GUIA DE SEGURIDAD EN EL TRANSPORTE, AUTENTICACIÓN Y GESTIÓN DE CORREOS ELECTRÓNICOS OUTLOOK 2010 DE LA SECRETARIA DE EDUCACIÓN MUNICIPAL DUITAMA

CAMILO ERNESTO HOYOS MALES
(AUTOR)

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
FACULTAD DE INGENIERIA
ESPECIALIZACION EN SEGURIDAD DE LA INFORMACION
DUITAMA
2015

GUIA DE SEGURIDAD EN EL TRANSPORTE, AUTENTICACIÓN Y GESTIÓN DE CORREOS ELECTRÓNICOS OUTLOOK 2010 DE LA SECRETARIA DE EDUCACIÓN MUNICIPAL DUITAMA

CAMILO ERNESTO HOYOS MALES

Proyecto de grado presentado para optar por el título de Especialista en Seguridad de la Información

Asesor
Martín Camilo Cancelado Ruiz
Ingeniero de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
FACULTAD DE INGENIERIA
ESPECIALIZACION EN SEGURIDAD DE LA INFORMACION
DUITAMA
2015

DOCUMENTO IDENTIFICACIÓN

Nombre del Proyecto:

Guía de Seguridad en el Transporte, Autenticación y Gestión de Correos Electrónicos Outlook 2010 de la Secretaria de Educación Municipal Duitama

Versión: 3
Fecha: 1 de septiembre de 2015

	Nombre	**Fecha**
Integrante	Camilo Ernesto hoyos Males	
Contacto Cliente	Secretaria de Educación Municipal Duitama	

A Dios y a la Virgen María.

Por permitirme llegar hasta este punto, por darme la fortaleza necesaria para seguir adelante y nunca desfallecer ante los problemas presentados, por haberme dado salud y por las múltiples bendiciones que me ha dado.

A mi Madre ***Yaneth Elena Males Ortiz***

Por siempre estar presentes, por preocuparse, apoyarme y acompañarme en cada uno de los momentos difíciles y que con su grande sabiduría me guio por el mejor camino.

A mi Esposa e Hija ***Andrea Liliana Sánchez Castro y Gabriela Hoyos Sánchez.***

Que se esforzaron e hicieron todo lo posible para que yo pudiera lograr mis sueños, que siempre me han apoyado y motivado.

AGRADECIMIENTOS

Expreso mi sincero agradecimiento a:

A la **UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD a la FACULTAD DE INGENIERIA**, por ser la base fundamental para obtener este logro.

AL Ing. Martín Camilo Cancelado Ruiz Ingeniero de Sistemas, director del proyecto, por sus grandes aportes, por su orientación y apoyo constante de principio a fin para el desarrollo de este trabajo.

CONTENIDO

PAG

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

A

Autenticación: La autenticación es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente siendo autenticado puede ser una persona que usa un ordenador, un ordenador por sí mismo o un programa del ordenador. En un web de confianza, "autenticación" es un modo de asegurar que los usuarios son quien ellos dicen que ellos son.

C

Correo Electrónico: Es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente mediante sistemas de comunicación electrónicos.

Crackers: Persona que diseña o programa los esquemas de protección anti copia de los programas comerciales, que sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican, para así poder utilizar o vender copias ilegales.

Cifrado: Encriptación de una señal por el proveedor del programa para evitar su uso no autorizado. La señal puede ser recuperada para ser utilizada con autorización.

Código malicioso: Término que hace referencia a cualquier conjunto de códigos, especialmente sentencias de programación, que tiene un fin malicioso. Esta definición incluye tanto programas malignos compilados, como 83 macros y códigos que se ejecutan directamente, como los que suelen emplearse en las páginas web (scripts).

Contraseñas: Una contraseña o password es una serie secreta de caracteres que permite a un usuario tener acceso a un archivo, a un ordenador, o a un programa. En sistemas multiusos, cada usuario debe incorporar su contraseña antes de que el ordenador responda a los comandos.

F

Firewalls: Es un elemento de software y hardware utilizado en una red para prevenir algunos tipos de comunicaciones prohibidos según las políticas de red que se hayan definido en función de las necesidades de la organización responsable de la red. La idea principal de un firewall es crear un punto de control de la entrada y salida de tráfico de una red.

H

Hackers: Usuario especializado en penetrar sistemas informáticos con el fin de obtener información secreta. En la actualidad, el término se identifica con el de delincuente informático, e incluye a los cibernautas que realizan operaciones delictivas a través de las redes de ordenadores existentes.

P

Password: Forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña normalmente debe mantenerse en secreto ante aquellos a quienes no se les permite el acceso.

Phishing: Es un tipo de engaño creado por hackers malintencionados, con el objetivo de obtener información importante como números de tarjetas de crédito, claves, datos de cuentas bancarias, etc. El objetivo más común, suele ser la obtención de dinero del usuario que cae en la trampa. Por lo general, el engaño se basa en la ignorancia del usuario al ingresar a un sitio que presume legal o auténtico.

PSI: Políticas de seguridad informática, forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.
Protocolo: Uno o un conjunto de procedimientos destinados a estandarizar un comportamiento humano o sistémico artificial frente a una situación específica.

S

Seguridad Informática: Consiste en asegurar que los recursos de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Servidores: Es un tipo de software que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos.

SGSI: Sistema de Gestión de la seguridad de la Información, como el nombre lo sugiere, un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001.
Spam: Son mensajes no solicitados y enviados comúnmente en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es por correo electrónico. Otras tecnologías de Internet que han sido objeto de spam incluyen grupos de noticias, motores de búsqueda y blogs. El spam también puede tener como objetivo los celulares a través de mensajes de texto y los sistemas de mensajería instantánea.

Spyware: es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

T

Tecnologías de la Información: Son un conjunto de técnicas, desarrollos y dispositivos avanzados que integran funcionalidades de almacenamiento, procesamiento y transmisión de datos.

TIC: Las Tecnologías de la Información y la Comunicación, también conocidas como TIC, son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Abarcan un abanico de soluciones muy amplio. Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesar información para poder calcular resultados y elaborar informes.

V

Vulnerabilidad: Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:

Permitir que un atacante ejecute comandos como otro usuario

Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos

Permitir a un atacante hacerse pasar por otra entidad

Permitir a un atacante realizar una negación de servicio

RESUMEN

TITULO. GUÍA DE SEGURIDAD EN EL TRANSPORTE, AUTENTICACIÓN Y GESTIÓN DE CORREOS ELECTRÓNICOS OUTLOOK 2010 DE LA SECRETARIA DE EDUCACIÓN MUNICIPAL DUITAMA

AUTOR: Camilo Ernesto Hoyos Males
PALABRAS CLAVES: Seguridad, seguridad de la información, Implementación, Correo Electrónico, Secretaria de Educación, niños, niñas y adolescentes, usuario final.

DESCRIPCIÓN

Con este proyecto se busca minimizar la vulnerabilidad en el transporte, autenticación y gestión de correos Outlook 2010 lo que nos permite aumentar la seguridad al servidor y a los equipos de los usuario de correos Outlook de la Secretaria de Educación Municipal Duitama, además de proteger la información, evitando al máximo el robo de esta de los diferentes delincuentes informáticos que observan en ella una fuente lucrativa para ser comercializada al mejor postor, lo anterior se hace posible por la explotación de vulnerabilidades que presenta en un gran porcentaje la no implementación de las herramientas de seguridad en estos servidores, facilitando el actuar de los delincuentes informáticos que no cesan nunca en su actuar buscando ingreso a bases de datos como la que maneja SIMAT de la Secretaria de Educación Municipal la que cuenta con toda la información personal de los estudiantes matriculados(niños, niñas y adolescentes) en los diferentes establecimientos educativos del sector oficial, así mismo información confidencial de estrategias de permanencia, proyectos de inclusión y bases de información de beneficiarios de los diferentes proyectos de transporte, alimentación y necesidades educativas de la cual son beneficiarios niños, niñas y adolescentes menores de edad en condición de vulnerabilidad.

ABSTRACT

TITLE. SAFETY GUIDE ON TRANSPORT, AUTHENTICATION AND MANAGEMENT OF EMAILS OUTLOOK 2010 OUTLOOK OF THE MUNICIPAL SECRETARY OF EDUCATION DUITAMA.

AUTHOR: Camilo Ernesto Hoyos Males
KEYWORDS: Security, security of the information, Implementation, Email, Secretariat of Education, children and adolescents end user.

DESCRIPTION.

This project seeks to minimize the vulnerability of transport, authentication and management of post Outlook 2010 which allows us to increase security to the server and the computers user Post Outlook of the Municipal Secretary of Education Duitama, and protect information avoiding the most of this theft of computer criminals different observing a lucrative source to be marketed to the highest bidder in it, the above is made possible by exploiting vulnerabilities posing in a large percentage of non-implementation tools security on these servers, facilitating the act of cyber criminals who never cease their actions seeking entry to databases such as handling SIMAT Municipal Secretary of Education which has all the personal information of enrolled students (boys and girls) in the different educational establishments in the formal sector, likewise confidential information retention strategies, projects and information bases inclusion of beneficiaries of the various projects for transportation, food and educational needs which beneficiaries are children and adolescents under age condition of vulnerability.

1. INTRODUCCIÓN

El presente trabajo da a conocer la importancia de minimizar la vulnerabilidad en el transporte, autenticación y gestión de correos Outlook 2010 lo que nos permite aumentar la seguridad al servidor y a los equipos de los usuario de correos Outlook de la Secretaria de Educación Municipal Duitama, buscando minimizar y mitigar vulnerabilidades a los servicios de correo Outlook 2010, además de proteger la información, evitando al máximo el robo de esta de los diferentes delincuentes informáticos que observan en ella una fuente lucrativa para ser comercializada al mejor postor todo esto se hace posible por la explotación de las vulnerabilidades que presenta en un gran porcentaje la no implementación de las herramientas de seguridad en estos servidores, facilitando el actuar de los delincuentes informáticos que no cesa nunca en su actuar buscando ingreso a bases de datos como las que maneja la Secretaria de Educación Municipal las cuales cuentan con toda la información personal de los estudiantes matriculados en los diferentes establecimientos educativos en el sector oficial, así mismo información confidencial de estrategias de permanencia, proyectos de inclusión y bases de información de beneficiarios de los diferentes proyectos de transporte, alimentación y necesidades educativas de la cual son beneficiarios niños, niñas y adolescentes menores de edad en condición de vulnerabilidad.

2. DESCRIPCIÓN DEL PROBLEMA

2.1 Planteamiento del Problema.

Debido al avance de la tecnología y la necesidad de comunicación rápida y segura las instituciones buscan la protección de su información de las vulnerabilidades y riesgos que existen en la red y que puedan poner en riesgo la información personal de menores de edad la cual es atractiva a los ataques de personas inescrupulosas como es el caso de la Secretaria de Educación del Municipio de Duitama que requiere implementar la seguridad en el transporte y gestión de los correos electrónicos dentro de sus diferentes dependencias y los 32 establecimientos educativos los cuales tienen la responsabilidad del manejo de la información personal de más de 16.630 educandos niños, niñas y adolescentes matriculados en los establecimientos oficiales de la ciudad de Duitama.

2.2 Formulación del problema

¿Qué estrategias a nivel de implementación se pueden aplicar entre un servidor y un cliente de correos Outlook 2010 de la Secretaria de Educación Municipal Duitama para que se establezcan mejoras de seguridad en cifrado y autenticación?

3. OBJETIVOS

3.1 Objetivo general.

Establecer los mecanismos de implementación en un cliente de correo Outlook 2010 que permitan minimizar vulnerabilidad en el transporte, autenticación y gestión de correo electrónico Outlook 2010 de la Secretaria de Educación Municipal Duitama.

3.2 Objetivos específicos.

- Identificar, clasificar y jerarquizar los mecanismos, protocolos y herramientas de gestión que permitan dar un mayor nivel de seguridad a la administración de correos electrónicos con Outlook (2010) de Microsoft.
- Capacitar y concientizar al usuario final sobre la manera adecuada de administrar su correo de forma responsable y así evitar vulnerar su privacidad.
- Evidenciar la vulnerabilidad asociadas a los mecanismos básicos seguros que deben implementarse en los cliente de correo.
- Realizar una comparación con un servidor Outlook implementado en la Secretaria de Educación Municipal y poder medir factores de riesgo asociados a estrategias seguras y optimizadas para garantizar seguridad de la información confidencial y personal de más de 16.000 niñas, niños y adolescentes y la comunicación con el servidor.

4. JUSTIFICACIÓN

Los servicios de correo electrónico con sus especificaciones y protocolos como (POP, SMTP, IMAP), son por diseño originalmente vulnerables a diferentes ataques pasivos o activos que afectan confidencialidad, contenido y filtrado de mensajes e interceptación de sesiones, usuarios y contraseñas.

Existen muchas aplicaciones de usuarios (como Outlook, Eudora, Netscape Thunderbird) entre otras, que para usuario final le permite administrar cierta seguridad y parametrizar ciertos criterios seguros que son caracterizados o definidos desde el lado servidor y algunas desde el lado cliente pero que no son suficientes cuando se maneja bases de datos tan importantes como es la información confidencial que contiene los datos personales de más de 16.000 estudiantes niños, niñas y adolescentes menores de edad que se encuentran matriculados en los Establecimiento Educativos oficiales del Municipio de Duitama.

Por lo anterior se hace necesario implementar el conjunto de mecanismos de seguridad desde el lado servidor y desde el lado de la gestión y aplicación de usuario para minimizar o mitigar vulnerabilidades a los servicios de correo Outlook de la Secretaria de Educación Municipal Duitama, que van desde la aplicación de estrategias o medidas preventivas a los escuchas de red, mecanismos de autenticación y cifrado, filtros con entidades de confianza y esquemas de trabajo en entornos seguros.

La información y su confidencialidad es un tema de gran importancia, tanto a nivel personal como empresarial, las consecuencias que se derivan de la mala utilización de las herramientas han contribuido a una degradación importante de los servicios de mensajería y correo electrónico, permitiendo la proliferación de "correo basura", robo de información y suplantación de entidades poniendo en entredicho la imagen de las organizaciones en la que los delincuentes informáticos observan una fuente lucrativa el hurto de información para ser comercializada al mejor postor y todo esto es posible por la explotación de las vulnerabilidades que presenta en un gran porcentaje en la no implementación de las herramientas de seguridad en estos servidores que se encuentran en el mercado para la ejecución de las mismas, facilitando el actuar de los delincuentes informáticos que no cesan nunca en su actuar buscando ingreso a bases de datos como las que maneja la Secretaria de Educación Municipal las cuales cuentan con toda la información personal de los estudiantes matriculados en los diferentes establecimientos educativos tanto en el sector oficial.

Una de las formas de mitigar tanto riesgo, es a la hora de implementar este tipo de servicios de correo. El hecho de establecer un conjunto ordenado y jerárquico de herramientas, protocolos, estándares y mecanismo de autenticación y cifrado,

seguramente permitirán minimizar las vulnerabilidades que presentan los gestores de correos, lo que replicaría a los usuarios finales de los correos dándoles mayor seguridad en el transporte de información generando credibilidad y confianza en la institución. Si bien es cierto que no todos los clientes de correo permiten asociar mecanismos de mejora ya sea a nivel de autenticación de usuario, replica de servicios, protocolos en la capa de transporte, extensiones de los mismos protocolos como APOP, SASL, TLS, máscaras y filtros, la mayoría son compatibles con los servicios más comunes. Para el caso se ha tomado como referente de estudio Outlook de Microsoft en su versión 2010. Las mejoras de estos clientes, ya permite activar mecanismos de autenticación y cifrado además de otras características como las de respuesta y parametrización automática cuando el servidor así lo perite y que se tendrán en cuenta en este estudio

5. TITULO DE PROYECTO

Implementar mecanismos de seguridad en el transporte, autenticación y gestión de correos electrónicos outlook 2010 de la secretaria de educación municipal duitama

6. DELIMITACION

6.1 Espacial.

El proyecto se realizará en el departamento de Boyacá, para ser implementado en el servidor de correos Outlook de la Secretaria de Educación del Municipio de Duitama. Se entregarán las recomendaciones y las metodologías para su puesta en marcha y control.

6.2 Temporal.

El proyecto se desarrollará en el transcurso del año 2015.

7. MARCO CONCEPTUAL

En esta sección se definen los conceptos generales relacionados con seguridad de la información aplicadas a correos Outlook 2010 y las estrategias requeridas para una implementación segura entre un servidor y un cliente de la Secretaria de Educación de Duitama. Estos conceptos y esquemas, son la base conceptual para el desarrollo del diseño teórico y el análisis del estudio planteado.

7.1 Correo electrónico.

Es utilizado a diario por millones de personas. Para muchos constituye la base diaria de su comunicación en el trabajo y el ámbito personal. De hecho, cuando enviamos un correo utilizando el **protocolo SMtP** o lo recibimos a través de **PoP3/iMAP**, tenemos que saber que tanto el usuario como la contraseña de la cuenta se envían en texto plano sin encriptar. Es decir, cualquier persona conectada a nuestra red o a la del servidor con un **sniffer de red** (**capturador de paquetes**) debidamente configurado podría ver esa información y, por supuesto, interceptar los paquetes dentro de los que viajan los datos de nuestros correos electrónicos. El funcionamiento del correo electrónico es similar al del **correo postal**. Ambos permiten enviar y recibir mensajes, que llegan a destino gracias a la existencia de una **dirección**. El correo electrónico también tiene sus propios buzones: son los **servidores** que guardan temporalmente los mensajes hasta que el destinatario los revisa.

7.2 Correo Outlook.

Outlook es un software que no solo le permite enviar, recibir y administrar el correo electrónico, sino que también administra el calendario y los contactos, como amigos y socios empresariales. Además, también puede compartir su calendario con familiares y colegas a través de Internet.

Outlook forma parte de “Office”, un conjunto de productos que combina varios tipos de software para crear documentos, hojas de cálculo y presentaciones, y para administrar el correo electrónico[1].

[1] Cómo usar Outlook. Grupo Microsoft. En Línea< https://support.office.com/es-es/article/>.

7.2.1 Novedades en su versión Outlook 2010

La versión del 2010 incluye:

- **Interfaz gráfica de usuario**: con la cinta de opciones (*Ribbon*) en todas las vistas. Esta es quizás la diferencia más notoria para los usuarios, y unifica visualmente al Outlook con el resto de aplicaciones de Microsoft.
- **Avisos de "Póngase en contacto",** mostrados en tarjetas con detalles de todos los participantes de mensajes registrados de su *Global Address List* (GAL) o por el propio usuario.
- **Agrupación de las conversaciones mejoradas:** incluye los mensajes de todas las carpetas y, opcionalmente, de una cuenta separada.
- **Mejora barra "Tareas pendientes":** En esta opción, por ejemplo, se muestran cuántas citas no se despliegan cuando el espacio es limitado.
- Opción "La gente del panel" y presentación de redes sociales.

7.2.2 Características de seguridad en correos Outlook.

Estas capacidades multimedia, sumadas a la característica de pre visualización, han permitido la proliferación de virus informáticos tipo gusano (*worm*) que se difunden a través de este programa (tan sólo al modificar su funcionamiento). Es mucho más que recomendable utilizarlo sólo en modo texto, o utilizar MUA's alternativos.

Así, se aconseja siempre configurar el programa para impedir la visualización de contenido activo, especialmente el uso de ActiveX en los mensajes, que es particularmente peligroso. Esto puede hacerse desactivando el panel de vista previa y configurando Internet Explorer de forma que Outlook Express advierta al usuario de la presencia de ActiveX y lance una pregunta para que éste decida si permite o no su ejecución. Esto permite que el usuario pueda autorizar su ejecución sólo cuando sea realmente necesaria.

7.3 Protocolos de Correo.

7.3.1 Protocolos de transporte de correo

La entrega de correo desde una aplicación cliente a un servidor, y desde un servidor origen al servidor destino es manejada por el Protocolo simple de transferencia de correo (Simple Mail Transfer Protocol o SMTP).

7.3.1.1 Protocolo SMTP.

El **protocolo SMTP** (Protocolo simple de transferencia de correo) es el protocolo estándar que permite la transferencia de correo de un servidor a otro mediante una conexión punto a punto.

Éste es un protocolo que funciona en línea, encapsulado en una trama TCP/IP. El correo se envía directamente al servidor de correo del destinatario. El protocolo SMTP funciona con comandos de textos enviados al servidor SMTP (al puerto 25 de manera predeterminada). A cada comando enviado por el cliente (validado por la cadena de caracteres ASCII CR/LF, que equivale a presionar la tecla Enter) le sigue una respuesta del servidor SMTP compuesta por un número y un mensaje descriptivo.

