

8. ¿Se utiliza antivirus acorde con la cantidad de empleados en la institución?
   - Si
   - No

9. ¿La red dispone de conexión inalámbrica?
   - Si
   - No

10. ¿Los equipos de red (conmutadores, cableado, conexiones a Internet) se encuentran en lugares cerrados con llaves y con acceso restringido?
    - Si

- No

11. ¿Realiza la institución evaluaciones de la seguridad del entorno a través de terceros? Y con qué frecuencia se llevan a cabo estas evaluaciones.

- Si
- No
- Trimestralmente
- Semanalmente
- Anualmente
- Cada dos años o menos

12. ¿Realiza la institución evaluaciones de la seguridad del entorno de forma interna? Y con qué frecuencia se llevan a cabo estas evaluaciones.

- Si
- No
- Trimestralmente
- Semanalmente
- Anualmente
- Cada dos años o menos