Las especificaciones básicas del protocolo SMTP indican que todos los caracteres enviados están codificados mediante el código ASCII de 7 bits y que el 8° bit sea explícitamente cero. Por lo tanto, para enviar caracteres acentuados es necesario recurrir a algoritmos que se encuentren dentro de las especificaciones MIME:

- **base64** para archivos adjuntos
- **quoted-printable** (abreviado *QP*) para caracteres especiales utilizados en el cuerpo del mensaje

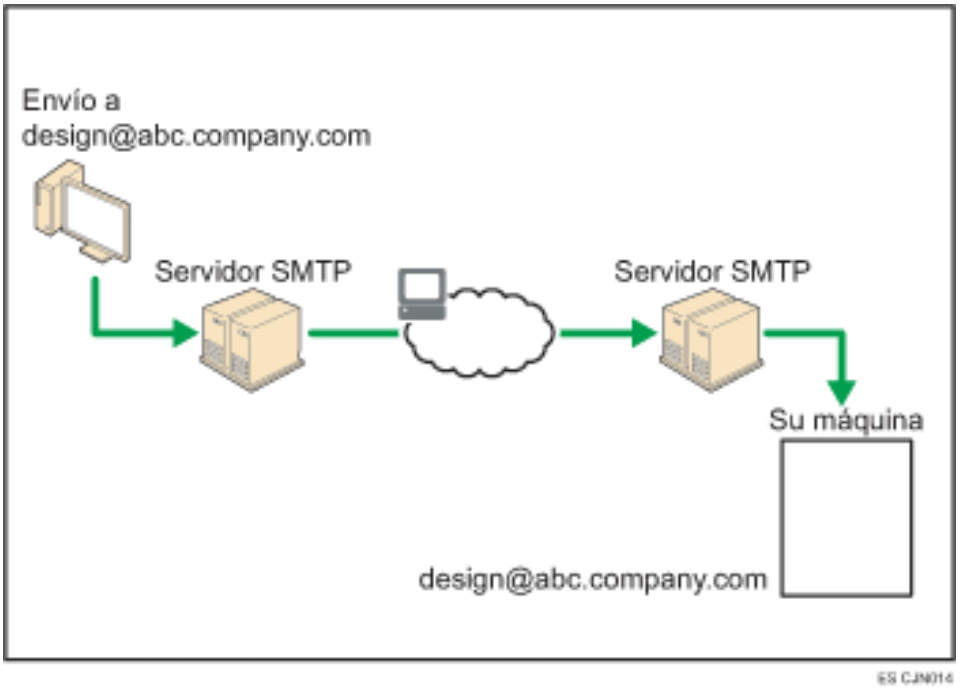
*** Principales comandos SMTP:**

Comando	Ejemplo	Descripción
HELO (ahora EHLO)	EHLO 193.56.47.125	Identificación que utiliza la dirección IP o el nombre de dominio del equipo remitente
MAIL FROM:	MAIL FROM: originator@domain.com	Identificación de la dirección del remitente

RCPT TO:	RCPT TO: recipient@domain.com	Identificación de la dirección del destinatario
DATA	DATA message	Cuerpo del correo electrónico
QUIT	QUIT	Salida del servidor SMTP
HELP	HELP	Lista de comandos SMTP que el servidor admite

Tabla 1. Principales Protocolos SMTP

Figura 1. Protocolo SMTP



Fuente: http://es.ccm.net/contents/279-protocolos-de-mensajeria-smtp-pop3-e-imap4#el-protocolo-smtp

7.3.2 *Protocolos de acceso a correo.*

Hay dos protocolos principales usados por las aplicaciones de correo cliente para recuperar correo desde los servidores de correo: el *Post Office Protocol* (*POP*) y el *Internet Message Access Protocol* (*IMAP*).

A diferencia de SMTP, estos protocolos requieren autenticación de los clientes usando un nombre de usuario y una contraseña. Por defecto, las contraseñas para ambos protocolos son pasadas a través de la red sin encriptar.

7.3.2.1 Protocolo POP3.

El **protocolo POP** (*Protocolo de oficina de correos*), como su nombre lo indica, permite recoger el correo electrónico en un servidor remoto (servidor POP). Es necesario para las personas que no están permanentemente conectadas a Internet, ya que así pueden consultar sus correos electrónicos recibidos sin que ellos estén conectados.

Existen dos versiones principales de este protocolo, POP2 y POP3, a los que se le asignan los puertos 109 y 110 respectivamente, y que funcionan utilizando comandos de texto radicalmente diferentes.

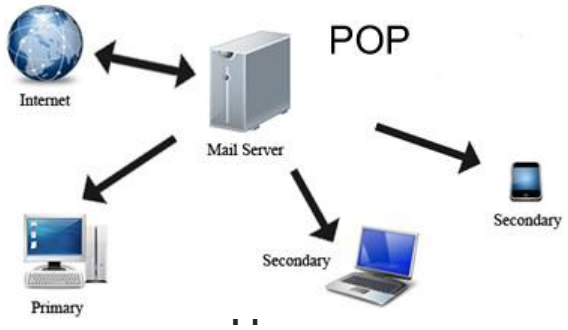
Al igual que con el protocolo SMTP, el protocolo POP (POP2 y POP3) funciona con comandos de texto enviados al servidor POP. Cada uno de estos comandos enviados por el cliente (validados por la cadena *CR/LF*) está compuesto por una palabra clave, posiblemente acompañada por uno o varios argumentos, y está seguido por una respuesta del servidor POP compuesta por un número y un mensaje descriptivo.

Principales comandos POP2:

Comandos POP2	
Comando	**Descripción**
HELLO	Identificación que utiliza la dirección IP del equipo remitente
FOLDER	Nombre de la bandeja de entrada que se va a consultar
READ	Número del mensaje que se va a leer
RETRIEVE	Número del mensaje que se va a recoger
SAVE	Número del mensaje que se va a guardar
DELETE	Número del mensaje que se va a eliminar
QUIT	Salida del servidor POP2

Tabla 2. Principales Protocolos POP2

Figura 2. Protocolo POP2



Fuente: http://es.ccm.net/contents/279-protocolos-de-mensajeria-smtp-pop3-e-imap4#el-protocolo-smtp

- **Principales comandos POP3:**

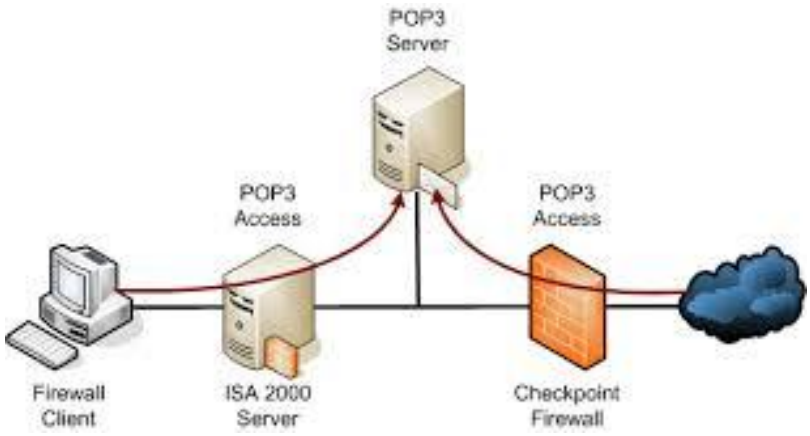
Comandos POP3	
Comando	**Descripción**
USER identification	Este comando permite la autenticación. Debe estar seguido del nombre de usuario, es decir, una cadena de caracteres que identifique al usuario en el servidor. El comando USER debe preceder al comando *PASS*.
PASS password	El comando *PASS* permite especificar la contraseña del usuario cuyo nombre ha sido especificado por un comando *USER* previo.
STAT	Información acerca de los mensajes del servidor
RETR	Número del mensaje que se va a recoger
DELE	Número del mensaje que se va a eliminar
LIST [msg]	Número del mensaje que se va a mostrar
NOOP	Permite mantener la conexión abierta en caso de inactividad
TOP <messageID> <n>	Comando que muestra *n* líneas del mensaje, cuyo número se da en el argumento. En el caso de una respuesta positiva del servidor, éste enviará de vuelta los encabezados del mensaje, después una línea en blanco y finalmente la primera *n* línea del mensaje.
UIDL [msg]	Solicitud al servidor para que envíe una línea que contenga

	información sobre el mensaje que eventualmente se dará en el argumento. Esta línea contiene una cadena de caracteres denominada *unique identifier listing (lista de identificadores únicos)* que permite identificar de manera única el mensaje en el servidor, independientemente de la sesión. El argumento opcional es un número relacionado con un mensaje existente en el servidor POP, es decir, un mensaje que no se ha borrado.
QUIT	El comando *QUIT* solicita la salida del servidor POP3. Lleva a la eliminación de todos los mensajes marcados como eliminados y envía el estado de esta acción.

Tabla 3. Principales Protocolos POP3

Por lo tanto, el protocolo POP3 administra la autenticación utilizando el nombre de usuario y la contraseña. Sin embargo, esto no es seguro, ya que las contraseñas, al igual que los correos electrónicos, circulan por la red como texto sin codificar (de manera no cifrada). En realidad, según RFC 1939, es posible cifrar la contraseña utilizando un algoritmo MD5 y beneficiarse de una autenticación segura. Sin embargo, debido a que este comando es opcional, pocos servidores lo implementan. Además, el protocolo POP3 bloquea las bandejas de entrada durante el acceso, lo que significa que es imposible que dos usuarios accedan de manera simultánea a la misma bandeja de entrada.

Figura 3. Protocolo POP3



Fuente: http://es.ccm.net/contents/279-protocolos-de-mensajeria-smtp-pop3-e-imap4#el-protocolo-smtp

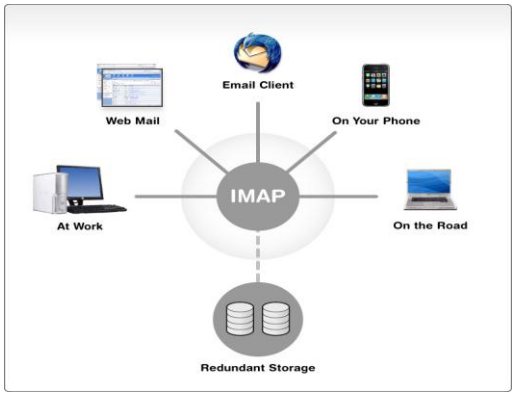
7.3.2.2 Protocolo IMAP.

El protocolo **IMAP** (Protocolo de acceso a mensajes de Internet) es un protocolo alternativo al de POP3, pero que ofrece más posibilidades:

- IMAP permite administrar diversos accesos de manera simultánea
- IMAP permite administrar diversas bandejas de entrada
- IMAP brinda más criterios que pueden utilizarse para ordenar los correos electrónicos

El servidor por defecto IMAP bajo Red Hat Enterprise Linux es /usr/sbin/imapd y es proporcionado por el paquete imap. Cuando utilice un servidor de correo IMAP, los mensajes de correo se mantienen en el servidor donde los usuarios pueden leerlos o borrarlos. IMAP también permite a las aplicaciones cliente crear, renombrar o borrar directorios en el servidor para organizar y almacenar correo. IMAP lo utilizan principalmente los usuarios que acceden a su correo desde varias máquinas. El protocolo es conveniente también para usuarios que se estén conectando al servidor de correo a través de una conexión lenta, porque sólo la información de la cabecera del correo es descargada para los mensajes, hasta que son abiertos, ahorrando de esta forma ancho de banda. El usuario también tiene la habilidad de eliminar mensajes sin verlos o descargarlos. Por conveniencia, las aplicaciones cliente IMAP son capaces de hacer caché de los mensajes localmente, para que el usuario pueda hojear los mensajes previamente leídos cuando no se esté conectado directamente al servidor IMAP. IMAP, como POP, es completamente compatible con estándares de mensajería de Internet, tales como MIME, que permite los anexos de correo.

Figura 4. Protocolo IMAP



Fuente: http://es.ccm.net/contents/279-protocolos-de-mensajeria-smtp-pop3-e-imap4#el-protocolo-smtp

7.4 Seguridad de la información.

Es un término que hace referencia a la seguridad de activos de forma general, incluyendo la seguridad informática, la seguridad TIC y la seguridad de los datos.

7.4.1 Seguridad informática.

“Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información segura y confiable.”(Aguilera López, Purificación, 2010).

7.4.2 Clasificación.

7.4.2.1 Seguridad pasiva.

“Está construida por el conjunto de medidas que se implementan con el fin de minimizar la repercusión debida a un incidente de seguridad y permitir la recuperación del sistema. A estas medidas podemos llamarlas de corrección.” (Aguilera López, Purificación, 2010).

7.4.2.2 Seguridad activa.

“Los mecanismos y procedimientos que permiten prevenir y detectar riesgos para la seguridad del sistema de información constituyen la seguridad activa del mismo.” (Aguilera López, Purificación, 2010).

7.4.2.3 Seguridad física.

“Se utiliza para proteger el sistema informático utilizando barreras y mecanismos de control. Se emplea para proteger físicamente el sistema informático.
Las amenazas físicas se pueden producir provocadas por el hombre, de forma accidental o voluntaria, o bien por factores naturales.” (Aguilera López, Purificación, 2010).

7.4.2.4 Seguridad lógica.

“Se encarga de asegurar la parte del software de un sistema informático, que se compone de todo lo que no es físico, es decir, los programas y los datos.” (Aguilera López, Purificación, 2010).

7.4.3 Servicios de seguridad.

7.4.3.1 Confidencialidad: se refiere a la protección de la información respecto al acceso no autorizado, sea en los elementos computarizados del sistema o en elementos de almacenamiento.

7.4.3.2 Integridad: Protección de la información respecto a modificaciones no autorizadas, tanto a la almacenada en los elementos computarizados de la organización como la usada como soporte. Estas modificaciones pueden llevarse a cabo de manera accidental, intencional, o por errores de hardware-software.

7.4.3.3 Autenticidad: Garantía que el usuario autorizado tiene para usar un recurso y que no sea suplantado por otro usuario.

7.4.3.4 Control de Acceso: Posibilidad de controlar los permisos a cualquier usuario para acceder a servicios o datos de la organización.

7.4.3.5 No Repudio: Al ser transferido un conjunto de datos, el receptor no puede rechazar la transferencia, y el emisor debe poder demostrar que envió los datos correspondientes.

7.4.3.6 Disponibilidad de los recursos y de la información: Protección de los elementos que poseen la información de manera que en cualquier momento, cualquier usuario autorizado pueda acceder a ella, sin importar el problema que ocurra.

7.4.3.7 Consistencia: Capacidad del sistema de actuar de manera constante y consistente, sin variaciones que alteren el acceso a la información.

7.4.3.8 Auditoría: Capacidad para determinar todos los movimientos del sistema, como accesos, transferencias, modificaciones, etc., en el momento en que fueron llevados a cabo (fecha y hora).

7.4.3.9 Vulnerabilidad: Consiste en cualquier debilidad que puede explotarse para causar pérdida o daño del sistema. De esta manera, el punto más débil de seguridad de un sistema consiste en el punto de mayor vulnerabilidad de ese sistema.

7.4.3.10 Amenaza: Será cualquier circunstancia con el potencial suficiente para causar pérdida o daño al sistema. De esta manera, el punto más débil.

7.4.3.10.1 Tipos de Amenazas

Existen infinidad de modos de clasificar un ataque y cada ataque puede recibir más de una clasificación. Por ejemplo, un caso de ***phishing*** puede llegar a robar la contraseña de un usuario de una red social y con ella realizar una suplantación de la identidad para un posterior acoso, o el robo de la contraseña puede usarse simplemente para cambiar la foto del perfil y dejarlo todo en una broma.

7.4.3.10.1.1 Amenazas por el origen

El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, y con esto, se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo el hecho de que la red no esté conectada a un entorno externo, como Internet, no nos garantiza la seguridad de la misma. De acuerdo con el Computer Security Institute (CSI) de San Francisco aproximadamente entre el 60 y 80 por ciento de los incidentes de red son causados desde dentro de la misma[2].

Basado en el origen del ataque podemos decir que existen dos tipos de amenazas:

- ✓ **Amenazas internas:** Generalmente estas amenazas pueden ser más serias que las externas por varias razones como son:

- Si es por usuarios o personal técnico, conocen la red y saben cómo es su funcionamiento, ubicación de la información, datos de interés, etc. Además tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo, lo que les permite unos mínimos de movimientos.
- Los sistemas de prevención de intrusos o IPS, y *firewalls* son mecanismos no efectivos en amenazas internas por, habitualmente, no estar orientados al tráfico interno. Que el ataque sea interno no tiene que ser exclusivamente por personas ajenas a la red, podría ser por vulnerabilidades que permiten acceder a la red directamente: rosetas accesibles, redes inalámbricas desprotegidas, equipos sin vigilancia, etc.

- ✓ **Amenazas externas:** Son aquellas amenazas que se originan fuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la

[2] Fuente: https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica. visto en: http://www.gocsi.com

manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.

7.4.3.10.1.2 Amenazas por el efecto

El tipo de amenazas por el efecto que causan a quien recibe los ataques podría clasificarse en:

- Robo de información.
- Destrucción de información.
- Anulación del funcionamiento de los sistemas o efectos que tiendan a ello.
- Suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información, venta de datos personales, etc.
- Robo de dinero, estafas.

7.4.3.10.1.3 Amenazas por el medio utilizado

Se pueden clasificar por el *modus operandi* del atacante, si bien el efecto puede ser distinto para un mismo tipo de ataque:

- ✓ **Virus informático:** malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

7.4.3.10.2 Clasificación de las amenazas en función del tipo de alteración:

7.4.3.10.2.1 De interrupción: El objetivo de la amenaza es deshabilitar el acceso a la información; por ejemplo, destruyendo componentes físicos como el disco duro, bloqueando el acceso a los datos, o cortando o saturando los canales de comunicación.

7.4.3.10.2.2 De interpretación: Personas, programas o equipos no autorizados podrían acceder a in determinado recurso del sistema y captar información confidencial de la organización, como pueden ser datos, programas o identidad de personas.

7.4.3.10.2.3 De modificación: Personas, programas equipos no autorizados no solamente accederían a los programas y datos de un sistema de información sino que además los modificarían.

7.4.3.10.2.4 De fabricación: Agregarían información falsa en el conjunto de información del sistema.

7.4.3.10.3 Según su origen las amenazas se clasifican en.

7.4.3.10.3.1 Accidentales: accidentes meteorológicos, incendios, inundaciones, fallos en equipos, en las redes, en los sistemas operativos o en el software, errores humanos.

7.4.3.10.3.2 Intencionadas: Son debidas siempre a la acción humana, como a introducción de software malicioso, malware, intrusión informática, robos o hurtos.

7.4.3.10.3.3 Ataques: Se define como cualquier acción que explota una vulnerabilidad.

- ✓ **Ataques Pasivos:** Consiste en sólo observar comportamientos o leer información, sin alterar el estado del sistema ni la información. En este sentido, un ataque pasivo sólo afecta la confidencialidad o privacidad del sistema o de la información.
- ✓ **Ataques Activos:** Por el contrario, tiene la capacidad de modificar o afectar la información o el estado del sistema o ambos. En consecuencia, un ataque activo afecta no sólo la confidencialidad o privacidad sino también la integridad y la autenticidad de la información o del sistema.

7.4.3.10.3.4 Riesgos: Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad.

Figura 5. Riesgos Seguridad

Fuente: www.ISO27000.es

8. MARCO CONTEXTUAL

8.1 Secretaria de educación municipal Duitama.

8.1.1 Misión

La Secretaria de educación de Duitama es una organización de carácter oficial, que garantiza la prestación del servicio educativo integral a la comunidad, con altos índices de calidad, cobertura eficiencia, pertinencia, tecnologías de información y optimización de recursos; formando ciudadanos con valores para construir una sociedad competitiva y productiva.

8.1.2 Visión.

En el 2019 la Secretaria de Educación de Duitama será un modelo de gestión y transparencia a nivel nacional, con algos estándares de cumplimiento en políticas educativas, afrontando los retos que imponen la dinámica del entorno para contribuir con la información integral de la población y el desarrollo social de nuestro país.

8.1.3 Política de Calidad.

La secretaria de Educación de Duitama presta un servicio educativo integral a la comunidad garantizando una atención oportuna, eficiente, eficaz y pertinente, enfocada a satisfacer a sus usuarios mediante el cumplimiento de la normatividad vigente, inmerso en un proceso de mejoramiento continuo, que permita el aumento de la cobertura y la calidad educativa, a través del talento humano idóneo, comprometido con el desarrollo del sistema educativo de los niños, niñas y adolescentes del Municipio.

8.1.3.1 Objetivos de Calidad

- Fortalecer la educación del Municipio mediante el aumento de la cobertura educativa, el mejoramiento de la calidad educativa, con eficiencia y pertinencia, asegurando el cumplimiento de la política educativa de Duitama.
- Mejorar la educación integral de nuestra población, fomentado su formación en valores, para garantizar que nuestros niños, niñas y adolescentes de Duitama, sean buenos seres humanos

- Promover una educción participativa, incluyente e igualitaria en oportunidades, integrando al proceso educativo a la familia y a la sociedad en general.
- Aumentar el nivel de satisfacción de los usuarios que solicitan la prestación de los servicios de la Secretaria de Educación y atender oportunamente las preguntas, quejas, reclamos y sugerencias de los mismos.
- Implementar programas de bienestar y capacitación permanente a los funcionarios del sector Educativo de Duitama con el fin de contar con talento humano idóneo y comprometido con el desarrollo del sistema Educativo del Municipio.

8.1.4 Dependencias que conforman la secretaria de educación Duitama

La secretaria de Educación Municipal de Duitama tiene a su cargo las siguientes dependencias:

- DESPACHO SECRETARIA EDUCACION
- CALIDAD
- PERMANENCIA
- INCLUSION
- COBERTURA
- NOMINA DOCENTES
- PROYECTOS
- INVENTARIOS
- FINANCIERA
- JURIDICA
- INFORMATICA

Quienes tienen como objetivo primordial brindar apoyo a cada uno de los 31 Establecimientos educativos oficiales del Municipio en cada una de sus ramas que tienen a su cargo enviado permanentemente información de los estudiantes que se encuentran matriculados en los establecimientos de todo los proyectos que se llevan a cabo en cabeza de la Secretaria como los relacionados a continuación:

- Inclusión niños, niñas y adolescentes en estado de incapacidad (auditiva, cognitivas, etc)
- Ni uno Menos
- Transporte Escolar
- Alimentación Escolar PAE
- Experiencias Significativas en Permanencia Escolar
- Atención Especial a Población Vulnerable entre otros.

Todos estos programas están enfocados de manera prioritaria a la población en situación de desplazamiento o personas vulnerable de bajos recursos. Se gestiona

con las secretarías de educación estrategias de búsqueda y caracterización de la población afectada por la violencia y se promueve la articulación de estrategias para la permanencia educativa de la población. Se implementan acciones de atención psicoafectiva y proyectos educativos transversales en las instituciones en las que se atiende a esta población: Niños y niñas y adolescentes en situación de desplazamiento; niños y niñas y adolescentes desvinculados del conflicto; adultos desmovilizados; hijos e hijas de adultos desmovilizados; niños y niñas y adolescentes víctimas o en riesgo de reclutamiento forzado y utilización de niños y niñas y adolescentes por parte de actores ilegales; y niños y niñas y adolescentes víctimas o en riesgo de minas anti persona, niños y niñas y adolescentes en situaciones de emergencia por desastre o conflicto armado.

Por todo lo anterior la Secretaria de Educación Municipal de Duitama en aras de proteger la información personal de cada uno de los niños, niñas y adolescentes matriculados en los establecimientos oficiales requiere con urgencia realizar la protección a la información que de ella se genera ya que es para la delincuencia cibernética (que bien pudieran ser "Crackers" o "Hackers" expertos en informática) es uno de los mejores y más rentables negocios atacar servidores que contengan información personal de niños, niñas y adolescentes que van a poder contactar por diferentes medios para tratar de cautivar la atención de los jóvenes y sacarles información que posteriormente usarán para fines generalmente perversos. De acuerdo con *Online Victimization of Youth*, uno de cada siete menores entre 10 y 17 años, ha recibido alguna solicitación sexual en línea y de ellos solo la cuarta parte, informan a sus padres.

> Para Paulo Sergio Pinheiro (2005)
> La violencia contra los niños es un fenómeno que no conoce fronteras políticas, culturales, económicas ni tecnológicas. En las últimas décadas, el boom de las tecnologías de la información y la comunicación (TIC) ha creado formas totalmente nuevas de establecer y mantener relaciones. Ésa es una realidad cotidiana muy normal para muchos niños y jóvenes, y una posibilidad emocionante para el resto. Los niños son vulnerables, de muchas maneras diferentes, a múltiples formas de violencia que amenazan su integridad física y psicológica. Y al igual que en el mundo físico, se debe establecer un marco para proteger a los niños en el ciberespacio que se base en instrumentos sobre derechos humanos y derechos del niño. No obstante, por lo general nuestra capacidad de seguir el ritmo del cambio y de responder queda retrasada respecto de dicha necesidad. El Estudio sobre la Violencia contra los Niños, encargado por el Secretario General de las Naciones Unidas, fue concebido para analizar el alcance del problema y ofrecer alternativas concretas para detener la violencia contra los niños en todos los entornos, incluidos los entornos virtuales o “ciberespacio”. Agradezco inmensamente a ECPAT International por preparar este

completo informe a nivel mundial, La violencia contra los niños en el ciberespacio, como contribución al Estudio Mundial sobre la Violencia contra los Niños. Este informe asiste en la evaluación general de lo que se puede hacer para detener la violencia contra los niños en el contexto de las tecnologías de Internet y de las comunicaciones. La violencia contra los niños en el ciberespacio ofrece nuevas perspectivas sobre la profundidad y el alcance de la violencia y el daño que se puede causar a los niños en relación con las nuevas TIC. Reúne información de un modo nuevo. Desde la aparición de Internet, se ha puesto mucho énfasis en zanjar la brecha digital, y ahora este informe presta atención a la necesidad de incluir simultáneamente medidas de protección, especialmente para niños y jóvenes. Además de reconocer el gigantesco impacto positivo de las nuevas tecnologías y el hecho de que seguirán expandiéndose en el futuro, este informe ayuda a explicar los escollos y trampas, particularmente ha quien no sabe mucho del tema, y brinda algunas indicaciones sobre lo que se puede hacer al respecto.

8.2 Factores de vulnerabilidad

Los niños, niñas y adolescentes de todas las clases sociales corren el riesgo de quedar expuestos a cualquiera de estas formas de violencia relacionadas con las nuevas tecnologías, o a todas. Es muy probable que la posibilidad de daño se incremente si no se consideran los intereses de los niños en la planificación de los desarrollos, especialmente en la planificación cuya finalidad consiste en promover las nuevas tecnologías de información y comunicación (TIC) y resolver las desigualdades en el acceso a las mismas. No sólo corren riesgos los niños y adolescentes que ya utilizan las nuevas TIC sino también quienes lo harán en el futuro. Además, los niños que no tienen acceso a los dispositivos de comunicación más novedosos también pueden recibir la influencia de su uso. Esos niños son víctimas a quienes se fotografía, cuyas fotos son luego enviadas al ciberespacio, o son publicitados en línea como mercancía, y/o se ven afectados por la violencia y el daño producto de las interacciones en línea de otras personas, como el uso de pornografía. Algunos niños corren más riesgo debido a distintos factores que aumentan su vulnerabilidad, y que son comunes a todos los entornos: se encuentran en situaciones sociales o económicas difíciles, ya han sufrido daños tales como abuso o explotación sexual, están solos, se sienten aislados de sus padres u otras personas, tienen una baja autoestima o no tienen confían en sí mismos. El género también se considera un factor de riesgo, pues aparentemente son más niñas que niños quienes resultan dañados por las interacciones en el ciberespacio (a pesar de que la presencia de niños en imágenes pornográficas que circulan en Internet es cada vez mayor) [1]

[1] Muir D, La Violencia contra los niños en el Ciber Espacio. En Línea <http://www.ecpat.net/sites/default/files/Cyberspace_SPA.pdf>. Citado en Septiembre de 2005.

8.3 Responsables.

La responsabilidad en el mundo físico de garantizar la protección de niños y jóvenes y sus derechos también se aplica al ciberespacio y al uso de las nuevas TIC. El ciberespacio no es un espacio vacío sino un escenario social en el que a la gente le ocurren cosas, en el que ocurren cosas entre la gente y en el que las vulnerabilidades y los factores de riesgo del mundo físico se repiten. Las interacciones en el ciberespacio tienen consecuencias en el mundo físico. Los gobiernos Quienes toman decisiones y crean políticas dentro de los gobiernos, en los distintos niveles, tienen la responsabilidad de actuar para proteger a los niños en el ciberespacio. En los últimos años, algunos gobiernos han aprobado e implementado leyes, políticas y sistemas bien articulados entre sí para proteger a los niños en el ciberespacio. Algunos han establecido fuerzas especiales específicas y participadas activamente en las consultas y en la cooperación con los países limítrofes para prevenir la violencia contra los niños, especialmente en lo que respecta a los materiales que muestran abuso sexual de menores (pornografía infantil). Sin embargo, en su mayoría, estas acciones han tenido lugar en respuesta a situaciones en las que el daño resultó obvio después de que una nueva tecnología fue presentada, adaptada para su uso en forma dañina o por parte de delincuentes, y tal vez incorporada rápidamente. Mientras tanto, muchos otros gobiernos se retrasan en la toma de medidas específicas adecuadas. Aún existen discrepancias respecto de la forma en que los países definen el daño, la niñez y las sanciones en relación con los delitos por Internet.

8.4 Establecimientos educativos Duitama

La secretaria de educación municipal de Duitama tiene bajo su responsabilidad 14 Establecimiento Educativos oficiales y sus respectivas sedes conformando un total de 31 establecimientos que prestan el servicio educativo a los estudiantes matriculados SIMAT en el sector oficial relacionados en la siguiente Tabla No. 1.

ITEM	ESTABLECIMIENTOS EDUCATIVOS DUITAMA
I	**CENTRO EDUCATIVO QUEBRADA DE BECERRAS**
1	CENTRO EDUCATIVO QUEBRADA DE BECERRAS
2	CENTRO EDUCATIVO QUEBRADA DE BECERRAS SEDE SANTA ANA
II	**COLEGIO BOYACA DE DUITAMA**
3	COLEGIO BOYACA DE DUITAMA SEDE BACHILLERATO Y PRIMARIA
III	**COLEGIO GUILLERMO LEON VALENCIA**
4	PRINCIPAL INTEGRADO
5	SEDE CAMPOAMOR

6	SEDE GABRIELA MISTRAL
IV	**COLEGIO NACIONALIZADO LA PRESENTACION**
7	COLEGIO NACIONALIZADO LA PRESENTACIÓN SEDE CENTRO
8	COLEGIO NACIONALIZADO LA PRESENTACIÓN SEDE EL CARMEN
9	COLEGIO NACIONALIZADO LA PRESENTACION SEDE NORTE
V	**COLEGIO TECNICO MUNICIPAL FRANCISCO DE PAULA SANTANDER**
10	COLEGIO TECNICO MUNICIPAL FRANCISCO DE PAULA SANTANDER
11	SEDE LA MILAGROSA
VI	**COLEGIO TECNICO MUNICIPAL SIMON BOLIVAR**
12	COLEGIO TECNICO MUNICIPAL SIMÓN BOLIVAR
13	SEDE AGUATENDIDA
14	SEDE JAIRO ANIBAL NIÑO
15	SEDE SAN FERNANDO
VII	**I.E. AGROINDUSTRIAL LA PRADERA**
16	I.E. AGROINDUSTRIAL LA PRADERA – SEDE PRINCIPAL
17	SEDE LA FLORIDA
18	SEDE SANTA LUCIA
19	SEDE SIRATA
VIII	**I.E. SAN ANTONIO NORTE**
20	I.E. SAN ANTONIO NORTE – SEDE PRICIPAL
IX	**I.E. SAN LUIS**
21	SEDE SAN LUIS
22	SEDE TOCOGUA
X	**I.E.COLEGIO LA NUEVA FAMILIA**
23	CENTRO EDUCATIVO RURAL HIGUERAS
24	INSTITUCIÓN EDUCATIVA COLEGIO LA NUEVA FAMILIA – SEDE PRINCIPAL
XI	**INSTITUCION EDUCATIVA AGROINDUSTRIAL FRANCISCO MEDRANO**
25	INSTITUCION EDUCATIVA AGROINDUSTRIAL FRANCISCO MEDRANO
26	SEDE AVENDAÑOS DOS
XII	**INSTITUTO TECNICO INDUSTRIAL RAFAEL REYES-DUITAMA**
27	INSTITUTO TECNICO INDUSTRIAL RAFAEL REYES-DUITAMA
XIII	**INSTITUTO TECNICO JOSE MIGUEL SILVA PLAZAS**
28	INSTITUTO TÉCNICO JOSÉ MIGUEL SILVA PLAZAS
29	SEDE SAN LORENZO
XIV	**INSTITUTO TECNICO SANTO TOMAS DE AQUINO**

30	INSTITUTO TECNICO SANTO TOMAS DE AQUINO SEDE BACHILLERATO
31	INSTITUTO TECNICO SANTO TOMAS DE AQUINO SEDE PRIMARIA

Tabla 4. Establecimientos Educativos de Duitama

Fuente: Elaboración Propia

8.5 Simat (Sistema Integrado de Matriculas).

El sistema integrado de matrícula SIMAT es una herramienta que permite organizar y controlar el proceso de matrícula en todas sus etapas, así como tener una fuente de información confiable y disponible para la toma de decisiones.

SIMAT es un sistema de gestión de la matrícula de los estudiantes de instituciones oficiales que facilita la inscripción de alumnos nuevos, el registro y la actualización de los datos existentes de un alumno, la consulta de alumnos por Institución, el traslado del alumno a otra Institución, así como la obtención de informes como apoyo para la toma de decisiones.

Adicionalmente como apoyo a la matricula se tiene el registro y consulta de las instituciones, la creación de Sedes, jornadas, grados y grupos y el manejo de las novedades relacionadas con estas, permitiendo la actualización de su información cuando sea necesario.

Mediante la automatización de este proceso, se logra sistematizar, consolidar y analizar la información implicada en el mismo. Esto mejora los procesos de inscripción, asignación de cupos y matrícula y por ende el servicio a la comunidad.

El Sistema Integrado de Matrícula SIMAT permite además efectuar un seguimiento completo y detallado al proceso de matrícula mediante el análisis de los informes que provee.

Este manual[3] contiene las diferentes opciones de la aplicación que permiten el manejo anteriormente mencionado:

8.5.1 Directorio de Instituciones

Esta opción permite manejar la información de instituciones y llevar a cabo una serie de operaciones sobre ellas tales como insertar, modificar, crear, etc.

[1] Ministerio de Educación Nacional Republica de Colombia. Sistema Integrado de Matriculas. En línea <http://www.sistemamatriculas.gov.co/ayuda/whnjs.htm>. Citado en 2015.

Una Institución, en su funcionamiento, tiene Sedes, jornadas, niveles y modelos educativos. Esta opción del SIMAT permite el manejo y operación de los mismos.

8.5.2 Cortes y Carga de Datos.

En esta opción es posible la definición de fechas de corte para cada uno de los procesos. También permite la carga de datos mediante la importación de archivos.

8.5.3 Registro de Estudiantes.

Esta opción permite el manejo de información de los estudiantes. Habilita el registro de *información de un estudiante, su actualización, consulta y eliminación*. El objetivo del registro de estudiantes es tener una base de datos completa y actualizada de los alumnos. En él se encuentran la información de los estudiantes, sus padres y acudientes con toda su información y la Institución-Sede-jornada-grado en que se encuentra cada uno.

8.5.4 Proyecciones.

En esta opción es posible definir los parámetros para realizar la proyección y realizar la proyección en si misma. El objetivo de la proyección de cupos es tener una base real para prever y asegurar la continuidad de los alumnos antiguos y establecer la capacidad para atender las solicitudes de alumnos nuevos

8.5.5 Inscripciones.

Esta opción permite realizar inscripciones de alumnos nuevos o retirados. Es posible realizar una inscripción, consultarla y/o modificarla.
El objetivo de la inscripción de alumnos nuevos es el registro de la información de las solicitudes de cupo en las instituciones, para poder brindar el acceso a la educación a la población que lo solicita.
La inscripción tiene la información de los estudiantes, sus padres y acudientes y una lista, en orden de preferencia, de las instituciones en las cuales quisiera matricularse el alumno.

8.5.6 Promoción.

El objetivo del proceso de promoción es tomar los alumnos matriculados actualmente y llevarlos al grado siguiente para el año lectivo siguiente. Es importante tener en cuenta que si se trata del último grado, los alumnos no se promocionan, se gradúan. En esta opción es posible seleccionar si se desea realizar la promoción por jerarquía, por Institución, por Sede o por jornada.

8.5.7 Matrícula.

El objetivo final del proceso de matrícula es matricular alumnos tanto antiguos como nuevos en el sistema educativo, ya que esto permite la ampliación de la cobertura de la educación como respuesta a la necesidad de educación de la población. En esta opción es posible llevar a cabo la matrícula de los estudiantes que tienen un cupo asignado en alguna Institución, así como registrar los estudiantes reprobados y cancelar o anular el registro de repitencia realizado.

8.5.8 Reportes.

El módulo de reportes permite la obtención de informes del proceso de matrícula y sus etapas, con el fin de obtener información que alimenta el propio sistema, así como poder contar con información estadística que sea un apoyo real y oportuno a la gestión del proceso. Este módulo permite la producción de los reportes que genera el sistema.

8.5.9 Estudiantes establecimientos oficiales matriculados en SIMAT.

El proceso de matrícula es el conjunto de políticas, procedimientos y actividades, que permiten organizar la continuidad de los alumnos antiguos y el ingreso de alumnos nuevos, en el Sistema de Educación Oficial del País SIMAT, a continuación se relaciona Tabla No.5 la matricula del municipio de Duitama de los 31 Establecimientos educativos.

CUADRO CONSOLIDADO ESTUDIANTES NIÑOS, NIÑAS Y ADOLECENTES MATRICULADOS EN LOS ESTABLECIMIENTOS OFICIALES DEL MUNICIPIO DE DUITAMA

ESTABLECIMIENTOS EDUCATIVOS DUITAMA	0	1	2	3	4	5	6	7	8	9	10	11	TOTAL
CENTRO EDUCATIVO QUEBRADA DE BECERRAS	**17**	**11**	**18**	**20**	**5**	**15**	**18**	**24**	**13**	**10**			**151**
CENTRO EDUCATIVO QUEBRADA DE BECERRAS	10	9	14	12	4	10	18	24	13	10			124
CENTRO EDUCATIVO QUEBRADA DE BECERRAS SEDE SANTA ANA	7	2	4	8	1	5							27
COLEGIO BOYACA DE DUITAMA	**111**	**138**	**138**	**126**	**137**	**125**	**161**	**144**	**130**	**130**	**116**	**97**	**1553**
COLEGIO BOYACA DE DUITAMA SEDE BACHILLERATO							161	144	130	130	116	97	778
COLEGIO BOYACA DE DUITAMA SEDE PRIMARIA	111	138	138	126	137	125							775
COLEGIO GUILLERMO LEON VALENCIA	**218**	**320**	**304**	**310**	**315**	**365**	**438**	**432**	**377**	**375**	**390**	**366**	**4210**
PRINCIPAL INTEGRADO	168	202	234	244	244	267	438	432	377	375	390	366	3737
SEDE CAMPOAMOR	25	52	36	29	36	62							240
SEDE GABRIELA MISTRAL	25	66	34	37	35	36							233
COLEGIO NACIONALIZADO LA PRESENTACION	**180**	**207**	**197**	**222**	**214**	**226**	**247**	**195**	**206**	**174**	**198**	**142**	**2408**

COLEGIO NACIONALIZADO LA PRESENTACIÓN SEDE CENTRO			71	222	214	226							733
COLEGIO NACIONALIZADO LA PRESENTACIÓN SEDE EL CARMEN	180	207	126										513
COLEGIO NACIONALIZADO LA PRESENTACION SEDE NORTE							247	195	206	174	198	142	1162
COLEGIO TECNICO MUNICIPAL FRANCISCO DE PAULA SANTANDER	**46**	**62**	**52**	**83**	**74**	**82**	**145**	**122**	**84**	**105**	**84**	**65**	**1004**
COLEGIO TECNICO MUNICIPAL FRANCISCO DE PAULA SANTANDER	42	54	41	72	70	73	145	122	84	105	84	65	957
SEDE LA MILAGROSA	4	8	11	11	4	9							47
COLEGIO TECNICO MUNICIPAL SIMON BOLIVAR	**69**	**87**	**108**	**126**	**127**	**118**	**181**	**185**	**156**	**128**	**135**	**103**	**1523**
COLEGIO TECNICO MUNICIPAL SIMÓN BOLIVAR	15	19	29	34	36	35	181	185	156	128	135	103	1056
SEDE AGUATENDIDA	23	22	22	42	37	27							173
SEDE JAIRO ANIBAL NIÑO	12	14	28	28	29	24							135
SEDE SAN FERNANDO	19	32	29	22	25	32							159
I.E. AGROINDUSTRIAL LA PRADERA	**14**	**27**	**27**	**29**	**31**	**32**	**40**	**32**	**27**	**13**	**18**	**19**	**309**
I.E. AGROINDUSTRIAL LA PRADERA - SEDE PRINCIPAL	11	18	20	24	27	25	40	32	27	13	18	19	274
SEDE LA FLORIDA	1	2	4	2	2	4							15
SEDE SANTA LUCIA	1	4	1	1	1	3							11
SEDE SIRATA	1	3	2	2	1								9
I.E. SAN ANTONIO NORTE	**11**	**21**	**20**	**32**	**19**	**33**	**48**	**49**	**31**	**23**	**32**	**11**	**330**
I.E. SAN ANTONIO NORTE - SEDE PRICIPAL	11	21	20	32	19	33	48	49	31	23	32	11	330
I.E. SAN LUIS	**18**	**23**	**23**	**20**	**23**	**21**	**39**	**34**	**29**	**19**	**24**	**15**	**288**
SEDE SAN LUIS	18	20	23	19	22	17	39	34	29	19	24	15	279
SEDE TOCOGUA		3		1	1	4							9
I.E.COLEGIO LA NUEVA FAMILIA	**40**	**32**	**44**	**46**	**49**	**56**	**65**	**66**	**62**	**66**	**63**	**35**	**624**
CENTRO EDUCATIVO RURAL HIGUERAS			11	13	9	11							44
INSTITUCIÓN EDUCATIVA COLEGIO LA NUEVA FAMILIA - SEDE PRINCIPAL	40	32	33	33	40	45	65	66	62	66	63	35	580
INSTITUCION EDUCATIVA AGROINDUSTRIAL FRANCISCO MEDRANO	**5**	**6**	**8**	**2**	**5**	**5**	**9**	**15**	**15**	**14**	**14**	**12**	**110**
INSTITUCION EDUCATIVA AGROINDUSTRIAL FRANCISCO MEDRANO	4	4	5	2	4	5	9	15	15	14	14	12	103
SEDE AVENDAÑOS DOS	1	2	3		1								7
INSTITUTO TECNICO INDUSTRIAL RAFAEL REYES-DUITAMA	**104**	**130**	**134**	**144**	**144**	**147**	**166**	**152**	**160**	**175**	**125**	**112**	**1693**
INSTITUTO TECNICO INDUSTRIAL RAFAEL REYES-DUITAMA	104	130	134	144	144	147	166	152	160	175	125	112	1693
INSTITUTO TECNICO JOSE MIGUEL SILVA PLAZAS	**33**	**36**	**53**	**53**	**44**	**47**	**80**	**44**	**27**	**23**	**42**	**16**	**498**
INSTITUTO TÉCNICO JOSÉ MIGUEL SILVA PLAZAS							80	44	27	23	42	16	232
INSTITUTO TÉCNICO JOSÉ MIGUEL SILVA PLAZAS SECCIONAL PRIMARIA LA TRINIDAD	26	22	39	35	32	31							185
SEDE SAN LORENZO	7	14	14	18	12	16							81
INSTITUTO TECNICO SANTO TOMAS DE AQUINO	**109**	**130**	**143**	**134**	**142**	**147**	**225**	**212**	**210**	**171**	**171**	**135**	**1929**
INSTITUTO TECNICO SANTO TOMAS DE AQUINO SEDE BACHILLERATO							225	212	210	171	171	135	1124
INSTITUTO TECNICO SANTO TOMAS DE AQUINO SEDE PRIMARIA	109	130	143	134	142	147							805
Total general	**975**	**1230**	**1269**	**1347**	**1329**	**1419**	**1862**	**1706**	**1527**	**1426**	**1412**	**1128**	**16630**

Tabla 5. Cuadro Consolidado Matricula Establecimientos Educativos
Fuente: SIMAT Secretaria de Educación Duitama

8.6 Código de Ética y Buen Gobierno.

Disposiciones voluntarias de autorregulación de quienes ejercen el gobierno de las entidades, que a manera de compromiso ético buscan garantizar una gestión eficiente, íntegra y transparente en la administración pública[1].

8.7 Clientes del MEN.

Son los estudiantes y la comunidad educativa, a quienes les llega directamente y a través de las Entidades Territoriales (secretarías de educación departamentales, distritos, municipios certificados y no certificados a través de secretarías departamentales) y las instituciones de educación superior.

8.8 Compromiso de confidencialidad.

Artículo 27. La Ministra de Educación Nacional, su equipo directivo y demás servidores del Ministerio, se comprometen a controlar y verificar de manera permanente que los servidores públicos que manejan infor- | 23 Ministerio de Educación Nacional Código de Ética y Buen Gobierno nación privilegiada o reservada del Ministerio, mantengan la confidencialidad sobre la misma ***y no la den a conocer a terceros o la utilicen en beneficio propio, de particulares, o en perjuicio de la entidad, así mismo se comprometen a establecer mecanismos de control y evaluación del riesgo por pérdida de información.*** En los contratos del Ministerio de Educación Nacional se estipulará una cláusula de confidencialidad en la que el contratista se obligue a guardar estricta reserva sobre toda información confidencial, conocida en virtud del desarrollo y ejecución del contrato. Esta obligación deberá estar vigente mientras conserve el carácter de confidencialidad.

8.8.1 Compromiso con la circulación y divulgación de la información.

Artículo 28. La Ministra de Educación Nacional, su equipo directivo y demás servidores del Ministerio, aplicarán mecanismos para que la información de la entidad llegue a la comunidad educativa, a los demás grupos de interés y a la sociedad en general de manera oportuna, actualizada, clara, veraz y confiable, bajo políticas efectivas de producción, manejo y circulación de la información, para

[1] Código de Ética y Buen Gobierno, Ministerio de Educación Nacional de Colombia ha elaborado el presente documento y sus anexos; http://www.mineducacion.gov.co/1621/articles-265914_archivo_pdf_codigo_etica.pdf

lo cual se adoptarán procesos de información y se utilizarán los medios de comunicación y gestión participativa virtuales y presenciales a los cuales haya lugar, de acuerdo con las condiciones de la comunidad a la que va dirigida.

8.8.2 Compromiso con el Gobierno en Línea.

Artículo 29. La Ministra de Educación Nacional, su equipo directivo y demás servidores del Ministerio, se comprometen a aplicar efectivamente la estrategia de Gobierno en Línea a través de la conformación de un comité que convoque a las diferentes dependencias de la entidad para la implementación de las acciones necesarias que contribuyan con la construcción de un Estado más transparente y participativo y que preste mejores servicios mediante el aprovechamiento de las **TIC,** en el marco del cumplimiento de la misión y las responsabilidades del Ministerio.

8.9 Fuga de Información

Hoy en día las empresas están obligas a enfrentar desafíos en la protección de su información confidencial. Con el objeto de comprender esta situación, Cisco encargó a InsightExpress, una compañía independiente de investigación de mercado, que realizara un estudio que abarcara a empleados y profesionales de TI en diversos países. Como parte del estudio, se realizaron encuestas en 10 países que Cisco seleccionó debido a las diferencias en sus culturas sociales y comerciales. En cada país, se encuestó a 100 usuarios finales y 100 profesionales de TI, cubriendo así a un total de 2000 personas.

La investigación descubrió que a pesar de las políticas, procedimientos y herramientas de seguridad actualmente en uso, los empleados de todo el mundo exhiben conductas arriesgadas que ponen en peligro los datos personales y empresariales[1].

Tales conductas incluyeron:

- Uso de aplicaciones no autorizadas: el 70% de los profesionales de TI cree que el uso de programas no autorizados fue responsable de hasta la mitad de los incidentes de pérdida de información en sus empresas.
- Uso indebido de computadoras de la empresa: el 44% de los empleados comparte dispositivos de trabajo con otras personas sin supervisión.

[1] Cisco Systems Inc. Informe Técnico Riesgos y errores comunes de los empleados. En Linea <http://www.cisco.com/web/offer/em/pdfs_innovators/LATAM/data_mist_sp.pdf?sid=177824_10>Citado en 2008.

● Acceso no autorizado tanto físico como a través de la red: el 39% de los profesionales de TI afirmó que ha debido abordar el acceso no autorizado por parte de un empleado a zonas de la red o de las instalaciones de la empresa.
● Seguridad de trabajadores remotos: el 46% de los empleados admitió haber transferido archivos (correos) entre computadoras del trabajo y personales al trabajar desde el hogar.
● Uso indebido de contraseñas: el 18% de los empleados comparte contraseñas con sus colegas. El porcentaje aumenta al 25% en China, India e Italia.

Para reducir la fuga de datos, las empresas deben integrar la seguridad en su cultura empresarial y evaluar constantemente los riesgos de cada interacción con redes, dispositivos, aplicaciones, datos y, por supuesto, otros usuarios.

8.9.1 ¿Por qué los empleados ponen la información en riesgo?

Generar estadísticas que muestren cuántos empleados exhiben conductas que merman la seguridad de la información es un ejercicio valioso, pero lo realmente importante es comprender cómo cambiar dichas conductas y aumentar la seguridad. Para ello, las empresas deben comprender qué piensan los empleados sobre la seguridad y por qué ignoran o vulneran los procedimientos empresariales.

En algunos casos, el problema no es que el empleado ignore la amenaza, sino que el empleado en sí constituye la amenaza. Si un empleado se siente infeliz en su trabajo, descontento con su jefe, o vengativo por alguna razón, puede convertirse en una “amenaza interna” capaz de dañar o causar una fuga de información en forma deliberada.
A pesar de los esfuerzos del departamento de TI, es posible que algunos empleados no comprendan los procedimientos de seguridad establecidos en sus entornos laborales. Lo más evidente, es que una gran mayoría de empleados desconocen la importancia del buen manejo de los correos institucionales y personales dentro del entorno laboral. Por todo esto se hace necesario educar y capacitar a los funcionarios de la secretaria de educación buscando diferentes métodos que permitan evitar la vulnerabilidad de la información.

8.10 Capacitaciones.

Crear conciencia sobre los temas de seguridad es fundamental para lograr el apoyo de los empleados. Cuando un empleado cree que los programas de seguridad son importantes, es más probable que acate los procedimientos pertinentes. Un plan de educación debe:

● Instruir y capacitar a los empleados con respecto a las expectativas que tiene la empresa en relación con la protección de datos.

● Incluir capacitación y prácticas de seguridad en la orientación de nuevos empleados.
● Capacitar a los empleados sobre las medidas de seguridad que deben considerar al responder el teléfono y al conectarse a sitios Web, redes sociales y el buen manejo del correo electrónico.
● Capacitar a los empleados sobre temas de seguridad física, como permitir que sólo empleados con credenciales de seguridad accedan a los edificios.

Enséñele a sus empleados que la información empresarial es esencialmente dinero: perder o favorecer la fuga de datos empresariales es lo mismo que tirar dinero a la basura y dejar que la competencia o personas delincuentes como traficantes de menores de edad puedan acceder de alguna forma a la información confidencial de la empresa buscando lucrarse con el fin de usarlos en diferentes actos ilícitos

"Una forma de instruir a los usuarios es concientizarlos en cuál sería el impacto negativo que podría tener un ataque informático. Ejemplificándolo, diciéndole al usuario: "debes elegir una contraseña que sea difícil".

Ahora, si la advertencia o el consejo vienen por el lado de decir, "bueno, estas usando tu correo para un montón de actividades que son importantes, entonces, toma conciencia que hay un montón de gente que puede estar intentando vulnerar la privacidad de tu correo electrónico".

De esta forma, podríamos ser más específicos y decir: "una de las maneras mediante la cual se intenta vulnerar una contraseña de correo electrónico, es probar palabras o combinaciones de palabras y números que puedan tener cierta relación con lo que es tu persona, fecha de nacimiento, numero de documento o lo que fuera". Entonces, hay que concientizar al usuario y decirle que puede haber gente que va a estar probando esas cosas y que tome conciencia y no elija ese tipo de contraseñas, porque de esa forma estará facilitando la tarea de un atacante para acceder a su cuenta.

De la misma manera sucede con lo que es el acceso a internet. Es decir, explicarles a los usuarios que la misma computadora que utilizan para ingresar al Home Banking –desde la cual manejan dinero-, no la utilicen para descargar cualquier programa que encuentren dando vuelta por internet. Hay que tener en cuenta que el software descargado puedo haber sido vulnerado y de esta forma le facilitamos el acceso a nuestra PC a cualquier atacante y perder dinero.

8.10.1 Folletos con consejos o tips para usuarios

Crear folletos y socializarlos con los empleados de la secretaria de educación que contengan de forma clara y precisa los principales problemas de vulnerabilidad de

información así como tips que les permitan controlar riesgos de pérdida de información.

Los empleados deben comprender y poner en práctica los siguientes procedimientos básicos de seguridad:

● Para proteger los sistemas utilice sólo aplicaciones y métodos de acceso autorizados, mantenga actualizado el software de seguridad además de las aplicaciones antivirus, respete y conserve las configuraciones de seguridad, comprenda las consecuencias de aceptar o rechazar las acciones emergentes de Security Agent, y prepárese para los distintos métodos de ataque como el correo no deseado, software malicioso y phishing.

● Para proteger los dispositivos portátiles, manténgalos con usted o bloqueados en todo momento, no comparta sus dispositivos laborales ni los utilice para actividades personales, no envíe información confidencial desde sistemas laborales a dispositivos personales, y no acceda a sitios inapropiados ni descargue información indebida.

● Para evitar el acceso no autorizado a información, cierre sesiones o bloquee los sistemas cuando se aleje momentáneamente de su computadora o se vaya a casa al final de la jornada, utilice buenas técnicas de creación de contraseñas, no comparta sus contraseñas con nadie y almacénelas en forma segura.

● Para evitar el robo de información cuando esté de viaje, baje la voz cuando tenga que hablar sobre información confidencial en público, use filtros de privacidad para evitar que alguien vea sobre su hombro, use una red VPN y nunca use una impresora compartida a menos que usted esté presente para recoger enseguida lo que imprimió

Los empleados deben comprender que son fundamentales para conservar la seguridad de la empresa y aceptar la responsabilidad de protegerla. Sacrificar el nivel de calidad y seguridad en pos de la conveniencia es un error que las empresas no pueden permitirse cometer. Todos los empleados deben:

● Regirse por el código de buena conducta comercial de la empresa al llevar a cabo sus actividades laborales cotidianas, especialmente aquéllas relacionadas con la seguridad de la información.
● Estar constantemente atentos al entorno y pensar en la seguridad en cada acción que realicen en la oficina, el hogar y cuando estén de viaje.
● Aprender cómo manejar los diferentes niveles de confidencialidad para los documentos de su empresa. Esto incluye comprender las diferencias entre información “pública”, “confidencial”, “sumamente confidencial” y “restringida”.

8.11 La ingeniería social como práctica para vulnerar humanos

"La ingeniería social se denomina al proceso mediante el cual logras un objetivo vulnerando la condición humana. Es decir, puedo tener varios mecanismos técnicos para obtener tu clave cuando accedes a tu correo electrónico. Supongamos que desde mi maquina ingreso a la tuya para obtener tus claves. Eso sería acceso a la información de manera técnica.

Otro método que puedo aplicar seria falsificar un mensaje de correo electrónico y enviártelo presumiendo que soy soporte técnico de quien te brinda servicio de correo electrónico a vos, diciéndote que tuvimos graves problema en la base de datos y es necesario que nos reportes tu usuario y contraseña. Entonces eso sería el uso de ingeniería social, donde mediante algo técnico se intenta explotar vulnerabilidades de características humanas"[1].

[1] Cryptex. Informe. La responsabilidad legal de las empresas frente a un ciberataque [ENATIC].En Linea. < http://seguridad-informacion.blogspot.com/2008/11/porqu-concientizar-los-usuarios-en-la.html; Visto en http://cyt.aimdigital.com.ar/ver_suple.php?id=3558> Citado en 4 de Agosto de 2015.

9. MARCO TEORICO

En esta sección podremos encontrar diferentes descripciones que nos permitirá entender de todo lo relacionado el proyecto de seguridad en el transporte y gestión de correos electrónicos implementación de seguridad en correo outlook 2010.

9.1. La seguridad en el transporte del correo

9.1.1 Estado actual de SASL en los servidores y clientes estudiados

Los clientes estudiados incorporan autenticación SASL de nivel básico, equivalentes a username y password clásicos, además Eudora incorpora APOP y CRAM-MD5. En algunos clientes el usuario debe configurar su aplicación para activar autenticación SASL y en otros casos el cliente responde automáticamente cuando el servidor ofrece la posibilidad.

Los servidores estudiados incluyen todas las opciones de autenticación SASL. En la compilación hay que indicar que se utilizará SASL y puede ser necesario tener las librerías cyrus-sasl instaladas[4].

9.1.2 Mejoras de seguridad de los protocolos vía TLS5 (antes SSL)

TLS es un protocolo mediante el cual es posible crear un canal cifrado entre el cliente y el servidor. Así el intercambio de información (identificación de usuario y contenido de los mensajes) se realiza en un entorno seguro y libre de ataques pasivos. Es un protocolo criptográfico mixto (basado en cifrado simétrico y asimétrico), que utiliza certificados x509 y que es el utilizado por los servidores http seguros.

Existen dos formas de negociación: la directa cuando es previa a cualquier intercambio de información y la que se produce a partir de una petición dentro del dialogo del protocolo. La directa es la que se establece entre clientes y servidores http seguros, mientras que los RFC 2487 y 2595 integran la negociación en el dialogo del protocolo POP, IMAP o SMTP a partir de una petición tipo STARTTLS.

---

[4] Sánchez E, Técnicas para fortalecer la seguridad en tu correo electrónico. En Linea< http://www.pcactual.com/articulo/zona_practica/paso_a_paso/paso_a_paso_software/11692/tecnicas_para_fortalecer_seguridad_correo_electronico.html#sthash.EqcQHrhT.dpuf.> Citado en 2015.

[5] RFC2595 (1999) TlS para POP, IMAP, ACAP y RFC 2487 (1999) TLS para SMTP.

9.1.3 La seguridad en el transporte del correo TLS

TLS es un protocolo mediante el cual es posible crear un canal cifrado entre el cliente y el servidor. Así el intercambio de información (identificación de usuario y contenido de los mensajes) se realiza en un entorno seguro y libre de ataques pasivos[6]. Es un protocolo criptográfico mixto (basado en cifrado simétrico y asimétrico), que utiliza certificados x509 y que es el utilizado por los servidores http seguros.

9.1.4 Mecanismos de autenticación.

Dentro de los mecanismos de autenticación disponibles, los más comunes son: PLAIN, LOGIN, CRAM-MD5[4], DIGEST-MD5, y NTLM (NT LAN Manager). De éstos, PLAIN, CRAM-MD5, y DIGEST-MD5 son mecanismos de autenticación estandarizados, mientras que LOGIN y NTLM son mecanismos propietarios de Microsoft. Sólo PLAIN y LOGIN puede utilizar la contraseña de usuarios en sistemas Unix o Linux. Como se puede observar en la documentación existente para SASL 0.1[5]: el uso de los diferentes mecanismos de autenticación, depende de los requerimientos de la aplicación que los esté usando. Mecanismos simples como LOGIN y PLAIN, están dirigidos a anclarse en mecanismos de autenticación existentes tales como /etc/passwd a través de PAM (Pluggable Authentication Module, Módulo de Autenticación Conectable). La respuesta del cliente a estos mecanismos es sencilla de implementar: al usuario sólo se le pide su nombre de usuario y su contraseña, y luego las llamadas al servidor pasan el nombre de usuario y la contraseña a las políticas de decisión definidas por el sistema de autenticación.

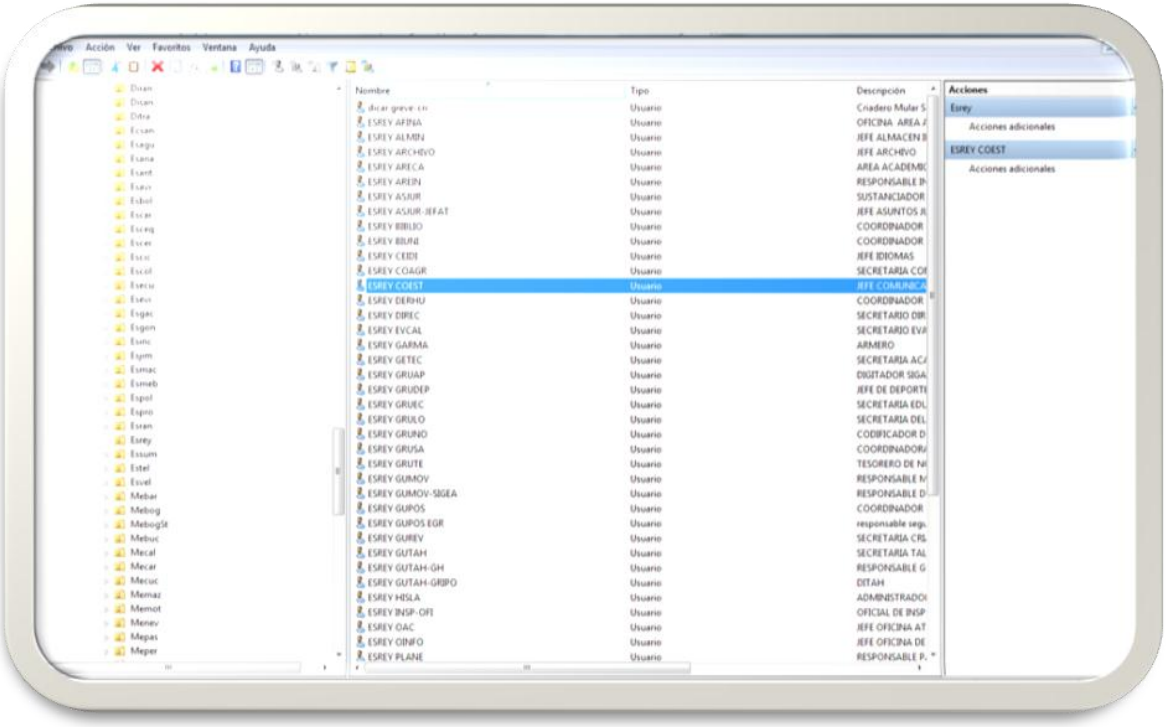
Se configura el servidor para la caducidad de contraseñas, en la que cada 30 días genere el usuario una alerta de cambio de credenciales bajo un parámetro de mínimo 10 caracteres alfanuméricos, un solo administrador de cuentas de correos donde no permite al usuario gestionar el desbloqueo de usuarios y todos lo realzaran en caso de bloqueo de las mismas a través de una solicitud de una mesa de ayuda.

[6]Borja O., Pérez P. La seguridad en el transporte del correo. En Línea. <http://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0CE4QFjAE&url=http%3A%2F%2Fwww.rediris.es%2Fmail%2Fgti%2Fgti-smail%2Fdoc%2Fseguridad-smail.doc&ei=G9WgU_WUAsrOsAT5kIGQAw&usg=AFQjCNHRFqIbfYGpCjCuqHVzP2HONLhEHQ&sig2=41bR9ZDs6q4aHG2YYojF3g&bvm=bv.69137298,bs.1,d.bGQ> Citado en el 2000.

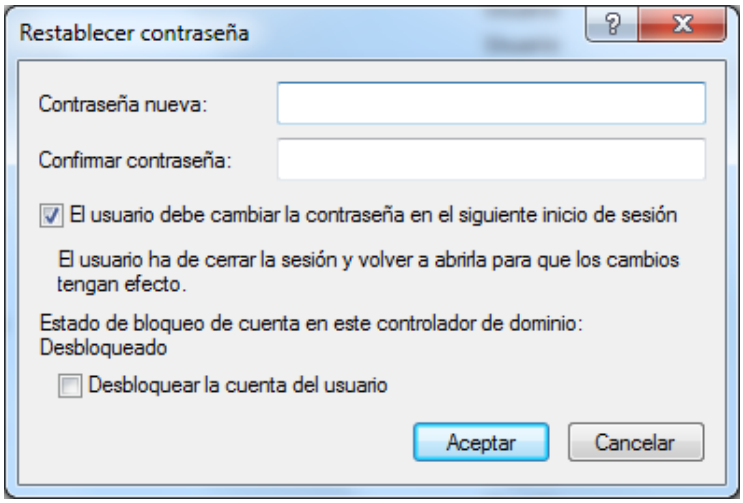
El servidor de correos quedara configurado con política de bloqueo al intento de ingreso con tres veces con claves erróneas.

- Configuración servidor para caducidad de contraseñas y políticas de bloqueo al ingreso:

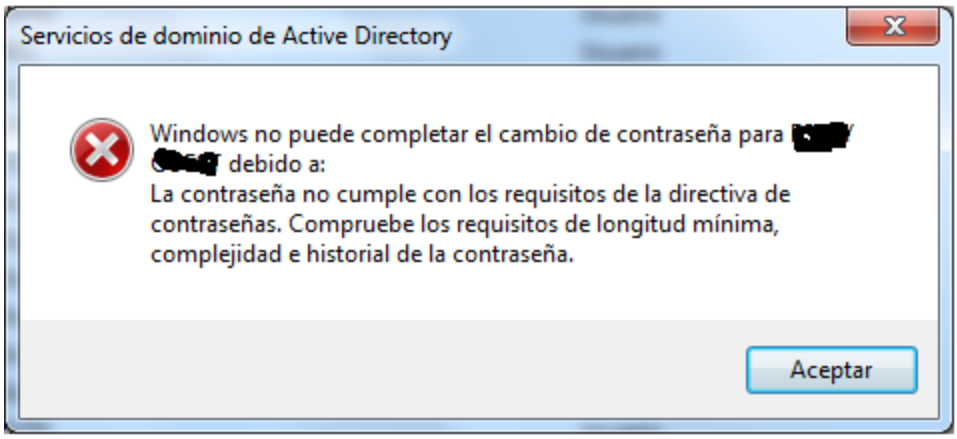
Paso 1: Ubicación del usuario en el directorio de direcciones.

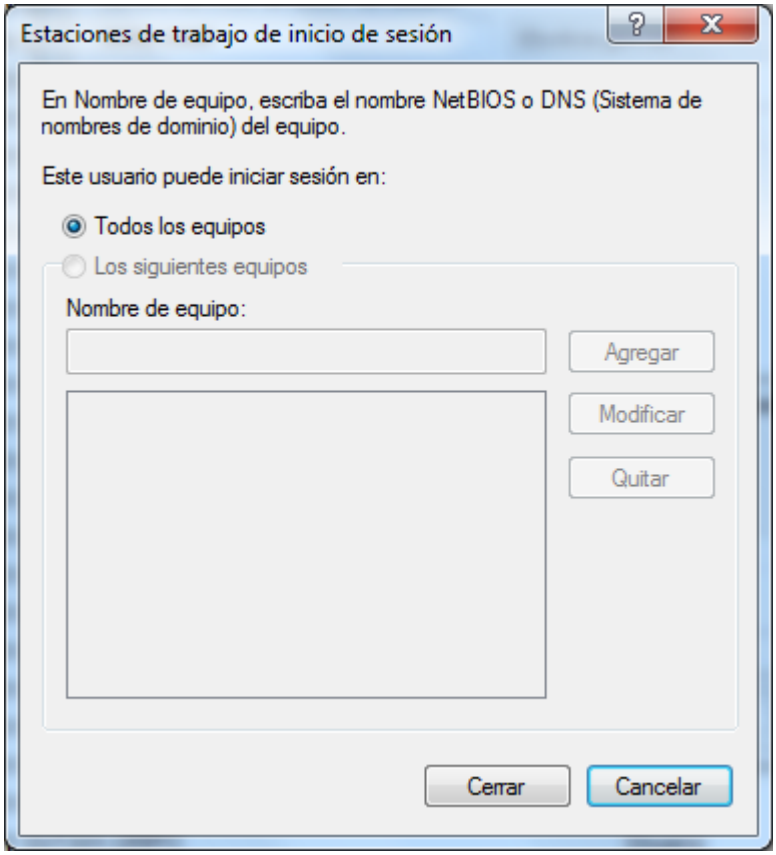


Paso 2: Configuración para que el usuario cambie la credencial de ingreso cada 30 días. Aviso de Alerta.



Paso 3: Configuración del servidor para que el usuario cambie por una contraseña fuerte que cumpla con los requisitos.





9.1.5 ¿Cómo Puede Medirse la Seguridad?

Por David A. Chapin -CISA, CISM, CISSP, IAM- y Steven Akridge -JD, CSM, CM, CISSP, IAMas métricas de seguridad tradicionales son, en el mejor de los casos, fortuitas; en el peor, dan una falsa sensación de seguridad, que lleva a una implantación ineficiente o insegura de medidas de seguridad. Este artículo presenta un enfoque donde se combinan madurez y calidad para proporcionar una imagen más completa y ordenada del estado de seguridad de una organización. Nos referiremos a este enfoque como Modelo de Madurez del Programa de Seguridad. Las métricas de seguridad -la medida de la eficacia de los esfuerzos en seguridad de una organización a lo largo del tiempo- han sido siempre difíciles de evaluar. ¿Cómo puede determinar una organización si se encuentra segura? La medida de la calidad del programa de seguridad sólo puede probarse realmente cuando la organización se ve agobiada por una crisis. Pero para evitar esa situación es precisamente para lo que se realiza el esfuerzo en seguridad. La gerencia necesita alguna medida de cómo de segura está la organización. Las organizaciones necesitan preguntarse:

• ¿Cuántos recursos son necesarios para estar "seguro"?
• ¿Cómo puede justificarse el coste de nuevas medidas de seguridad?
• ¿Recibe la organización algo a cambio de su inversión?
• ¿Cuándo sabe la organización que está "segura"?
• ¿Cómo puede comparar la organización su estado con otras del sector y con los estándares de buenas prácticas?

La respuesta tradicional a estas preguntas se relaciona con la evaluación del riesgo y el riesgo residual que la organización está dispuesta a asumir en función de sus necesidades de negocio y limitaciones de presupuesto. La gestión del riesgo puede darse por sentada, no conduciendo necesariamente a un estado de mayor seguridad. Imagine, por ejemplo, un análisis de riesgos que contiene una matriz de amenazas y el coste de mitigar los riesgos. Algunos de los elementos de la lista tendrían un coste insignificante. Otros elementos serían muy caros. Con frecuencia, la gerencia puede decidir mitigar el mayor número de elementos por la menor cantidad de dinero, posiblemente dejando de lado los elementos más caros. La suposición es que añadir controles de reducción del riesgo es la mejor opción. Por ello, hay una tendencia a comprar grandes cantidades de herramientas de seguridad y evitar los controles más caros y menos glamurosos. Los controles más complicados tienden a ser de naturaleza organizativa, requiriendo cambios culturales (tales como un plan de recuperación de desastres), más que soluciones llave en mano (tales como cortafuegos y sistemas de detección de intrusos -IDSs-). La dirección piensa que está comprando más seguridad por menos dinero. Sin embargo, ¿quién dice que se compre más seguridad? ¿Cómo puede medir la organización la protección relativa obtenida con cada adquisición? ¿Está comprando la organización las salvaguardas de seguridad en el orden correcto? ¿Está exponiéndose la organización a más riesgo debido al enfoque no sistemático de la implantación? Crear programas de

seguridad desde cero permite abordar estos problemas tradicionales de métricas de seguridad de otra forma. Una mirada renovada a dichos problemas facilita el desarrollo de una solución exhaustiva para cualquier sector. Este enfoque nuevo, más sistemático, de las métricas de seguridad permitirá:

- Generar mediciones reproducibles y justificables.
- Medir algo que tenga valor para la organización.
- Determinar el progreso real en el estado de la seguridad.
- Ser aplicable a un amplio espectro de organizaciones, al tiempo que produce resultados similares.
- Determinar el orden en que deberían aplicarse los controles de seguridad.
- Determinar los recursos que necesitan ser destinados al programa de seguridad.

Métricas de seguridad tradicionales.

9.1.6 Las Tecnologías de Información y comunicación, el correo electrónico

La implantación de tecnología de información en las Organizaciones y las consecuencias estratégicas de la misma se ha estudiado bajo diversas perspectivas. Porter (1985), Sethi y King (1994), Toraskar y Joglekar (1993) hacen referencias a casos concretos de obtención de ventajas por un uso apropiado de las tecnologías de información en los procesos de comunicación. Para McKeen y Smith (1993), el uso de la tecnología de información puede tener repercusiones no sólo en las relaciones entre organizaciones sino también en las relaciones internas de las mismas. Brown (1995) menciona las inversiones en sistemas de información estratégicos como una forma a través de la que las organizaciones buscan ventajas competitivas.

Dos Santos (1993) mantiene que el impacto de las inversiones en tecnología de información en la organización no pueden comprenderse de forma completa atendiendo únicamente al desempeño medido en altos niveles de creación de valor, puesto que no lleva a distinguir las aplicaciones y usos de la misma. Para entender el impacto de una determinada tecnología dentro de las organizaciones, parece apropiado examinar cómo se usa en los procesos en los que se está aplicando. Resulta útil identificar diferencias en cómo se percibe la tecnología de información por los usuarios en una organización como medio de buscar competitividad y cómo esta percepción se lleva a cabo en la realidad.

Las tecnologías de información están afectando a la forma de intercambio información entre diferentes miembros de las organizaciones. Permiten, en muchos casos, sustituir el contacto físico. Numerosos autores han examinado de forma empírica el papel de los medios electrónicos en la comunicación (Eveland y Bikson, 1988; Finfholt y Sproull, 1990; Markus,

1994; Rice y Asociados, 1984; Fulk, 1993; Sproull y Kiesler, 1991; Trevino, Lengel y Daft, 1987).

Yates y Orlikowski (1992; 1994) hablan de géneros de comunicación organizativa, como por ejemplo una memo, una reunión de comité o un resumen, en cuanto acciones tipificadas comunes y reconocidas de forma social como una manera con un propósito y características comunes determinadas. El propósito de comunicación de un género no es un motivo individual privado para comunicar sino un propósito construido y reconocido por la comunidad y usado para ciertas situaciones. Por ejemplo el propósito socialmente reconocido de una reunión de un comité es discutir, tomar decisiones, delegar o implantar acciones relativas a sus competencias.

Ricoma (1996) habla de dos tipos de tecnologías disponibles para la comunicación en las Organizaciones: tecnologías de pantalla o tecnologías de voz y datos, donde podríamos incluir el fax, el correo electrónico y las tecnologías de voice and mail.

En los últimos quince años, el uso de ordenadores personales ha popularizado un número considerable de servicios de información, incluyendo el correo electrónico. El e-mail es una forma de intercambio de información en la que se mandan mensajes de un ordenador personal o terminal a otro vía módem y sistemas de telecomunicaciones.

El uso del correo comenzó con ARPAnet (red precursora de Internet) en 1969 y 1970 en los Estados Unidos, se extendió de forma gradual con el uso de los mainframes y miniordenadores basados en redes locales en los setenta y tuvo un rápido crecimiento con el uso de Internet en la década de los ochenta. El correo electrónico en sus inicios se plantea como un medio de intercambio de información para grupos pequeños y selectos. Actualmente su uso se ha extendido a millones de usuarios por todo el mundo. El correo electrónico es el servicio más utilizado de los que existen hoy en Internet. Desde el año 1970 se ha empleado como herramienta de comunicación para relaciones académicas y personales. Por el año 1990, la popularidad y ubicuidad del correo sobre el resto de los medios de comunicación tradicionales ha permitido que se reconozca como medio estándar de comunicación.

El correo electrónico permite el envío de mensajes por medios informáticos. Los mensajes se almacenan en un buzón personal. Cuando cada usuario consulta su correspondencia puede visualizar, almacenar o reenviar mensajes recibidos. Los mensajes enviados pueden estar en cualquier tipo

de formato, texto, gráficos, imágenes, sonido, etc.

El e-mail es un medio electrónico que permite la instantaneidad de comunicación entre receptor y emisor. Sáenz Vacas hace referencia al correo electrónico bajo las siglas EAUDI tratando destacar las características típicas que hacen a este medio idóneo para ciertos tipos de comunicación en las organizaciones (electrónico, asíncrono, ubicuo, digital e informático).

- Electrónico: utiliza medios electrónicos de gestión y transporte
- Asíncrono: no necesita sincronía en envío y recepción
- Ubicuo: permite su acceso en diferentes lugares
- Digital: utiliza información digitalizada
- Informático: está en relación con las tecnologías de la información

9.1.7 Protocolos para el intercambio de correo electrónico.

En el primer grupo, los dos protocolos más populares son IMAP (Internet Message Access Protocol, Protocolo de Acceso a Mensajes de Internet) y POP (Post Office Protocol, Protocolo de Oficina de Correo). La principal diferencia reside en que el protocolo IMAP permite el acceso a los mensajes alojados en el servidor y POP la descarga en la máquina local, borrándolos o dejando una copia en el servidor, según se indique[7].

POP fue diseñado inicialmente para leer correos sin conexión. El usuario se conectaba y descargaba los correos a su máquina local después de lo cual éstos eran borrados del servidor. IMAP en cambio, fue pensado para permitir el acceso y la gestión de los mensajes desde más de un computador. Además soportaba modos de acceso “en línea”, “sin conexión” y “desconectado”.

[7] Modelo de Conectividad para Redes Humanas. Implementación De Un Servicio De Correo Electrónico Seguro. <http://www.iered.org/joiner/docfinal/2-e_correo-seguro/ implementación de un servicio de correo electrónico seguro> Citado en 2004.

9.2 Vulnerabilidad.

9.2.1 Vulnerabilidad Certificado - CVE-203-3870

❖ **Descripción.**

Certificado - CVE-203-3870 Existe una vulnerabilidad de ejecución remota de código en la forma en que Microsoft Outlook analiza mensajes electrónicos especialmente diseñados en S/MIME. Un atacante que explote por completo esta vulnerabilidad puede tomar el control por completo del sistema afectado. Un atacante podría instalar programas; ver, cambiar o borrar datos; o crear nuevas cuentas con todos los privilegios de usuario.

❖ **Impacto.**

Mensaje de vulnerabilidad certificado - CVE-203-3870. Un atacante que explote por completo esta vulnerabilidad podría ejecutar código arbitrario como el usuario conectado. Si un usuario está conectado con privilegios de administrador, el atacante podría tomar el control por completo del sistema afectado. Un atacante podría instalar programas; ver, cambiar o borrar datos; o crear nuevas cuentas con todos los privilegios de usuario. Usuarios cuyas cuentas estén configuradas para tener pocos privilegios sobre el sistema podrían ser menos impactados que usuarios que cuenten con privilegios de administrador[8].

9.3 Investigaciones cuantitativas

9.3.1 Investigación evaluativa

- Verificación de seguridad mínima en servidores Outlook 2010 en servicios particulares, mediante herramientas de scaneo (Nessus: Es la herramienta de evaluación de seguridad "Open Source" de mayor renombre. Nessus es un escáner de seguridad remoto para Linux, BSD, Solaris y Otros Unix. Está basado en plug-in(s), tiene una interfaz basada en GTK, y realiza más de 1200 pruebas de seguridad remotas. Permite generar reportes en HTML,

[8] Coordinación de Seguridad de la Información. Vulnerabilidad en Microsoft Outlook podría permitir la ejecución remota de código. En línea < http://www.seguridad.unam.mx/vulnerabilidadesDB/?vulne=6457>. Citado en 10 de Septiembre 2013.

XML, LaTeX, y texto ASCII; también sugiere soluciones para los problemas de seguridad).

- El procedimiento que realizaremos es la evaluación del servidor Secretaria de Educación Municipal Duitama que se ejecuta como gestor de correos verificando los protocolos de seguridad que tienen configurados para minimizar los riesgos.
- Investigación de los protocolos de seguridad actuales en el mercado configurables en correos Outlook 2010.
- Configuración de correo Outlook 2010 de acuerdo a los protocolos de seguridad establecidos una vez verificadas las vulnerabilidades en el gestor de correos de la Secretaria de Educación Municipal.

9.3.2 Diseño metodológico

1. Debido a los continuos fallos en la seguridad de los correos presentados en los gestores como Outlook 2010 por motivos a la mala configuración de los servidores destinados para la prestación y administración de este servicio reflejados en la implementación y utilización de los protocolos de seguridad existentes.

2. Verificación de la existencia de estudios similares en Seguridad en el transporte y gestión de correos electrónicos Implementación de seguridad en correo Outlook 2010 donde identifico que existen estudios anteriores a servidores de correos para minimizar los riesgos en el transporte de información.

3. Una vez verificado los estudios previos observamos que se hace necesario documentar un procedimiento para la configuración de servidores destinado para la administración de correos electrónicos debido a la gran demanda que tiene este medio de comunicación donde está en muchas ocasiones en juego la continuidad del negocio por los riesgos que representa las vulnerabilidades en el transporte de la información o como es nuestro caso la vulnerabilidad de la información personal de los niños, niñas y adolescentes que ponen en riesgo la seguridad personal de cada uno de ellos.

4. Formulación del problema definidos los riegos que representa el transporte de la información sin seguridad la cual se debe parametrizar en el servidor de correos adoptando los esquemas y herramientas disponibles que aran que la información viaje más segura garantizando la integridad, confidencialidad y disponibilidad.

5. Se establece las área a afectar y la población que será beneficiada por la configuración dentro de un protocolo establecido, para la Secretaria de Educación del Municipio de Duitama brindándole seguridad en su comunicación a través de los correos Outlook 2010.

10. MARCO LEGAL

En esta sección podremos encontrar las leyes o reglamentos donde se fundamenta la investigación.

10.1 Guía/norma de seguridad de las tic (ccn-stic-814) seguridad en correo electrónico

Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC[9].

Adicionalmente a las reglas anteriores, es importante que la organización evalúe la conveniencia de denegar, en el cortafuegos corporativo, todo el tráfico SMTP saliente hacia Internet con excepción del generado en los servidores de correo electrónico; esto evitará, entre otros, propagaciones masivas de malware desde equipos de usuario, uso de equipos internos para realizar ataques de phishing, etc. Como inconveniente, los usuarios que utilicen diferentes servidores de correo –por ejemplo, que gestionen diferentes cuentas desde su equipo-, no podrán hacerlo salvo que, una a una, se permitan estas conexiones SMTP salientes en el cortafuegos de la organización.

10.2 Ley Estatutaria 1266 De 2008

Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

[9] S2 Grupo y Antonio Villalón Huerta han elaborado el presente documento. En Linea <https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/814-Seguridad_en_Correo_Electronico/814_Seguridad-en-correo-electronico.pdf> Citado en 2010.

10.2.1 Artículo 2o. Ámbito de Aplicación.

La presente ley se aplica a todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada.

Esta ley se aplicará sin perjuicio de normas especiales que disponen la confidencialidad o reserva de ciertos datos o información registrada en bancos de datos de naturaleza pública, para fines estadísticos, de investigación o sanción de delitos o para garantizar el orden público.

Se exceptúan de esta ley las bases de datos que tienen por finalidad producir la Inteligencia de Estado por parte del Departamento Administrativo de Seguridad, DAS, y de la Fuerza Pública para garantizar la seguridad nacional interna y externa.

Los registros públicos a cargo de las cámaras de comercio se regirán exclusivamente por las normas y principios consagrados en las normas especiales que las regulan.

Igualmente, quedan excluidos de la aplicación de la presente ley aquellos datos mantenidos en un ámbito exclusivamente personal o doméstico y aquellos que circulan internamente, esto es, que no se suministran a otras personas jurídicas o naturales. [1].

10.3 Ley 1273 De 2009

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

10.3.1 Capitulo. I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo,

[1] Congreso de la Republica. En línea http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html> Citado en 26 de Agosto de 2015.

incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: ***Obstaculización ilegítima de sistema informático o red de telecomunicación****.* El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: ***Interceptación de datos informáticos*****.** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: ***Daño Informático*****.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: ***Uso de software malicioso*****.** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: ***Violación de datos personales*****.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: ***Suplantación de sitios web para capturar datos personales*****.** El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: ***Circunstancias de agravación punitiva***: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

10.4 Decreto 1377 De 2013

Que mediante la Ley 1581 de 2012 se expidió el Régimen General de Protección de Datos Personales, el cual, de conformidad con su artículo 1°, tiene por objeto *"(...) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma".*

Que la Ley 1581 de 2012 constituye el marco general de la protección de los datos personales en Colombia.

Que mediante sentencia C-748 del 6 de octubre de 2011 la Corte Constitucional declaró exequible el Proyecto de ley Estatutaria número 184 de 2010 Senado, 046 de 2010 Cámara.

Que con el fin de facilitar la implementación y cumplimiento de la Ley 1581 de 2012 se deben reglamentar aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales, este último tema referido a la rendición de cuentas.

10.4.1 Capítulo II

Artículo 12. ***Requisitos especiales para el tratamiento de datos personales de niños, niñas y adolescentes***. El Tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7° de la Ley 1581 de 2012 y cuando dicho Tratamiento cumpla con los siguientes parámetros y requisitos:

1. Que responda y respete el interés superior de los niños, niñas y adolescentes.

2. Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos. Para este fin deberán aplicarse los principios y obligaciones establecidos en la Ley 1581 de 2012 y el presente decreto.

La familia y la sociedad deben velar porque los responsables y encargados del tratamiento de los datos personales de los menores de edad cumplan las obligaciones establecidas en la Ley 1581 de 2012 y el presente decreto.

.

10.5 Ley Estatutaria 1581 De 2012

10.5.1 Objeto, ámbito de aplicación y definiciones

Artículo 1°. *Objeto*. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Artículo 7°. *Derechos de los niños, niñas y adolescentes.* En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública.

Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás. El Gobierno Nacional reglamentará la materia, dentro de los seis (6) meses siguientes a la promulgación de esta ley.

11. CONCRECION DEL MODELO

11.1 Metodología utilizada

Para el desarrollo del objetivo general en el que se requiere establecer los mecanismos de implementación en un cliente de correo Outlook 2010 que permita minimizar vulnerabilidad en el transporte, autenticación y gestión de correo electrónico Outlook 2010 de la Secretaria de Educación Municipal Duitama fue necesario abordar unos puntos específicos con acciones que se definirán a continuación:

Identificar las herramientas o mecanismos de seguridad que permitan la protección de la información que contiene cada uno de los correos Outlook de los funcionarios de la secretaria de educación y los 14 establecimientos educativos oficiales, estos mecanismos nos permitirán resguardar la información que se genera del software o sistema SIMAT (Sistema Integrado de Matricula) información que es transportada por varios medios entre estas dependencias, la función principal es indicar la manera en que se deben ejecutar las acciones y así evitar la vulnerabilidad en la misma.

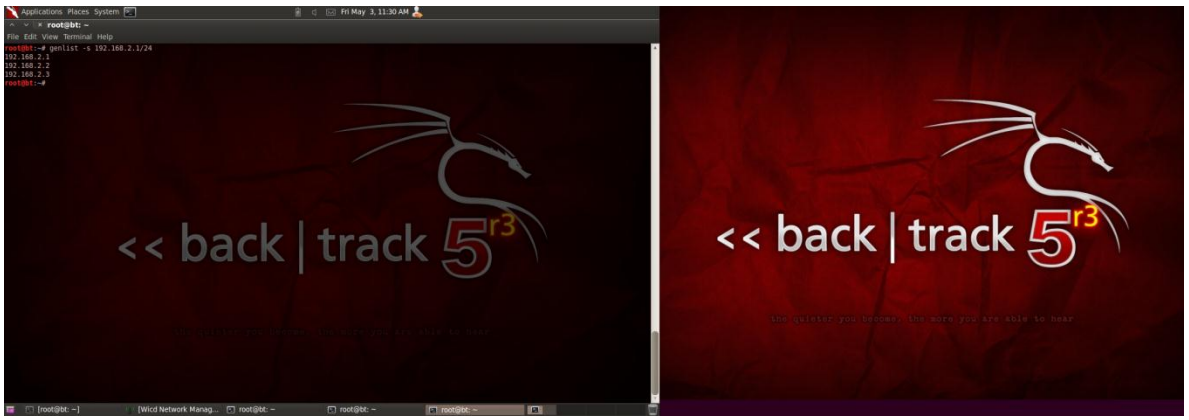
Las herramientas o mecanismos utilizados son:

- ✓ **Mecanismos preventivos.** Se realizó monitoreo de la información que maneja cada uno de los funcionarios, registro de las actividades y los diferentes usuarios que acceden a ella donde se evidencio que el transporte de información se realiza por diferentes medios como son dispositivos extraíbles lo que generan perdida de información y por medio de correo electrónico con vulnerabilidad. Para prevenir la ocurrencia de un ataque informático se realizó el bloqueo de los dispositivos extraíbles en cada uno de los equipos de los funcionarios de la secretaria y se realizó escaneo por medio de la herramienta Nessus para identificar la vulnerabilidad que presenta el correo Outlook 2010.

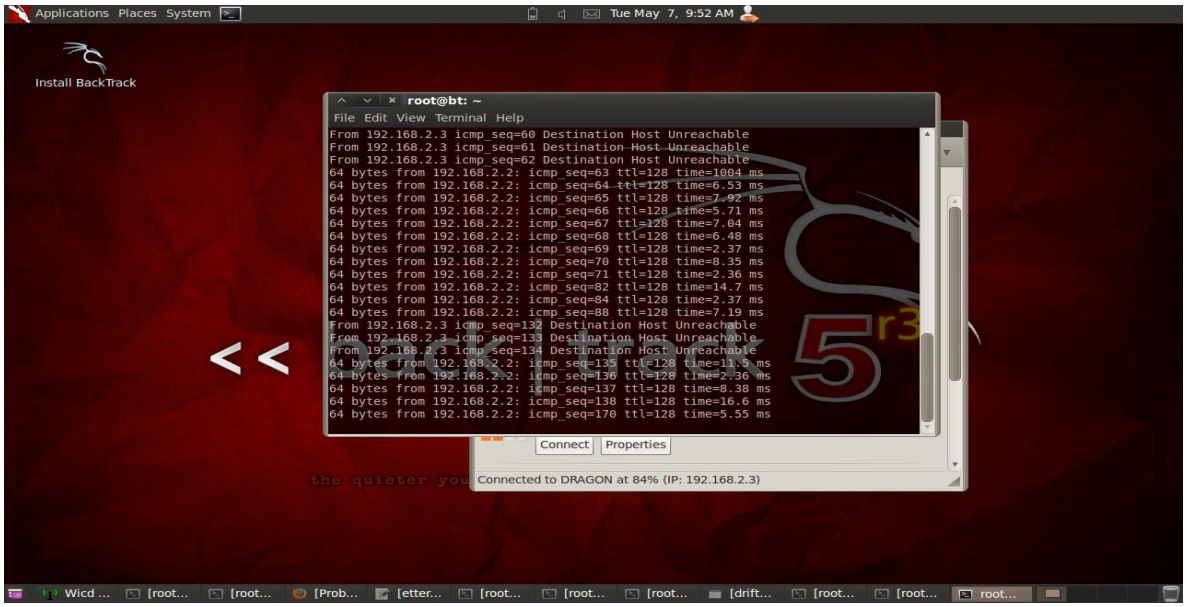
- ✓ **Mecanismos detectores.** Se utilizaron herramientas de monitoreo ettercap, urlsanrf y drifnet las tienen como objetivo detectar todo aquello que pueda ser una amenaza para la información de la Secretaria de Educación.

Como primera instancia verificamos nuestra configuracion de las tarjetas de red y cual es la que vamos a utilizar con ifconfig.

Con el comando genlist –s y la ip que ya verificamos de nuestra conexión de internet escaneamos la red para verificar cuales estan conectados, de igualforma lo podemos hacer con nmap.

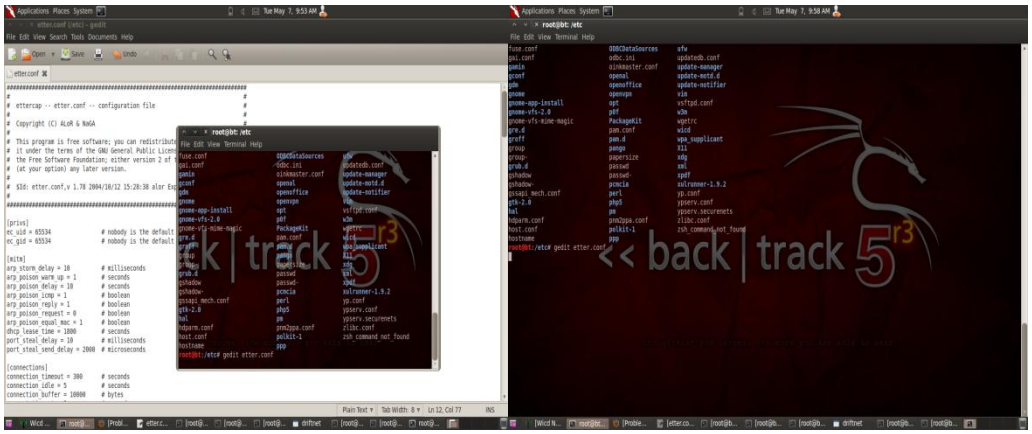


Realizamos ping al host de destino para lo cual ejecutamos desde consola ping ip.



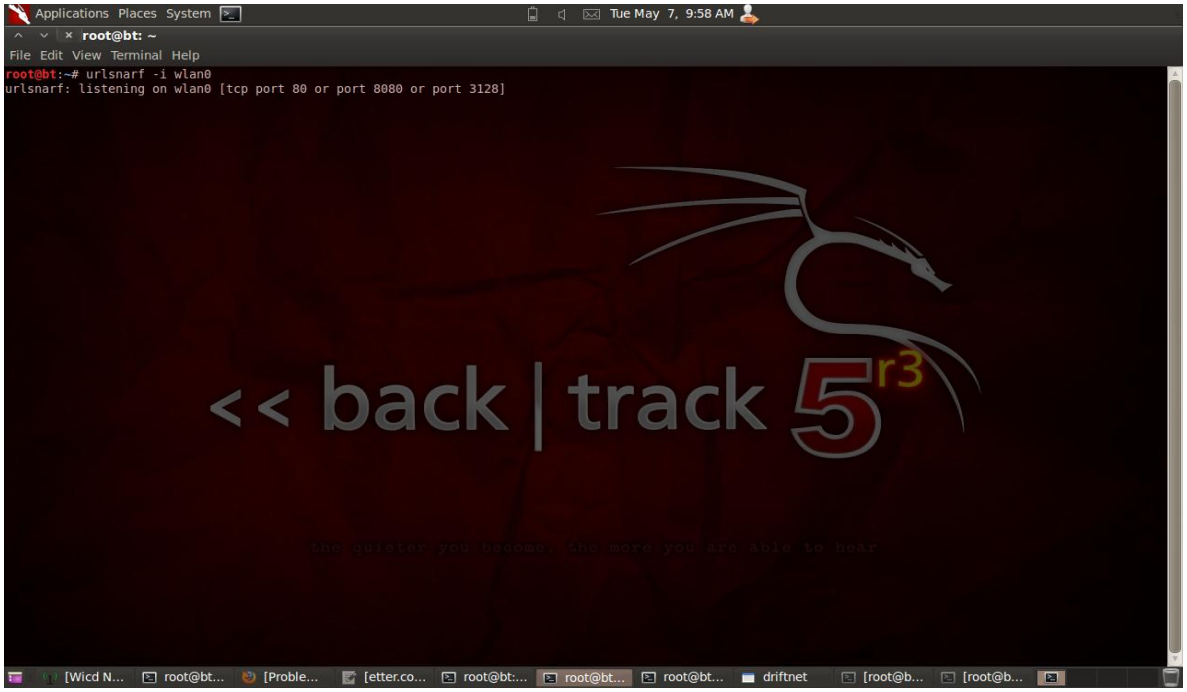
Ahora vamos a utilizar ettercap que es una herramienta que tenemos en las herramientas de backtack para lo cual como primera instancia lo configuramos para que recepciones todo el tráfico de la red y no me dé un error.

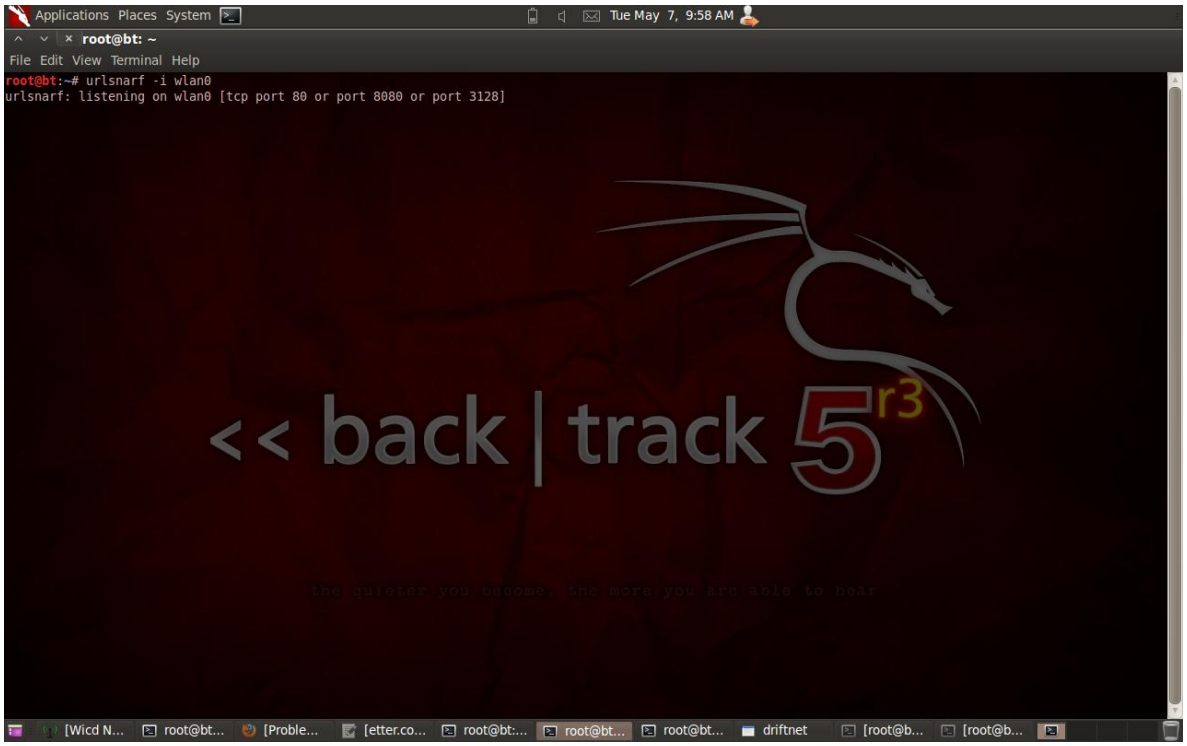
Configuración nos ubicamos en el etter.conf
Cd /etc/etter.conf con gedit para editar y quitamos las almohadillas# en Linux

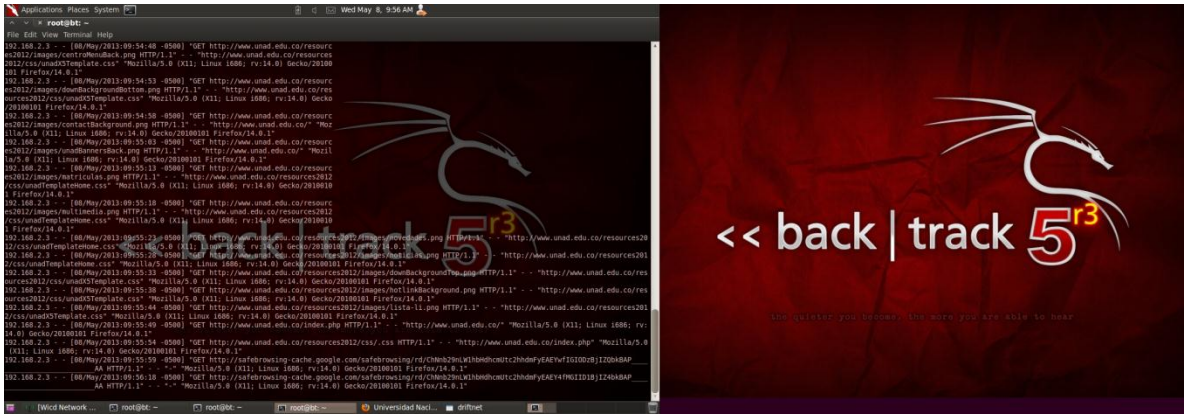


Lanzamos el ataque ettercap -T -Q -i wlan0 // //

Otra herramienta que utilizamos es urlsnarf –i lan0 para que me verifique todas las direcciones que se visitan en la red que estamos escaneando.



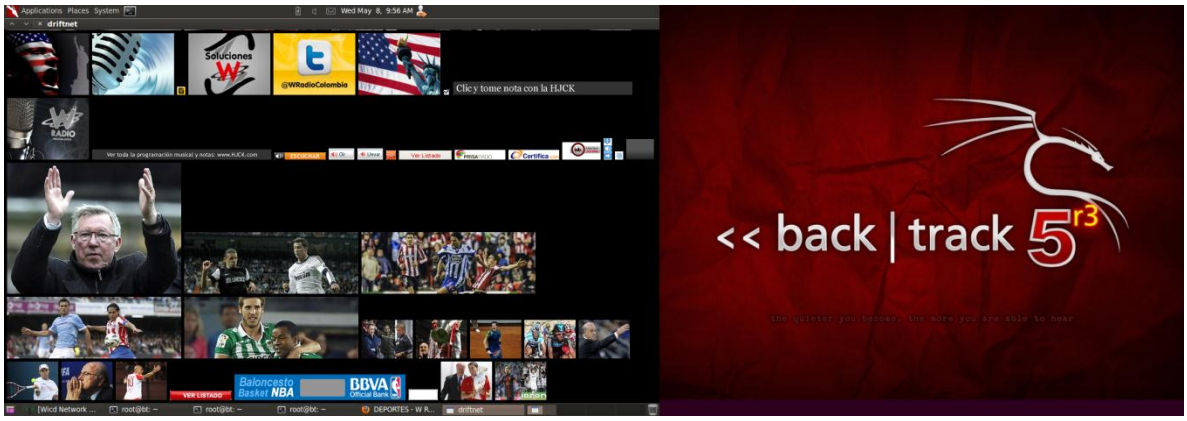




Por ultimo utilizamos DRIFTNET –I WLAN0 con esta herramienta nos muestra de modo grafico lo que esta pasando en la red les recuerdo que estamos snifiando el puerto 80


Applications Places System
Tue May 7, 9:58 AM
root@bt: ~
File Edit View Terminal Help
root@bt:~# driftnet -i wlan0
<< back | track 5 r3
the quieter you become, the more you are able to hear


Applications Places System
Wed May 8, 9:54 AM
driftnet
De Jericó para el Mundo
Santa Madre Laura
No se pierda la gira
Redescwbriendo
Colombia
Mundo W
Haga parte del exclusivo Mundo W, gane muchos premios
¡Inscríbase ya!
Soluciones W
@WRadioColombia
Clic y tome nota con la HJCK
<< back | track 5 r3
the quieter you become, the more you are able to hear



- ✓ **Mecanismos correctivos.** El mecanismo correctivo utilizado fue correr la actualización que permite corregir la vulnerabilidad certificado - CVE-203-3870 en correos Outlook 2010 manualmente en cada uno de los equipos de los funcionarios de la Secretaria de Educación.

- ✓ **Mecanismos disuasivos.** Se realizó capacitación concientizando al usuario para gestionar de modo eficiente su información teniendo un correcto uso de gestión y creación de contraseñas seguras y fuertes, la importancia de la seguridad de la información y lo que puede acarrear su perdida para la empresa.

- Documentar y consultar sobre la seguridad de la información, correo electrónico, protocolos de correo, vulnerabilidad en el transporte, autenticación y gestión de correo electrónico Outlook 2010, información de la empresa a la que se aplicara la solución, leyes y normas que reglamentan el proyecto de investigación

Para desarrollar el primer objetivo específico que cita sobre la documentación e indagación o consulta de todos los conceptos relacionados anteriormente se realizaron consultas en fuentes confiables como libros y artículos de revistas reconocidas, en la Web, además se buscó apoyo en trabajos relacionados con el tema todo lo anterior quedo documentado en nuestro marco conceptual, teórico y legal descrito en las sesiones anteriores.

- Capacitar y concientizar al usuario final sobre la manera adecuada de administrar su correo de forma responsable y así evitar vulnerar su privacidad, además de dar a conocer la importancia de la seguridad de la información para cualquier empresa especialmente para la Secretaria de Educación del Municipio de Duitama.

Para cumplir el objetivo se realizó capacitación al personal administrativo que conforman la secretaria de educación, rectores de los Establecimientos Educativos del municipio de Duitama y Secretarios de los establecimientos Educativos, con una duración de 3 horas denominado **"Seguridad de la Información y el buen uso del correo electrónico Outlook 2010"**,

Se realizó entrega del folleto informativo sobre seguridad de la información que maneja la Secretaria de Educación Municipal buscando el concientizar al usuario final sobre los riesgos que se corren si no se usa adecuadamente correo electrónico Outlook 2010.

- Evidenciar la vulnerabilidad asociada a los mecanismos básicos seguros que deben implementarse en los cliente de correo

Para cumplir el objetivo se realizó indagaciones e investigó en diferentes medios como proyectos relacionados con el tema, la Web, libros y demás artículos que me pudieran documentar sobre que vulnerabilidades o vulnerabilidad se había presentado en la realidad con el Correo Outlook 2010 encontrado como fuente la siguiente información:

Subdirección de Seguridad de la Información - UNAM-CERT -- DGTIC-UNAM Vulnerabilidad de Seguridad UNAM-CERT-2013-062 Vulnerabilidad en Microsoft Outlook podría permitir la ejecución remota de código.

Esta actualización de seguridad resuelve una vulnerabilidad reportada de manera privada en Microsoft Outlook. La vulnerabilidad podría permitir la ejecución remota de código si un usuario abre o visualiza un correo electrónico especialmente diseñado usando una versión afectada de Microsoft Outlook.

• Fecha de Liberación: 10-Sep-2013
• Ultima Revisión: 12-Sep-2013
• Fuente: CVE ID: CVE-2013-3870
• Riesgo: Crítico
• Problema de Vulnerabilidad Remoto: Tipo de Vulnerabilidad Ejecución remota de código y Elevación de privilegios.

Sistemas Afectados:
Microsoft Windows Windows Microsoft Outlook 2007 SP3
Microsoft Windows Windows Microsoft Outlook 2010 SP1 (32-bit editions)
Microsoft Windows Windows Microsoft Outlook 2010 SP1 (64-bit editions)
Microsoft Windows Windows Microsoft Outlook 2010 SP2 (32-bit editions)
Microsoft Windows Windows Microsoft Outlook 2010 SP2 (64-bit editions)

- **Índice de Explotabilidad:** Mensaje de Código de explotación dificil de crear

- **Descripción**: Mensaje de vulnerabilidad certificado - CVE-203-3870 Existe una vulnerabilidad de ejecución remota de código en la forma en que Microsoft Outlook analiza mensajes electrónicos especialmente diseñados en S/MIME. Un atacante que explote por completo esta vulnerabilidad puede tomar el control por completo del sistema afectado. Un atacante podría instalar programas; ver, cambiar o borrar datos; o crear nuevas cuentas con todos los privilegios de usuario. 2. Impacto Mensaje de vulnerabilidad certficado - CVE-203-3870 Un atacante que explote por completo esta vulnerabilidad podría ejecutar código arbitrario como el usuario conectado. Si un usuario está conectado con privilegios de administrador, el atacante podría tomar el control por completo del sistema afectado. Un atacante podría instalar programas.

UNAM-CERT Vulnerabilidad de Seguridad UNAM-CERT-2013-062 Vulnerabilidad en Microsoft Outlook podría permitir la ejecución remota de código cambiar o borrar datos; o crear nuevas cuentas con todos los privilegios de usuario. Usuarios cuyas cuentas estén configuradas para tener pocos privilegios sobre el sistema podrían ser menos impactadas que usuarios que cuenten con privilegios de administrador. [1]

Comparación Con Un Servidor Outlook

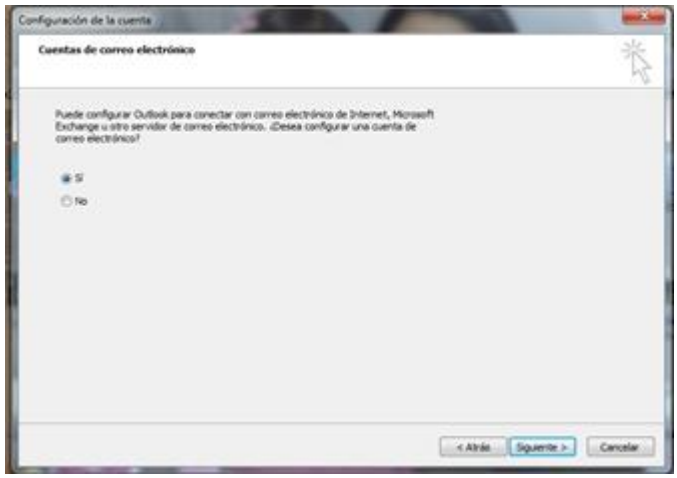
Se realizó comparación del servidor implementado en la Secretaria de Educación Municipal para poder medir factores de riesgo asociados a estrategias seguras y optimizadas y así garantizar seguridad de la información confidencial y personal de más de 16.000 niñas, niños y adolescentes y la comunicación con el servidor.

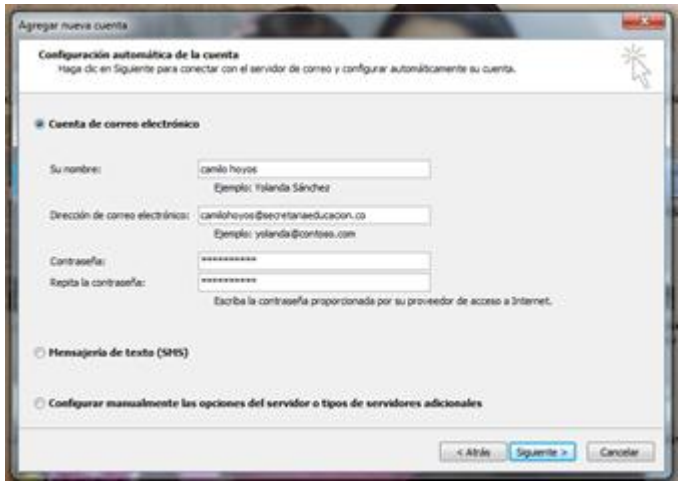
Para cumplir el objetivo se realizaron los procedimientos relacionados a continuación:

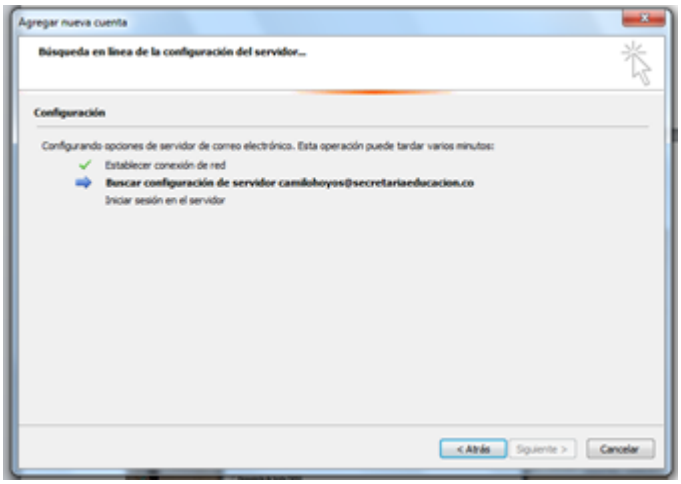
El procedimiento se realizaba automáticamente como se describe a continuación.

[1] subdirección de Seguridad de la Información/UNAM-CERT. Equipo de Respuesta a Incidentes UNAM. Traducido por Edgar Israel Rubi Chavez y Manuel Ignacio Quintero Martínez, 2013.


Inicio de Microsoft Outlook 2010
Inicio de Microsoft Outlook 2010
Éste es el Asistente para inicio de Microsoft Outlook 2010, que le guiará a través del proceso de configuración de Microsoft Outlook 2010.
< Atrás
Siguiente >
Cancelar


Configuración de la cuenta
Cuentas de correo electrónico
Puede configurar Outlook para conectar con correo electrónico de Internet, Microsoft Exchange u otro servidor de correo electrónico. ¿Desea configurar una cuenta de correo electrónico?
Sí
No
< Atrás
Siguiente >
Cancelar


Agregar nueva cuenta
Configuración automática de la cuenta
Haga clic en Siguiente para conectar con el servidor de correo y configurar automáticamente su cuenta.
Cuenta de correo electrónico
Su nombre:
camilo hoyos
Ejemplo: Yolanda Sánchez
Dirección de correo electrónico:
camilohoyos@secretariaeducacion.co
Ejemplo: yolanda@contoso.com
Contraseña:
Repita la contraseña:
Escriba la contraseña proporcionada por su proveedor de acceso a Internet.
Mensajería de texto (SMS)
Configurar manualmente las opciones del servidor o tipos de servidores adicionales
< Atrás
Siguiente >
Cancelar

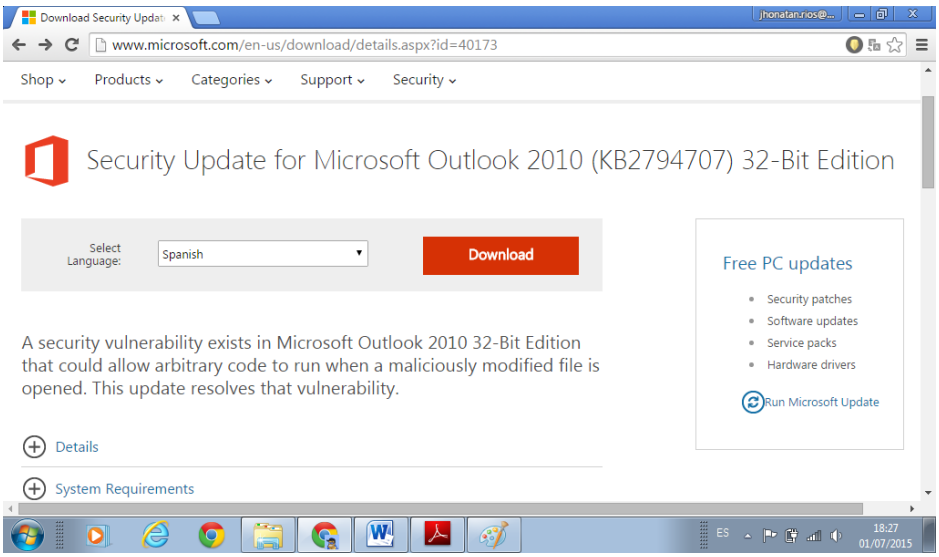


INSTALACION ACTUALIZACION DE SEGURIDAD EN EL SERVIDOR DE CORREOS OUTLOOK 2010

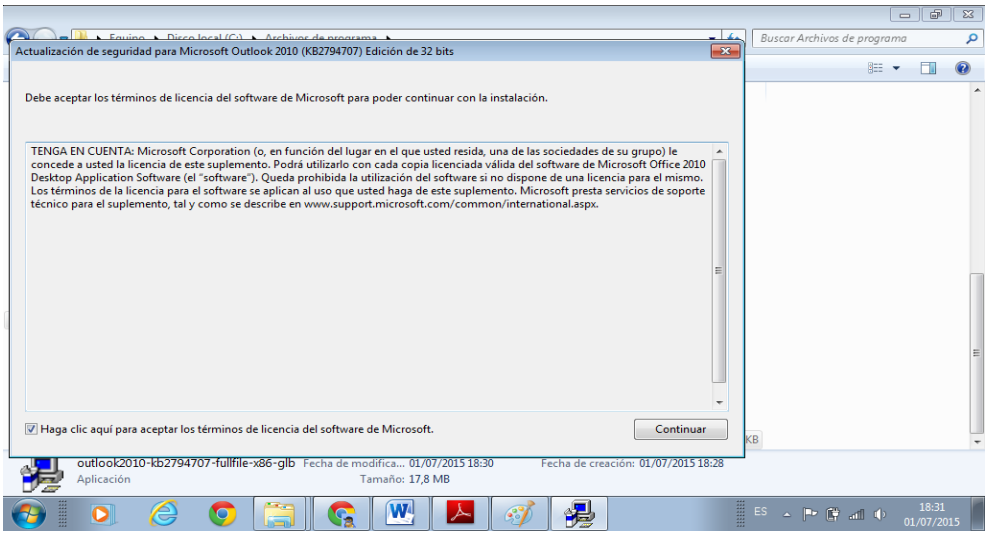
Se realizó la instalación en el servidor de correos Outlook 2010 de la secretaria de educación, en 15 equipos de computo de los funcionarios de secretaria de educación y en los 14 equipos de computo de los establecimientos educativos oficiales que pertenecen a la secretaria de educación actualización de seguridad que resuelve la vulnerabilidad reportada de manera privada en Microsoft Outlook 2010. Logrando la protección de los datos y minimizando la vulnerabilidad de la información transportada mediante correo por los funcionario de las diferentes cedes generando credibilidad y confianza de toda una comunidad frente al manejo de la información soportada en los tres pilares fundamentales de la seguridad de la información disponibilidad, integridad y confidencialidad.

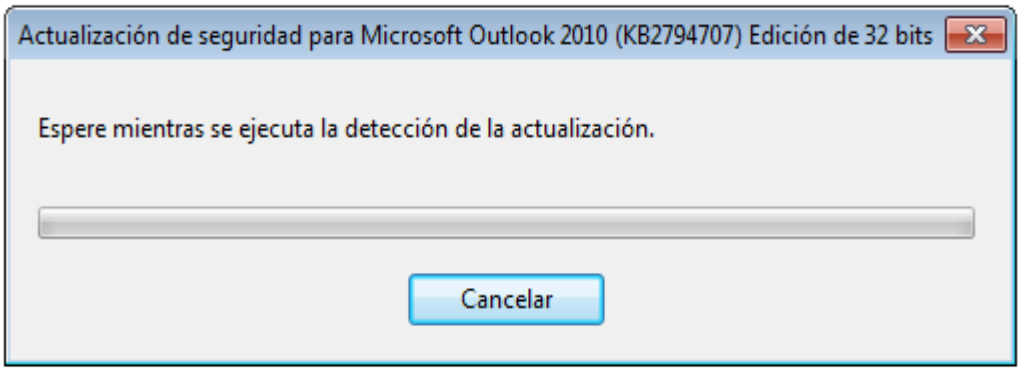
- Procedimiento que se describe a continuación:

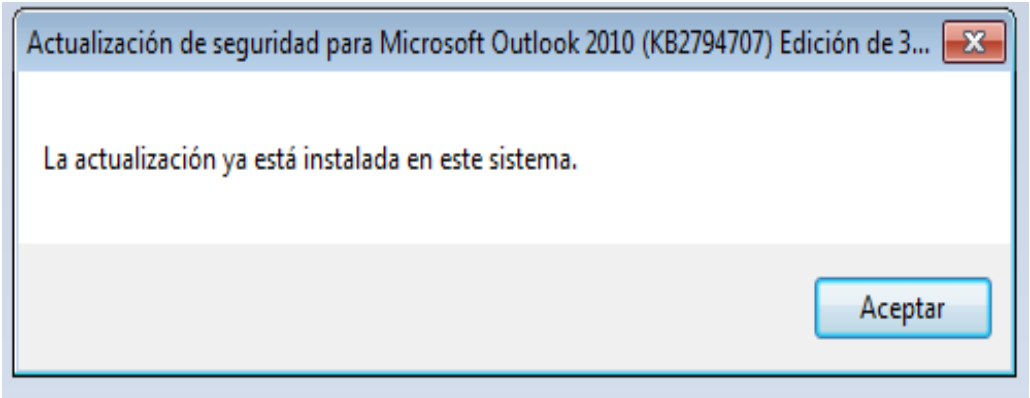
- **Paso 1:** Busca y descarga de la actualización en la Web que corresponda a la versión del Outlook instalado en la maquina.



- **Paso 2:** Ejecutar la Instalación en el equipo de computo.



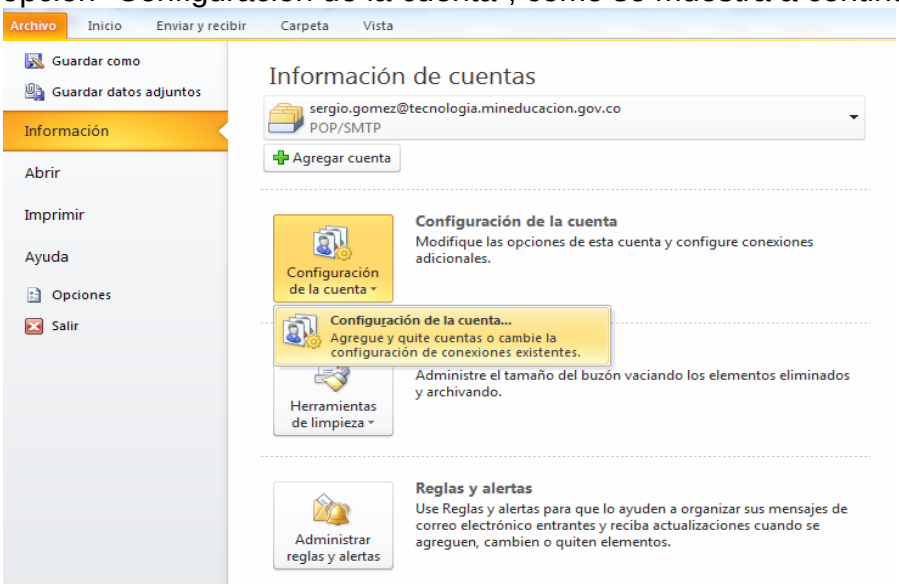




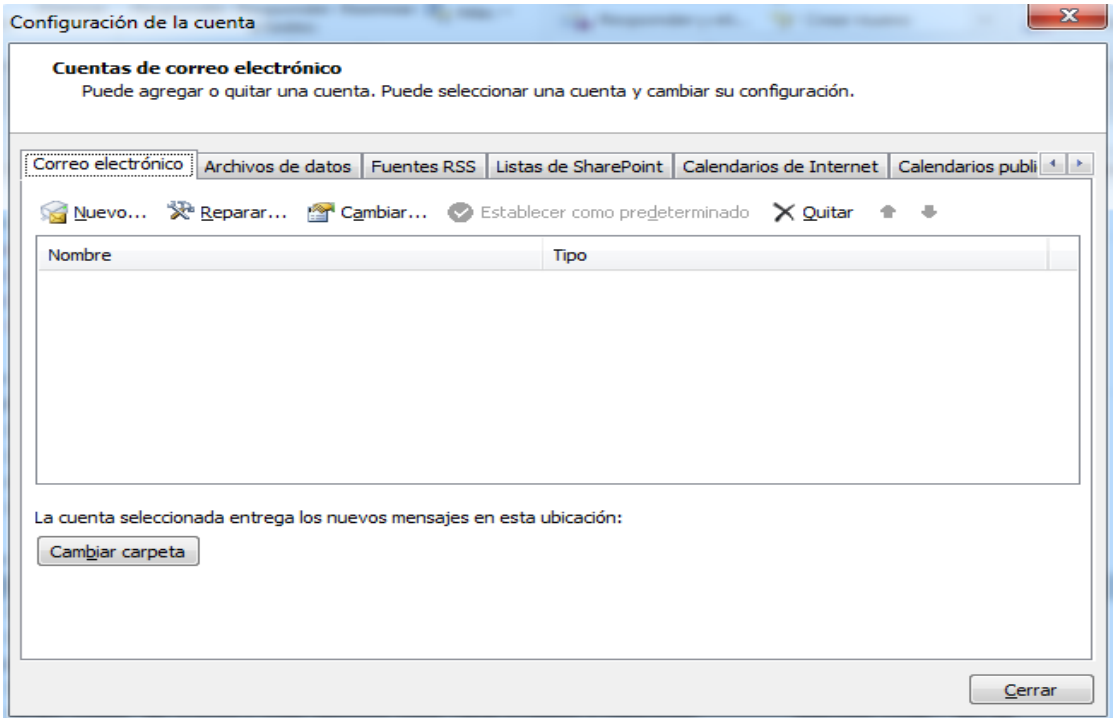
- Se realizó la configuración adecuada que nos permitirá minimizar la vulnerabilidad en el transporte, autenticación y gestión de correo electrónico Outlook 2010 de la Secretaria de Educación Municipal de Duitama como se evidencia en los siguientes pantallazo

CONFIGURACION CORREO OUTLOOK 2010

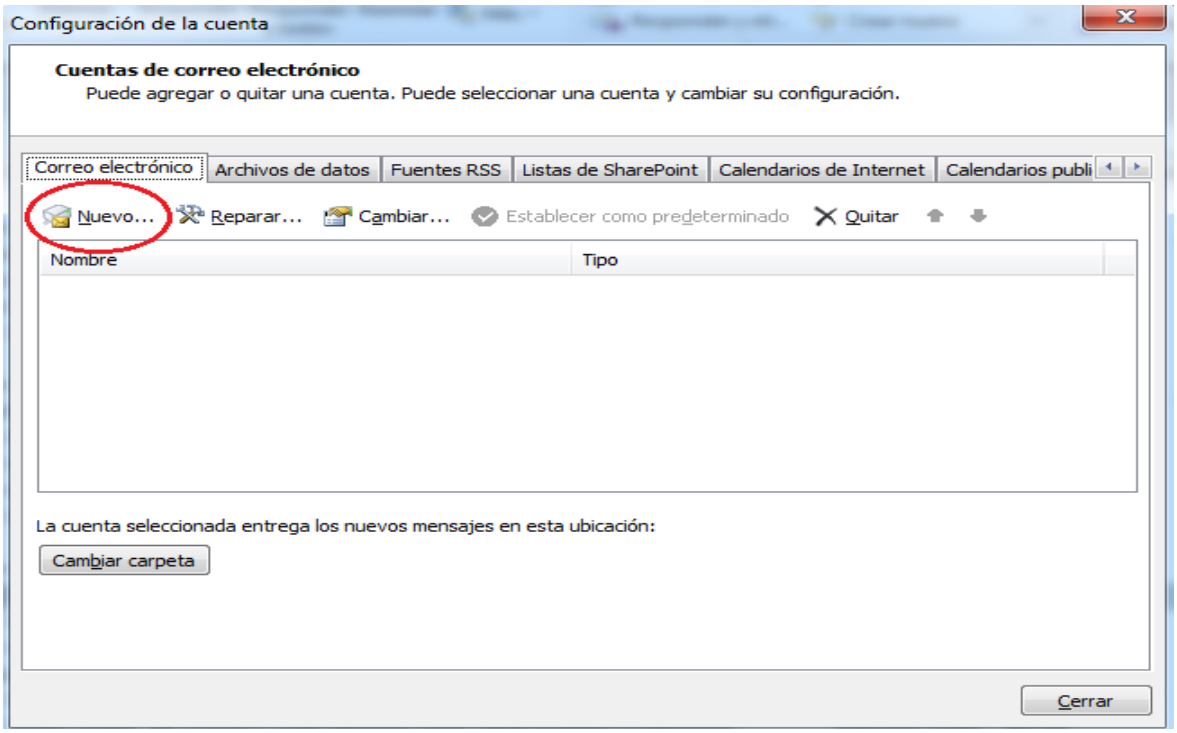
1.- Abre el programa. En el Menú, selecciona la sección "Archivo" y después la opción "Configuración de la cuenta", como se muestra a continuación:



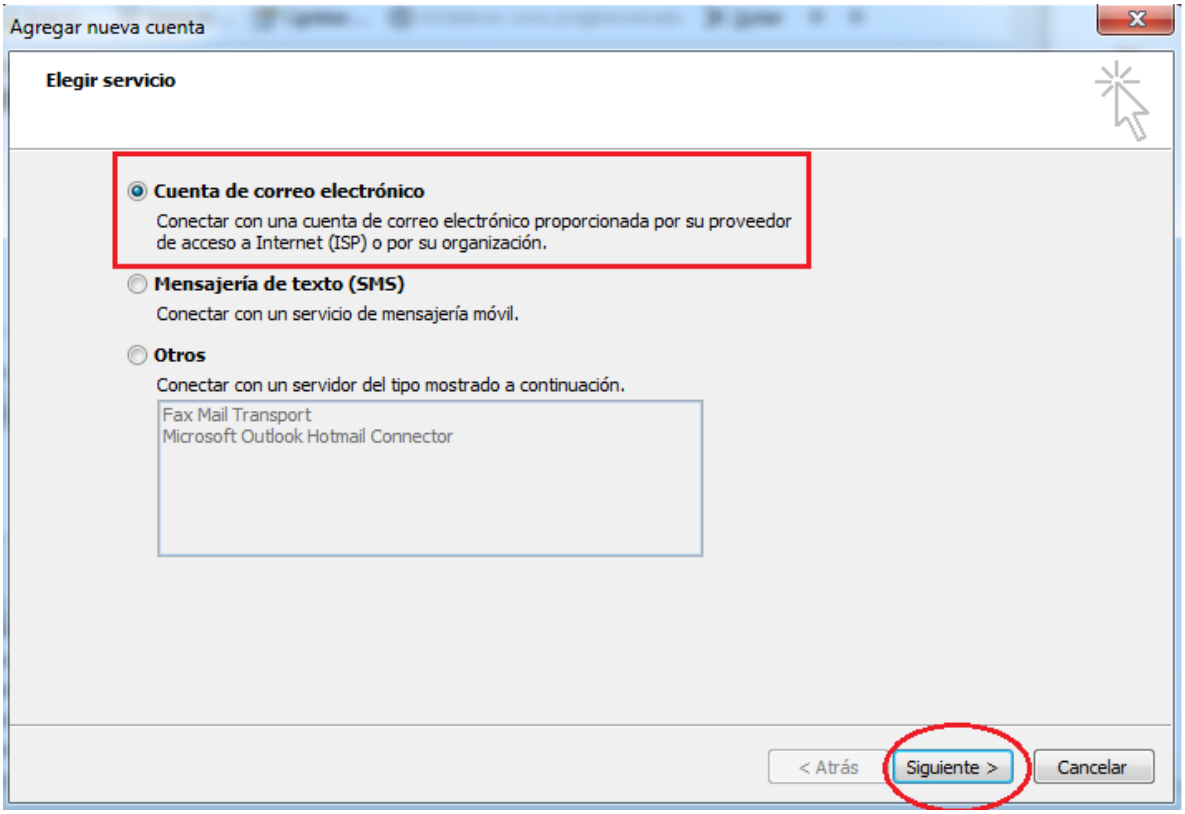
2. En la siguiente ventana selecciona "Nuevo..." para comenzar la configuración de una nueva cuenta de correo:



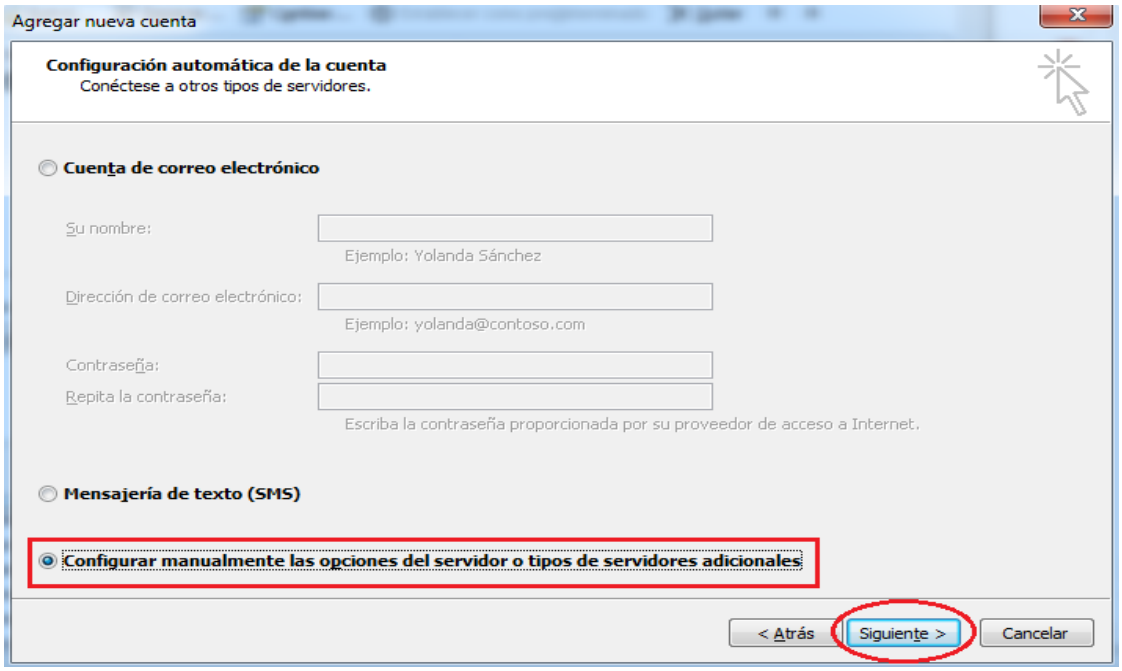
Ahora debemos seleccionar la opción Nuevo, como se muestra en la imagen



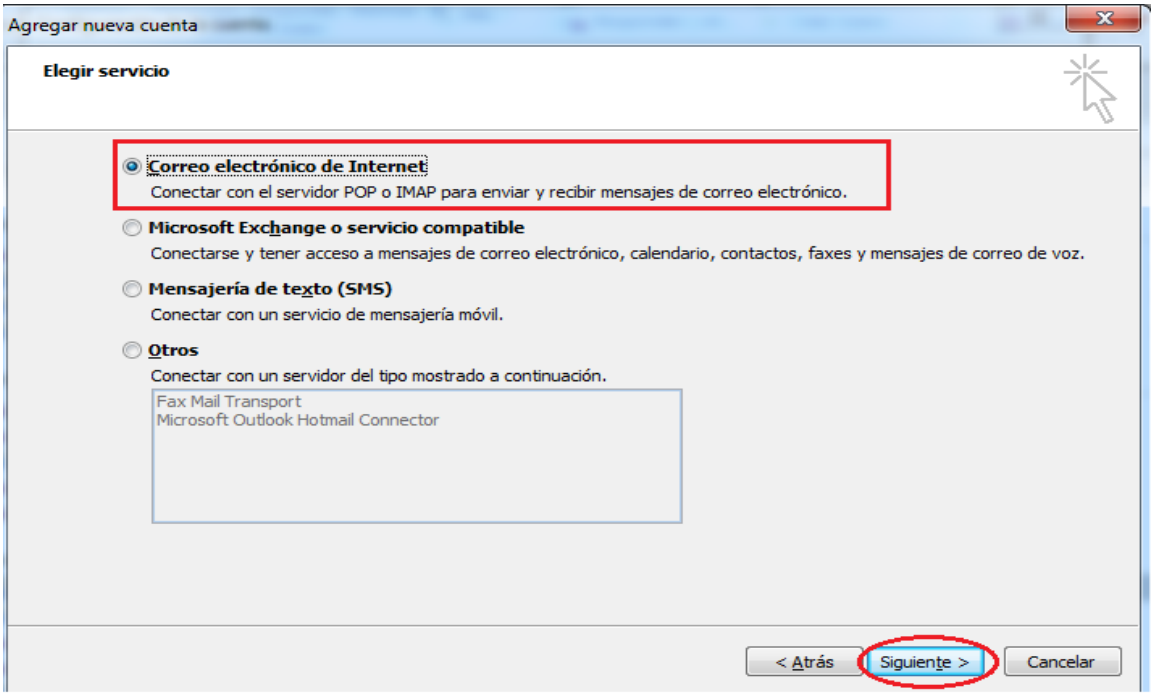
3. En la siguiente ventana selecciona la primera opción:



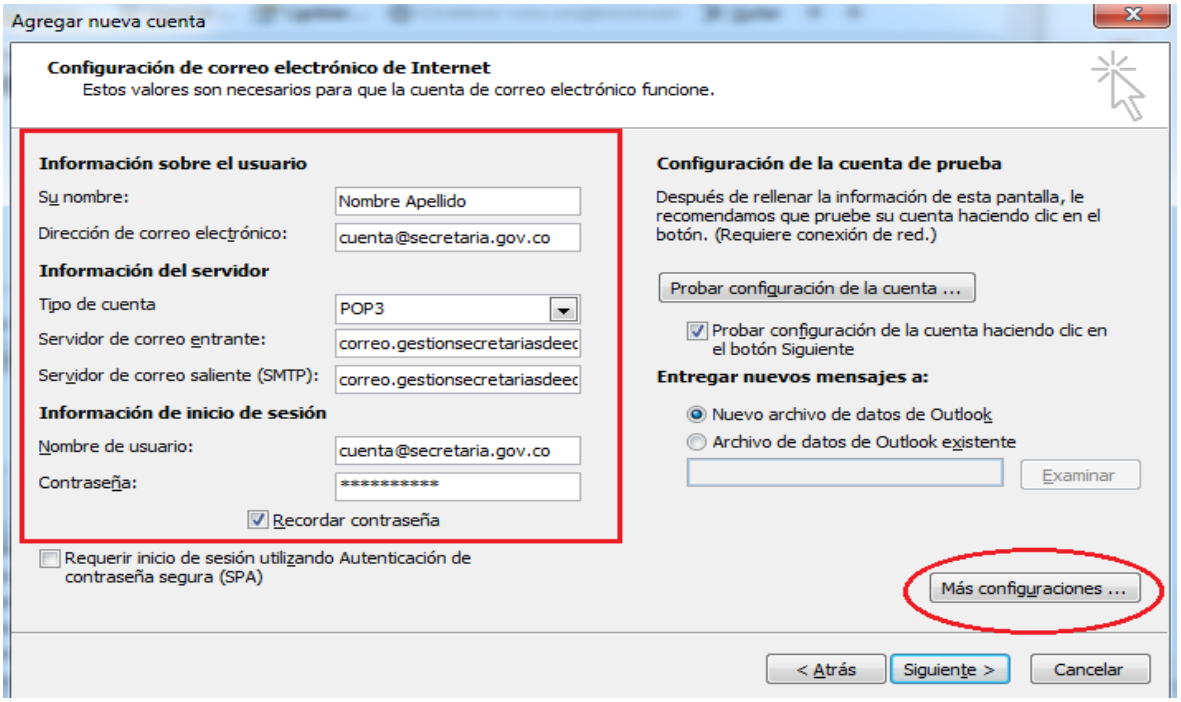
4. En la ventana que se muestra a continuación se deben marcar la última opción Configuración manualmente las opciones del servidor o tipos de servidores adicionales y oprimir SIGUIENTE.



5. Selecciona la primera opción Correo electrónico de internet y oprimimos SIGUIENTE:

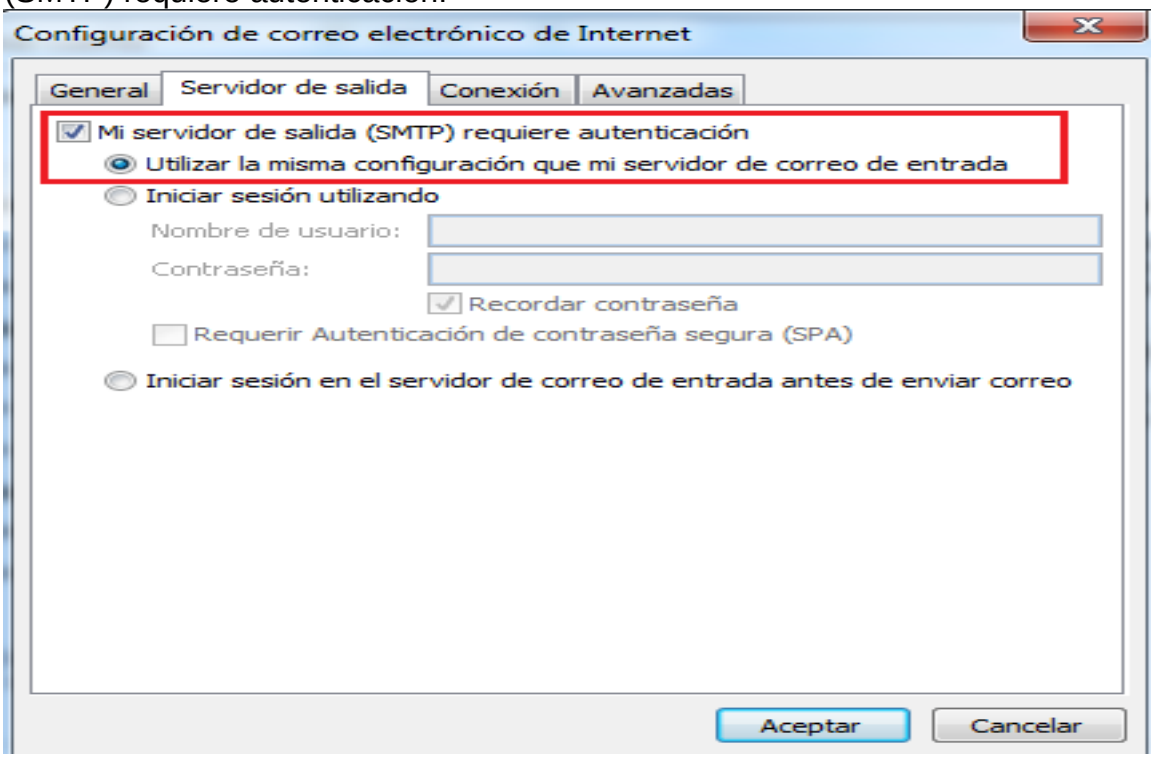


6. Diligenciar los siguientes campos y después accede a "Más configuraciones":

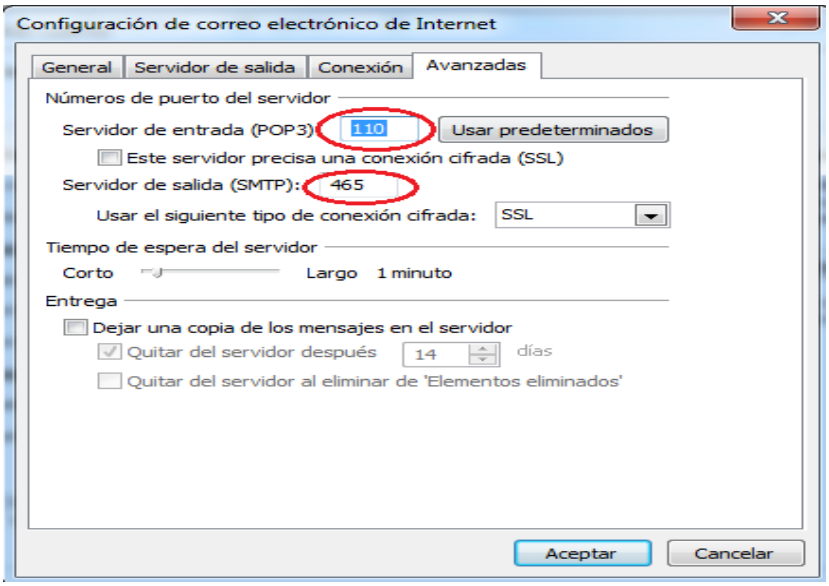


Servidor de correo entrante:
correo.gestionsecretariasdeeducacion.gov.co
Servidor de correo saliente (SMTP):
correo.gestionsecretariasdeeducacion.gov.co

7. En la pestaña "Servidor de salida" marca la opción "Mi servidor de salida (SMTP) requiere autenticación:



8. En la pestaña "Avanzadas" como servidor de salida digitamos "465" y usar conexión cifrada “SSL”. Finalmente oprime ACEPTAR finalizando así la configuración de la cuenta de correo.



12. CRONOGRAMA DE ACTIVIDADES

Fecha de inicio: 15 Abril 2015
Fecha de finalización: 4 de Septiembre 2015
Realizador: Camilo Ernesto Hoyos Males
Asesor: Ing. Martín Camilo Cancelado Ruiz

CRONOGRAMA ACTIVIDADES PROYECTO																											
ITEM	ACTIVIDAD	MES	ABRIL				MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE			
		SEMANA	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Identificar el problema																									
2	Investigar estudio similares																									
3	Justificación del anteproyecto																									
4	Formulación del problema																									
5	Delimitacion consolidacion de objetivos																									
6	Consolidación Documento																									
7	Revisión.																									
8	Producto Final.																									

13. PRESUPUESTO

• **RECURSOS DISPONIBLES**

Descripción	Unidad	Cantidad	Costo unitario	Costo total
Servidor	Unidad	1	$ 50.000.000	$ 50.000.000
Servicio de internet	megas	20 megas	$ 1.666.666	$ 20.000.000
Ingeniero	Unidad	2	$ 3.000.000	$ 6.000.000
computador	Unidad	1	$ 4.000.000	$ 4.000.000
			Total	**$ 80.000.000**

CONCLUSIONES

Con el análisis de las vulnerabilidad existentes en la secretaria de educación se implementaron reglas, herramientas como la utilización de contraseñas fuertes establecidas desde el servidor, la caducidad de las mismas en un tiempo de 30 días calendarios, buzones con no más de 250 megas de almacenamiento en la bandeja principal.

Como resultado de la investigación se logro la identificación de herramientas de gestión que proporcionan mayor nivel de seguridad a los correos electrónicos Outlook 2010 como la configuración de intentos máximos de contraseñas erróneas, un administrador de correos con privilegios elevados para restablecimientos de credenciales, el transporte de información no más de 10 megas como capacidad máxima, mitigando el riesgo de la fuga de información y mejorando la imagen de la institución en la protección de los datos de los usuarios.

A partir de la capacitación realizada se evidencio que la falta de conocimiento es una de las vulnerabilidades más utilizadas por los delincuentes informáticos.

De acuerdo al estudio realizado y descrito anteriormente se identifico el fallo de seguridad que posee el correo Outlook 2010 denominado Certificado - CVE-203-3870 siendo solucionado mediante actualización entregada por el fabricante.

Con el fin de minimizar los riesgos de seguridad de la información se realiza la configuración manual de los correos en cada una de las cedes de la secretaria de educación Duitama.

14. REFERENCIA BIBLIOGRAFÍCA

Aguilera López, Purificación. (2010) *Seguridad Informática*. Madrid - España: Editex SA.

García, Alfonso. Hurtado Cervigón. Alegre Ramos, María del Pilar. (2011) Seguridad informática. Madrid – España: Paraninfo SA.

Auditar Mi PC.com, "GUID - GloballyUniqueIdentifier"- Consultado el 12 de mayo de 2012. Disponibles desde: http://www.auditmypc.com/ acronym/GUID.asp

Boone; Kurtz..(2003) Contemporary Business. New York: Times.

Borghello, Cristian. (2001) Seguridad Informática sus implicancias e implementación. Bogotá: Universidad Tecnológica Nacional.

Huerta, Antonio. (2000). *Seguridad en Unix y redes.* España: Edición.

Regueiro, Arturo. (2009). Autoridades de Certificación y Confianza Digital. Consultado el 4 de mayo de 2012. Disponible desde: http://www.fundaciondike.org.ar/seguridad/firmadigital-autoridades.html
Smilor. (1993). *Al-Ali, Nermien; "Comprehensive Intellectual Capital Management. Step by Step", 2003; John Wiley & Sons, Inc.*New Jersey: Hoboken. 80.

Sophos, "los análisis de virus de Sophos." Consultado el 23 de mayo de 2012. Disponible desde: http://www.sophos.com/virusinfo/analyses/

Summers, Rita C. (1996). *Seguridad informática: Amenazas y Salvaguardias*. México: McGraw-Hill Companies.

Vásquez, Fernando; Rodríguez, Penélope. Solución Negociada de Conflictos. Cali; Pontificia Universidad Javeriana.

Fletscher Bocanegra, Luis Alejandro. (2007). *Implementación de clustersbeowulf como firewall.*

Gómez Guerra, John Alexis. (2007) Modelo de solución de enrutamiento de datos a bajo costo basado en software libre.

García, Alfonso. Hurtado, Cervigón. Algre Ramos, María del Pilar. (2011). Seguridad informática. España. Paraninfo.
Daltabuit Godás, Enrique. Hernández Audelo, Leobardo. Mallén Fullerton, Guillermo. Vázquez Gómez, José de Jesús. (2007) La seguridad de la información. Mexico. Limusa.

Martin, Mercedes. (2008) Guía de seguridad

Universidad de Alicante Disponible desde: http://si.ua.es/es/cau/preguntas-frecuentes-faq/correo-electronico/configuracion-del-correo-saliente-con-autenticacion-y-tls.html#outlook

Antonio. Villalon, (2011) Guía Norma de Seguridad de las Tic (Ccn-Stic-814) Seguridad en Correo Electrónico Disponible desde: ttps://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/814-Seguridad_en_Correo_Electronico/814_Seguridad-en-correo-electronico.pdf

Equipo de Respuesta a Incidentes UNAM. (2013) Vulnerabilidad de Seguridad UNAM-CERT-2013-062 Vulnerabilidad en Microsoft Outlook podría permitir la ejecución remota de código Disponible desde: http://www.seguridad.unam.mx/vulnerabilidadesDB/?vulne=6457.

ANEXO A

PRESENTACION CAPACITACION CORREO ELECTRONICO OUTLOOK

ANEXO B

FOLLETO IMPORTANCIA DE PROTEGER LA INFORMACIÓN DE SU EMPRESA

ANEXO C

REGISTRO DE ASISTENCIA CAPACITACION SEGURIDAD DE LA INFORMACION Y CORREOS OUTLOOK 2010 REALIZADA A LOS FUNCIONARIOS SECRETARIA EDUCACION MUNICIPAL DUITAMA